RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:

Bid Receiving - PWGSC / Réception des soumissions - TPSGC
11 Laurier St. / 11, rue Laurier
Place du Portage, Phase III
Core 0B2 / Noyau 0B2
Gatineau
Quebec
K1A 0S5
Bid Fax: (819) 997-9776

REQUEST FOR PROPOSAL
DEMANDE DE PROPOSITION

Proposal To: Public Works and Government Services Canada

We hereby offer to sell to Her Majesty the Queen in right of Canada, in accordance with the terms and conditions set out herein, referred to herein or attached hereto, the goods, services, and construction listed herein and on any attached sheets at the price(s) set out therefor.

Proposition aux: Travaux Publics et Services Gouvernementaux Canada

Nous offrons par la présente de vendre à Sa Majesté la Reine du chef du Canada, aux conditions énoncées ou incluses par référence dans la présente et aux annexes ci-jointes, les biens, services et construction énumérés ici sur toute feuille ci-annexée, au(x) prix indiqué(s).

Comments - Commentaires

Title - Sujet
ITQ – EAPIMS for Health Canada

Solicitation No. - N° de l'invitation	**Date**
HT300-193651/A	2020-05-08

Client Reference No. - N° de référence du client
HT300-193651

GETS Reference No. - N° de référence de SEAG
PW-$EEM-052-37776

File No. - N° de dossier	**CCC No./N° CCC - FMS No./N° VME**
052eem.HT300-193651	

Solicitation Closes - L'invitation prend fin
at - à 02:00 PM
on - le 2020-06-05

Time Zone
Fuseau horaire
Eastern Daylight Saving Time EDT

F.O.B. - F.A.B.
Plant-Usine: ☐ **Destination:** ☐ **Other-Autre:** ☐

Address Enquiries to: - Adresser toutes questions à:	**Buyer Id - Id de l'acheteur**
Nkiama, Ngoma	052eem

Telephone No. - N° de téléphone	**FAX No. - N° de FAX**
(613) 850-1643 ( )	(819) 956-2675

Destination - of Goods, Services, and Construction:
Destination - des biens, services et construction:

Specified Herein
Précisé dans les présentes

Instructions: See Herein

Instructions: Voir aux présentes

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

Delivery Required - Livraison exigée	**Delivery Offered - Livraison proposée**
See Herein	

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

Telephone No. - N° de téléphone
Facsimile No. - N° de télécopieur

Name and title of person authorized to sign on behalf of Vendor/Firm (type or print)
Nom et titre de la personne autorisée à signer au nom du fournisseur/ de l'entrepreneur (taper ou écrire en caractères d'imprimerie)

Signature **Date**

Issuing Office - Bureau de distribution
Mainframe & Business Software Procurement Division / Div des achats des ordi principaux et des logiciels de gestion
Terrasses de la Chaudière
4th Floor, 10 Wellington Street
4th etage, 10, rue Wellington
Gatineau
Quebec
K1A 0S5

INVITATION TO QUALIFY (ITQ)

FOR

EMPLOYEE ASSISTANCE PROGRAM INFORMATION MANAGEMENT SYSTEM (EAPIMS)

FOR

HEALTH CANADA

IMPORTANT NOTICE:

THIS DOCUMENT CONTAINS A SECURITY REQUIREMENT

TABLE OF CONTENT

PART 1 GENERAL INFORMATION

1.1 Introduction

The Invitation to Qualify (ITQ) is divided into five parts. The five parts are as follows:

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

Part 2 Instructions to Respondents: provides the instructions, clauses and conditions applicable to the Invitation to Qualify (ITQ) phase;

Part 3 Response Preparation Instructions: provides Respondents with instructions on how to prepare their Response and the evaluation criteria that must be addressed;

Part 4 Evaluation Procedures and Selection of Qualified Respondents: indicates how the evaluation will be conducted and the basis of qualification;

Part 5 Certifications: includes the certifications to be provided in the Response, additional certifications may be included in RFP, if any.

1.2 Summary

(a) This Invitation to Qualify (ITQ) is issued by Canada in respect of the Project generally described in Section 1.3 below for the provision of Employee Assistance Program Information Management System (EAPIMS) for Health Canada. The Employee Assistance Services (EAS) Division within Health Canada has, by Order-in-Council, been provided the authority to deliver the Employee Assistance Program (EAP) and related services to federal public agencies, departments and federally regulated organizations.

(b) The purpose of this ITQ is to invite interested parties to submit a Response indicating their interest in, and qualifications for, the Project. Based on these Responses, Canada intends to select, in accordance with the terms of this ITQ, a list of up to eight (8) Qualified Respondents to participate in any subsequent phases of the procurement process, namely the Review and Refine Requirements (RRR) Phase and the Request for Proposals (RFP) Phase for the selection of a single Contractor to provide the required EAPIMS.

(c) In this ITQ, except to the extent where the context or the express provisions of this ITQ otherwise require, any capitalized word or term not otherwise defined in the ITQ Respondent Instructions has the meaning set out for it in Annex A - Definitions and Interpretation.

(d) Any interested party or parties may submit a Response. Respondents may be individuals, corporations, joint venture/consortia, partnerships or any other legal entities.

(e) There are no security clearances required to participate in this ITQ. Annex D – Draft Security Requirements applicable to on premise Solutions at the RFP stage, Annex E - Security Requirements Check List (SRCL) and Annex F – Draft Security Requirements applicable to SaaS Solutions at the RFP stage outline the essential mandatory security requirements applicable to the RFP stage. These requirements address some, but not necessarily all of the requirements which Canada intends to address in the RFP. Additional security requirements may be included in

subsequent phases of this procurement process. Canada is including these requirements in this ITQ to provide respondents advance notice of some of the requirements that are likely to be included in the associated RFP.

(f) Due to the time involved in obtaining such security clearances, potential Respondents are strongly encouraged to initiate the security clearance process and submit to the Contracting Authority the required documentation as soon as possible during the ITQ Stage. A common reason for delay in clearance is incomplete or incorrectly completed documents. As such, potential Respondents are encouraged to check the documents carefully prior to submission.

(g) This ITQ is neither a bid solicitation nor a tender and is intended only to pre-qualify Respondents. No contract will result from this ITQ. This ITQ may be partially or completely cancelled by Canada at any time, and therefore there is no guarantee of a subsequent procurement phase. Because the ITQ is not a tender, Respondents and Qualified Respondents may withdraw from this procurement phase at any time.

(h) This requirement is subject to the provisions of the Comprehensive Economic and Trade Agreement (European Union) (CETA), World Trade Organization - Government Procurement Agreement (WTO-GPA), the North American Free Trade Agreement (NAFTA), the Canada-Chile Free Trade Agreement (CCFTA), the Canada-Peru Free Trade Agreement (CPFTA), the Canada-Colombia Free Trade Agreement (CColFTA), the Canada–Honduras Free Trade Agreement (CHonFTA), the Canada–Korea Free Trade Agreement (CKorFTA), the Canada-Panama Free Trade Agreement (CPanFTA), the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and the Canadian Free Trade Agreement (CFTA).

1.3 Project Information

The overall objective of the Project is to select a single Contractor for the provision of an Employee Assistance Program Information Management System (EAPIMS) as required to meet the needs of Health Canada as set out in Annex B – Draft Statement of Requirements (SOR) and as further defined in the subsequent RFP.

The Contractor selected through the RFP process will be awarded a contract for the provision of required EAPIMS for a period of up to 10 years. The detailed EAPIMS requirements and the terms and conditions of the contract will be provided to those Respondents qualified to participate in the Review and Refine Requirements (RRR) Phase and subsequent RFP process as set out in Part 4 – Evaluation Procedures and Selection of Qualified Respondents, of this ITQ.

While the Contract period will be defined at the RFP stage, it is Canada’s intention to continue to use the EAPIMS for as long as it makes business sense to do so. The contract period will not necessarily reflect the expected useful life of the solution. The Contract will include options that may be exercised in the future to address any necessary time extensions. Canada also intends to benefit from any technological advances (product evolution) that may occur during the useful life of the EAPIMS. Therefore contract amendments may take place as deemed appropriate, so that Canada always has access to the core capabilities of the product as it evolves. It is contemplated that the EAPIMS deliverables may include professional services, a Warranty, Maintenance and Support Services, Training and Documentation.

This procurement process will also allow Canada to make the EAPIMS available to any department or Crown corporation (as those terms are defined in the Financial Administration Act) or any other party for which the Department of Public Works and Government Services is authorized to act from time to time under section 16 of the Department of Public Works and Government Services Act (each a "Client"). Although Canada may make the EAPIMS available to any or all the Clients, this procurement process does not preclude Canada from using another method of supply for entities of the Government of Canada with the same or similar needs.

1.3.1 Project Background

The Employee Assistance Services (EAS) group of Health Canada operates the Employee Assistance Program (EAP) and related services to federal public agencies, departments and federally regulated organizations.

EAS exists within the Specialized Health Services Directorate (SHSD) of the Corporate Services Branch (CSB) of Health Canada and provides 24/7, fully-bilingual, intake and referral, to access confidential, professional, bilingual face-to-face counselling services. EAS operates on a fully cost-recovered basis and is fully accredited by the Council on Accreditation (COA). EAS has nearly 1,000 private practice counsellors located across the country and supports approximately 1.6 million eligible clients (employees and family members) of more than 80 Federal Departments and Agencies, the Canadian Armed Forces, the Royal Canadian Mounted Police and Veterans. EAS is the largest provider of these services to the Federal Public Service.

EAP is the core service provided by EAS. In 2019, the EAP responded to over 77,000 calls and handled nearly 29,200 cases in FY2018-19. It is expected that demand for EAP services will continue to increase in the near future due to continued efforts to reduce the stigma of mental illness and the recent Safe Workspaces initiative commenced by former Clerk of the Privy Council Michael Wernick.

Based on a Request for Information (RFI) conducted by Canada in 2018, commercial off the shelf solutions exist in the marketplace that would address core EAP requirements. The primary group impacted by the implementation of the new solution would be the people involved in the delivery and management of the EAP program such as intake counsellors, the case management team and the call center manager. Secondary groups impacted by the change are the Service Providers and Business Office team due to updates in processes.

1.3.2 Project Objectives

The project's goals are to:

1. Secure and implement a solution that is available all the time (system availability), with rapid response times (system performance) and that is easy to learn and use (user friendly);
2. Have high quality data from various sources available to users without having to go through significant effort (Data Quality);
3. Have a solution that is easy to work with in terms of changes needed to add, remove or modify fields and values from dropdown lists, etc. to address changes in the work environment (system flexibility);
4. Implement a solution that can easily be scaled up or down (scalability);
5. Have operational efficiency; and
6. Ensure Client confidentiality.

1.3.3 Target Environment

The preliminary EAPIMS target environment is as set out in Annex B – Draft Statement of Requirements. The Contractor selected through the ITQ and subsequent RFP process must provide and deliver an integrated EAPIMS where:

1. The EAPIMS must provide and deliver the range of EAPIMS business functionality as set out in Section 3.2 of Annex B – Draft Statement of Requirements and as clarified through the procurement process.

2. The EAPIMS must be deployed on GC provided infrastructure services as set out in Appendix A to Annex B – Draft Statement of Requirements and as clarified through the procurement process.
3. The services are provided for the detailed design, configuration, integration, deployment, transition-in, ongoing support of the provided EAPIMS and the eventual transition-out to a successor solution or services as set out in Section 3.3 of Annex B – Draft Statement of Requirements and as clarified through the procurement process.
4. The EAPIMS must comply with the security requirements of Canada as set out in the ITQ and the subsequent RFP.

1.4 Overview of the Procurement Process

This ITQ is the first phase in the procurement process for the Project. Although the procurement process remains subject to change (and even to cancellation, in accordance with the Standard Instructions), Canada currently anticipates that the procurement process will be conducted in the following phases:

1.4.1 Phase 1: Invitation to Qualify (ITQ)

The objective of this ITQ is to qualify Respondents who meet the requirements of the ITQ (Qualified Respondents). A maximum of eight (8) highest ranked Qualified Respondents will be invited to participate in any subsequent phases of the procurement process. Respondents will be qualified and ranked based on the process set out in Part 4 of this ITQ. In the event of a tie between two or more Respondents as the 8th and final Qualified Respondent, Canada will select all Respondents as Qualified Respondents that are in this situation. If there are less than eight (8) Qualified Respondents then all Qualified Respondents will be invited. The ITQ will be posted on the Government Electronic Tendering Services (GETS) for a period of Twenty Five (25) calendar days, in English and French.

Should there be an insufficient number of Qualified Respondents after Phase 1 to permit subsequent phases, Canada reserves the right to cancel any subsequent phases or to modify the requirements of Phase 1 and re-publish the solicitation using the same or a different approach.

1.4.2 Phase 2: Review and Refine Requirements (RRR)

The RRR process with the Qualified Respondents may be held after the ITQ phase. The objective of the RRR phase is to obtain feedback from Qualified Respondents on Canada's requirements for the Project, including the draft RFP and Resulting Contract Terms and Conditions.

The RRR is intended to be a collaborative process and may involve interactions such as workshops, one-on-one sessions, and/or written questions and answers. Canada will consider the feedback provided by Qualified Respondents when refining the requirements and preparing its procurement documents for the Project. Further details regarding the RRR will be provided to those Respondents who qualify as a result of this ITQ.

1.4.3 Phase 3: Request for Proposals (RFP)

The information provided in this section does not represent a commitment by Canada and is provided solely for information purposes. It may be modified by Canada in its sole discretion, at the RFP stage.

As part of the RFP, Canada intends to invite Qualified Respondents to submit proposals that must contain, in respect of the Project, a technical submission and a financial submission. The form of the RFP submission will be described in the RFP and will address both technical and financial aspects of the Project and may include, at Canada's discretion, a Proof of Proposal. The RFP will be posted on the Government Electronic Tendering Services (GETS) for a period of forty (40) calendar days, in English and French.

The successful Bidder will be identified taking into consideration technical and financial criteria as set out in the RFP. Details regarding the submission requirements for the RFP and the factors to be considered in the evaluation of proposals will be set out in the RFP.

1.5 Conflict of Interest - Unfair Advantage

In order to protect the integrity of the procurement process, Respondents are advised that Canada may reject a Response in the following circumstances:

a) if the Respondent, any of its members or subcontractors, or any of their respective employees or former employees was involved in any manner in the preparation of the strategies and documentation related to this procurement process or is in any situation of conflict of interest or appearance of conflict of interest;

b) if the Respondent, any of its members or subcontractors, or any of their respective employees or former employees had access to information related to this procurement process that was not available to other suppliers and that would, in Canada's opinion, give or appear to give the Respondent an unfair advantage.

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

First Name	Last Name	Organization
Jocelyn	Décoste	BDO Canada LLP
John	Davis	BDO Canada LLP

The experience acquired by a Respondent who is providing or has provided the goods and services described in this ITQ (or similar goods or services) to Canada will not, in itself, be considered by Canada as conferring an unfair advantage or creating a conflict of interest. This Respondent remains, however, subject to the criteria established above.

If Canada intends to disqualify a response under this section, the Contracting Authority will inform the Respondent and provide the Respondent an opportunity to make representations before making a final decision. Respondents who are in doubt about a particular situation should contact the Contracting Authority before the closing date. By submitting a response, the Respondent represents that it does not consider itself to be in conflict of interest nor to have an unfair advantage. The Respondent 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.

1.6 Debriefings

Respondents may request a debriefing on the results of the ITQ phase. Respondents should make the request to the Contracting Authority within 5 working days of receipt of the results of qualification process outlined in this document.

PART 2 RESPONDENT INSTRUCTIONS

2.1 Standard Instructions, Clauses and Conditions

(a) All instructions, clauses and conditions identified in the ITQ by number, date and title are 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.

(b) Respondents who submit a response agree to be bound by the instructions, clauses and conditions of the ITQ.

(c) The 2003 (2019-03-04) Standard Instructions - Goods or Services - Competitive Requirements are incorporated by reference into and form part of the ITQ, except that:

(i) Wherever the term "bid solicitation" is used, substitute "Invitation to Qualify (ITQ)";

(ii) Wherever the term "bid" is used, substitute "response";

(iii) Wherever the term "Bidder(s)" is used, substitute "Respondent(s)".

(iv) Subsection 5.4, which discusses a validity period, does not apply, given that this ITQ invites Respondents simply to qualify. Canada will assume that all Respondents who submit a response continue to wish to qualify unless they advise the Contracting Authority in writing that they wish to withdraw their response.

(d) If there is a conflict between the provisions of 2003 and this document, this document prevails.

2.2 Response Submission Instructions

(a) Responses must be submitted only to Public Works and Government Services Canada (PWGSC) Bid Receiving Unit by the date, time and place indicated in the ITQ.

(b) If the Respondent chooses to submit its response electronically, Canada requests that the Respondent submits its response in accordance with section 08 of the 2003 standard instructions. The epost Connect system has a limit of 1GB per single message posted and a limit of 20GB per conversation.

The approved formats for documents are any combination of:

A. PDF documents; and
B. Documents that can be opened with either Microsoft Word or Microsoft Excel.

The response must be gathered per section and separated as follows:

A. Section I: ITQ Mandatory and Rated Selection Criteria (as described in Annex C - Evaluation and Qualification Criteria)
B. Section II: Certifications and Additional Information

(c) If the Respondent chooses to submit its response in soft copies on electronic media, Canada requests that the Respondent submits its response in separately bound sections as follows:

A. Section I: ITQ Mandatory and Rated Qualification Criteria (as described in Annex C – Evaluation and Qualification Criteria) (2 soft copies on USB keys)
B. Section II: Certifications and Additional Information (2 soft copies on USB keys)

(d) If the Respondent is simultaneously providing copies of its response using multiple acceptable delivery methods, and if there is a discrepancy between the wording of any of these copies and the electronic copy provided through epost Connect service, the wording of the electronic copy provided through epost Connect service will have priority over the wording of the other copies.

(e) Note that no prices must be indicated in the ITQ Response.

(f) Due to the nature of this ITQ responses transmitted by facsimile will not be accepted.

2.3 Enquiries

(a) All enquiries must be submitted in writing to the Contracting Authority no later than 5 calendar days before the ITQ closing date. Enquiries received after that time may not be answered.

(b) Respondents with questions regarding this ITQ may direct their enquiries to:

Contracting Authority: Ngoma Nkiama

E-mail Address: Ngoma.Nkiama@tpsgc-pwgsc.gc.ca

(c) Respondents should reference as accurately as possible the numbered item of the ITQ to which the enquiry relates. Care should be taken by Respondents to explain each question in sufficient detail in order to enable Canada to provide an accurate answer.

(d) 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 questions or may request that the Respondent do so, so that the proprietary nature of the question is eliminated, and the enquiry can be answered with copies to all Respondents. Enquiries not submitted in a form that can be distributed to all Respondents may not be answered by Canada.

2.4 Joint Venture Experience

(i) Except where expressly provided otherwise, where the Respondent is a joint venture with existing experience as that joint venture, it may submit the experience that it has obtained as that joint venture. A joint venture Respondent may rely on the experience of one of its members to meet any given mandatory requirement of this ITQ.

(ii) Joint venture members cannot pool their abilities with other joint members to satisfy a single mandatory requirement of this ITQ. However, a joint venture member can pool its individual experience with the experience of the joint venture itself. Wherever substantiation of a mandatory requirement is required, the Respondent is requested to indicate which joint venture member satisfies the requirement.

(iii) Any Respondent with questions regarding the way in which a joint venture response will be evaluated should raise such questions through the Enquiries process as early as possible during the ITQ period.

(iv) Example 1: A Respondent is a joint venture consisting of members X, Y and Z. If a Response requires: (a) that the Respondent has 3 years of experience providing maintenance service, and (b) that the Respondent has 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 requirement, such as the requirement for 3 years of experience providing maintenance services, the Respondent cannot include that each of members X, Y and Z has one year of experience, totaling 3 years. Such a response would be declared non-responsive.

(v) Example 2: A Respondent is a joint venture consisting of members L and M. A Response requires that the Respondent demonstrates 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 Respondent has previously done this work. This Respondent 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 in that ITQ.

(vi) Example 3: A Respondent is a joint venture consisting of members A and B. If a Response requires that the Respondent demonstrates experience providing resources for a minimum number of 100 billable days, the Respondent may demonstrate that experience by submitting either:

- Contracts all signed by A, or
- Contracts all signed by B, or
- Contracts all signed by A and B in joint venture, or
- Contracts signed by A and contracts signed by A and B in joint venture, or
- Contracts signed by B and contracts signed by A and B in joint venture.

That show in total 100 billable days.

2.5 Applicable Laws

The relations between the parties will be determined by the laws in force in Ontario, Canada.

Note to Respondents: A respondent may, at its discretion, substitute the applicable laws of a Canadian province or territory of their choice without affecting the validity of its response, by deleting the name of the Canadian province or territory specified and inserting the name of the Canadian province or territory of its choice. If no change is made, it acknowledges that the applicable laws specified are acceptable to the Respondent. Respondents are requested to indicate in their Master ITQ Submission Form the Canadian province or territory they wish to apply to their response.

PART 3 RESPONSE PREPARATION INSTRUCTIONS

3.1 Response Preparation Instructions

(a) Canada requests that Respondents provide their response as follows:

(i) Section I: ITQ Mandatory and Rated Qualification Response (as described in Annex C – Evaluation and Qualification Criteria);

(ii) Section II: Certifications and Additional Information

Pricing is not a requirement and should not be included in the response.

(b) **Language for Future Communications:** Respondents are requested to identify in the Master ITQ Submission Form their language of choice (English or French) for future communications with Canada regarding this procurement process and solicitation documents.

3.2 Qualification Response

Respondents must demonstrate that they have the required expertise and experience in a thorough, concise and clear manner. Simply repeating the criteria is not sufficient.

(a) A Qualification Response consists of the following:

(i) **Master ITQ Submission Form:** Respondents are requested to include the Master ITQ - Submission Form with their responses. It provides a common form in which Respondents can provide information required for evaluation, such as a contact name, the Respondent's Procurement Business Number, the Respondent's status under the Federal Contractors Program for Employment Equity, etc. Using the Master ITQ - Submission Form to provide this information is not mandatory, but it is recommended. If Canada determines that the information required by the Master ITQ Submission Form is incomplete or requires correction, Canada will provide the Respondents with an opportunity to do so.

(ii) **Mandatory Qualification Criteria**: The technical response must substantiate the compliance with the specific criteria of the Mandatory Qualification Requirements as set out at Annex C. The substantiation must not simply be a repetition of the requirement(s), but must explain and demonstrate how the Respondent meets the requirements to carry out the required Work. Simply stating that the Respondent or its proposed solution or resources comply is not sufficient. Where Canada determines that the substantiation is not complete, the Respondent will be considered non-responsive and disqualified. The substantiation may refer to additional documentation submitted with the response.

(iii) **Rated Qualification Criteria:** The technical response should substantiate compliance with the specific criteria of the Rated Qualification Requirements as set out at Annex C. Criteria in this section, while not mandatory themselves, will be used to provide a ranking of Respondents that meet the Mandatory Qualification Criteria describe in section (ii) above. The substantiation must not simply be a repetition of the requirement(s), but must explain and demonstrate how the Respondent meets the requirements. Simply stating that the Respondent or its proposed solution or resources comply is not sufficient. Where Canada determines that the substantiation is not complete, the Respondent will not receive a score for that given criterion. The substantiation may refer to additional documentation submitted with the response.

(iv) **Previous Project References Forms**: Respondents are requested to use the Form C-1 – Previous Project Reference Forms where compliance is determined through an external customer reference solution implementation. Although all the content of Form C-1 is required, using the form itself to provide this information is not mandatory. For

Respondents 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 C-1 may result in the response being declared non-responsive. The Respondent should, at a minimum, provide with the response the name, the title, the telephone number, e-mail address and role in the project of the external customer's person who possessed oversight or approval authority over the work as a contact person. If the external customer's contact information is not provided with the response, the Contracting Authority will so inform the Respondent and provide the Respondent with a timeframe within which to submit the information. Failure to comply with the request of the Contracting Authority and meet the requirement within the time-period will render the response non-responsive. If the named individual is unavailable when required during the evaluation period, the Respondent may provide the name and contact information of an alternate contact from the same external customer. If more external customer references are provided than requested, Canada will evaluate the reference in order they have been submitted by the Respondent up to the number of references requested.

PART 4 EVALUATION PROCEDURES AND SELECTION OF QUALIFIED RESPONDENTS

4.1 Evaluation Procedures

(a) Responses will be evaluated in accordance with the entire requirement of the ITQ, including the mandatory and rated qualification criteria. There are multiple steps in the evaluation process, which are described below. Even though the evaluation 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 Respondent has successfully passed all the previous steps. Canada may conduct steps of the evaluation in parallel.

(b) An evaluation team composed of representatives of Canada will evaluate the responses. Canada may hire any independent consultant, or use any Government resources, to evaluate any response. Not all members of the evaluation team will necessarily participate in all aspects of the evaluation.

(c) In addition to any other time periods established in the ITQ:

(i) **Requests for Clarifications**: If Canada seeks clarification or verification from the Respondent about its response, the Respondent 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 response being declared non-responsive.

(ii) **Requests for Further Information**: If Canada requires additional information in order to do any of the following pursuant to the Section entitled “Conduct of Evaluation” in 2003, Standard Instructions - Goods or Services - Competitive Requirements:

(A) verify any or all information provided by the Respondent in their response;

(B) contact any or all references supplied by the Respondent to verify and validate any information submitted by the Respondent,

the Respondent must provide the information requested by Canada within 2 working days of a request by the Contracting Authority.

(iii) **Extension of Time**: If additional time is required by the Respondent, the Contracting Authority may grant an extension in his or her sole discretion.

4.2 Response Evaluation

(a) **ITQ Mandatory Qualification Criteria:** Each response will be reviewed for compliance with the ITQ Mandatory Qualification Criteria outlined in the ITQ. Any element of the bid solicitation that is identified specifically with the words "must" or "mandatory" is a mandatory requirement. Response that do not comply with each and every mandatory requirement will be declared non-responsive and be disqualified.

(b) **Point-Rated Qualification Criteria:** Each response will be rated by assigning a score to the rated requirements, which are identified in the ITQ by the word "rated" or by reference to a score. Respondent who fail to submit complete response with all the information requested by this ITQ will be rated accordingly. The point-rated qualification criteria are described in Annex C - Evaluation and Qualification criteria.

4.3 Reference Checks

(a) For reference checks, Canada will conduct the reference check in writing by email. Canada will send all email reference check requests to contacts supplied by all the Respondents on the same day using the email address provided in the response. A Respondent will not meet the mandatory experience requirement (as applicable) unless the response is received within 10 working days of the date that Canada's email was sent.

(b) On the fifth working day after sending out the reference check request, if Canada has not received a response, Canada will notify the Respondent by email, to allow the Respondent to contact its reference directly to ensure that it responds to Canada within 10 working days. If the individual named by a Respondent is unavailable when required during the evaluation period, the Respondent may provide the name and email address of an alternate contact person from the same customer. Respondents 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 Respondent 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 10 working days will not be extended to provide additional time for the new contact to respond.

(c) Wherever information provided by a reference differs from the information supplied by the Respondent, the information supplied by the reference will be the information evaluated.

(d) Points will not be allocated and/or a respondent will not meet the mandatory experience requirement (as applicable) if (1) the reference customer states he or she is unable or unwilling to provide the information requested, or (2) the customer reference is not a customer of the Respondent itself (for example, the customer cannot be the customer of an affiliate of the Respondent instead of being a customer of the Respondent itself). Nor will points be allocated or a mandatory met if the customer is itself an affiliate or other entity that does not deal at arm's length with the Respondent.

(e) Whether or not to conduct reference checks is discretionary. However, if PWGSC chooses to conduct reference checks for any given rated or mandatory requirement, it will check the references for that requirement for all Respondents who have not, at that point, been found non-responsive.

4.4 Financial Viability Assessment

Respondents must be financially viable to enter into this Qualification process. To determine the Respondent's financial viability, the Contracting Authority may, by written notice to the Respondents, require the submission of some or all of the financial information detailed below during the evaluation of the responses.

The Respondent must provide the following information to the Contracting Authority within 5 working days of the request or as specified by the Contracting Authority in the notice:

a. Audited financial statements, if available, or the unaudited financial statements (prepared by the Respondent's outside accounting firm, if available, or prepared in-house if no external statements have been prepared) for the Respondent's last three fiscal years, or for the years that the Respondent has been in business if this is less than three years (including, as a minimum, the Balance Sheet, the Statement of Retained Earnings, the Income Statement and any notes to the statements).

b. If the date of the financial statements in (a) above is more than five months before the date of the request for information by the Contracting Authority, the Respondent must also provide, unless this is prohibited by legislation for public companies, 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.

c. If the Respondent has not been in business for at least one full fiscal year, the following must be provided:

   i. the opening Balance Sheet on commencement of business (in the case of a corporation, the date of incorporation); and

   ii. 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.

d. A certification from the Chief Financial Officer or an authorized signing officer of the Respondent that the financial information provided is complete and accurate.

If the Respondent is a joint venture, the financial information required by the Contracting Authority must be provided by each member of the joint venture.

If the Respondent is a subsidiary of another company, then any financial information in (a) to (d) above required by the Procurement Authority must be provided by the ultimate parent company.

The Respondent is not required to resubmit any financial information requested by the Procurement Authority that is already on file at PWGSC 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:

a. the Respondent identifies to the Procurement Authority in writing the specific information that is on file and the requirement for which this information was provided; and

b. the Respondent authorizes the use of the information for this requirement.

It is the Respondent's responsibility to confirm with the Contracting Authority that this information is still on file with PWGSC.

Canada reserves the right to request from the Respondent any other information that Canada requires to conduct a complete financial capability assessment of the Respondent. The Respondent also understands that a complete financial capability review of the Respondent may also be conducted during the subsequent RFP process.

Confidentiality: If the Respondent 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 as permitted by the *Access to Information Act*, R.S., 1985, c. A-1, Section 20(1) (b) and (c).

Respondents must submit their financial statements for the legal entity outlined in their Response. Canada reserves the right to request further information if required.

4.5 Selection of Qualified Respondents

A Response must comply with the requirements of the ITQ, meet all mandatory technical evaluation criteria and obtain the required minimum scores for the rated evaluation criteria as specified in Annex C - Evaluation and Qualification Criteria, to be declared responsive.

For each Response, the rated score for each of the rated evaluation criteria will be added to obtain a total aggregate score.

The eight (8) Qualified Respondents with the highest total aggregate score will be selected as the Qualified Respondents for subsequent participation in any subsequent phases of the procurement process.

In the event of a tie between two or more Respondents as the 8th and final Qualified Respondent, Canada will select all Respondents as Qualified Respondents that are in this situation.

If there are less than 8 Qualified Respondents, all Qualified Respondents will be selected for participation in any subsequent phases of the procurement process. Should there be an insufficient number of Qualified Respondents after the ITQ Phase to permit a competition in subsequent phases of the procurement process, Canada reserves the right to cancel any subsequent phases of the procurement processor to modify the requirements of the ITQ phase and re-publish the solicitation using the same or a different approach.

Canada reserves the right to re-evaluate the qualification of any Qualified Respondent at any time during the procurement process. For example, if the Respondent's security clearance changes or lapses, so that the Respondent no longer meets the requirements of the ITQ, Canada may disqualify the Qualified Respondent.

4.6 Invitation to Sign a Submission Agreement

The Contracting Authority will invite a maximum of eight (8) Respondents who have qualified in accordance with section 4.5 above to sign the Submission Agreement, as a condition of being selected to participate in any subsequent phases of the procurement process.

If any of these Qualified Respondents fail or refuse to execute the Submission Agreement within the allocated period, the Contracting Authority may, in its sole discretion, withdraw the invitation and extend it to the next highest ranked Qualified Respondent to sign the Submission Agreement, and participate in any subsequent phases of the procurement processing accordance with the Submission Agreement.

PART 5 CERTIFICATIONS

(a) Respondents must provide the required certifications to be declared a “qualified” Respondent. The certifications provided by Respondents to Canada are subject to verification by Canada at all times. Canada will declare a Response non-responsive, or will declare a contractor in default if any certification made by the Respondent is found to be untrue, whether made knowingly or unknowingly, during the evaluation period or during the contract period. The Contracting Authority will have the right to ask for additional information to verify the Respondent's certifications. Failure to comply and to cooperate with any request or requirement imposed by the Contracting Authority will render the response non-responsive or constitute a default under the Contract.

(b) The required certifications should be submitted with the response, but may be submitted afterwards. If any of these required certifications is not completed and submitted as requested, the Contracting Authority will inform the Respondent 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 provided will render the response non-responsive.

5.1 Integrity Provisions - Declaration of Convicted Offences

(a) In accordance with the Integrity Provisions of the Standard Instructions, all bidders must provide with their bid, **if applicable**, the Integrity declaration form available on the Forms for the Integrity Regime website (http://www.tpsgc-pwgsc.gc.ca/ci-if/declaration-eng.html), to be given further consideration in the procurement process.

ANNEXES AND FORMS

ANNEX A – DEFINITIONS AND INTERPRETATION

1. Acronyms

Acronym or Abbreviation	Definition
ATO	Authority to Operate
CM	Case Management
DOS	Designated Organizational Screening
DR	Disaster Recovery
EAPIMS	Employee Assistance Program Information Management System
FSC	Facility Security Clearance
GC	Government of Canada
PB	Protected B
PSPC	Public Services and Procurement Canada
PSTN	Public Switched Telephone Network
QA	Quality Assurance
RFP	Request for Proposals
RTO	Recovery Time Objectives
SOR	Statement of Requirements
SRCL	Security Requirements Checklist
SSC	Shared Services Canada
TA	Task Authorization

2. Definitions

Terms	Meaning
Acceptance Test	Any and all tests of all or any part of the Deliverables to be carried out by Canada or its representatives to determine if such Deliverables conform to the requirements, Specifications, warranties and standards set out in or incorporated into the Statement of Requirements.
Application	Any program or group of programs that is designed for the end user and includes all documentation, source code, media, data and databases that perform specific data processing and telecommunication tasks.
Amendment	An addition to, deletion from, correction or modification of any solicitation document, resulting agreement or contract.
Authority to Operate	An Authorization to Operate (ATO) is a formal declaration by a Designated Approving Authority (DAA) that authorizes operation of an IT solution and explicitly accepts the risk to agency operations. The ATO is signed after a Certification Agent (CA) certifies that the system has met and passed all security requirements to become operational. An interim authorization to operate may be issued for a short period of time, or under limited conditions, until it is approved or denied. In the context of this contract the final Certification Agent will be ESDC IT Security.
Business Day	A day other than a Saturday, Sunday or statutory holiday in the Province of Ontario

Terms	Meaning
Business Hours	The hours of 6:00 AM through 6:00 PM inclusive during a Business Day in the Location of Work in which the work is being formed.
Business Unit	An organizational unit within a company (e.g.: a division or unit within the Bidder's organization) or a company (e.g.: specialized subcontractor) that provides a focal point for the provision of specialized skills or expertise in a target business area, service delivery area or infrastructure service. These specialized skills, services or expertise can be demonstrated by subject-area specific assets within that unit or company, and these assets may include but are not limited to people, processes and potentially specific infrastructure or technologies that provide heightened capabilities in that target business area.
Canada	Her Majesty the Queen in Right of Canada as represented by the Minister of Public Works and Government Services Canada
Commercially Available	"Commercially Available" means that the software or services as proposed is freely available for purchase, has a published product / service definition and pricing structure, and has an ongoing funded development and support investment behind it. In the case where the Solution consists of multiple, independent products, each product proposed must be "commercially available" as defined above. ALPHA or BETA versions of a product or service do NOT qualify as commercially available.
Contractor	Means the person, entity or entities named in the Contract to supply goods, services or both to Canada.
Core EAPIMS	As a Commercially Available product, an Integrated software solution that offers at least the following functional capabilities in its COTS instance: [Intake Management; Case Management; Service Provider Management; Referral Management; Report Management; User Management; Financial Management; Portal Management]
COTS	Commercial-off-the-shelf, i.e. Commercially Available products.
Data centre	Contractor or Third Party Facility used to house networked computer servers typically used by organizations for the centralized call processing, network management services, remote storage, processing, or distribution of large amounts of data.
Disaster Recovery (DR)	The ability of an organization to respond to significant events that result in the temporary inability of the organization to function normally. With respect to provision of hosted critical business systems and services, DR incorporates specific capabilities to minimize service disruption by providing, for example, data centre services protection that is provided out of region and across data centres using replication technologies such as platform based replication and asynchronous storage based replication.
Documentation	Documents, whether in printed or electronic form, including installation guides, instructional materials, layouts, maintenance materials, manuals, system documentation, training materials, and user guides, and includes all developments and modifications to the foregoing.
Employee	A person that has a formal employer/employee relationship with the Bidder/Contractor as defined by the Canada Revenue Agency (CRA).
End User	Internal staff or external parties that have been granted access to the Application for use.
Enquiry	The meaning set out in this ITQ Section 2.3.
Facility(ies)	The location(s) within the sovereign territory of Canada from which the Contractor will provide and deliver EAPIMS related service as required by Canada.
Facility Security Clearance (FSC):	A clearance that permits the recipient of the clearance and its security-cleared employees to access Sensitive Information and/or restricted work sites
Incident	"Incident" as defined for ITIL V.3 means an unplanned interruption to an IT Service or a reduction in the quality of an IT Service.
Integrated	A software solution that, while potentially comprised of two or more modules (e.g. geolocation, reporting, CRM, portal), and without compromising functionality, reliability, security or system performance, provides the end-to-end user experience of a single application.
ITIL	Information Technology Infrastructure Library. See https://www.itlibrary.org/

Terms	Meaning
Joint venture	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, sometimes referred as a consortium, to respond together on a requirement. In any contract they will be determined as being joint and several.
Master Project Schedule	The Master Project Schedule identifies the major milestones with associated business outcomes, deliverables and target dates associated with the transition of the current EAPIMS to the provided EAPIMS as provided by the selected Contractor.
Platform	General purpose information systems components used to process and store electronic data, such as desktop computers, servers, network devices, and mobile devices. Platforms usually contain server hardware, storage hardware, utility hardware, software and operating systems.
Procurement Authority	The authority identified in Summary of Key Information
Product	Any copyrighted/trademarked item that has been manufactured and marketed for sale off the shelf and for which the name of the manufacturer and the model or version # can be easily identified.
Project	As described in Section 1.3 and further defined in Annex B – Statement of Requirements, for the provision of EAPIMS software and services in support of the Government of Canada Employee Assistance Program within Health Canada
Proposal	The formal proposal submitted by a Proponent or Bidder in response to the RFP
PWGSC	Public Works and Government Services Canada, also known as Public Services and Procurement Canada (PSPC)
Rated Qualification Criteria	The rated qualification criteria set out in Annexx C – Evaluation and Qualification Criteria
Recovery Point Objective (RPO)	The maximum tolerable period of time in which data might be lost from an IT service due to a major incident.
Recovery Time Objective (RTO)	The duration of time and a service level within which a business process must be restored after a disaster
Respondent	The person or entity (or, in the case of a consortium, the persons or entities) submitting a Response for this ITQ.
Respondent Team	for a Respondent means the Respondent and all of its Team Members
Response	The formal response by a Respondent to this ITQ submitted to Canada
RFP	The Request for Proposals, as amended over time
Scalability	The ability to run the Software Solution on whatever size system makes sense and be able to move that application to either smaller or larger systems when needed.
Services	All technical and professional services provided in accordance with the resulting contract and must include, without limitation, those services required to: 1. plan, design, install, configure, test, make operational, and support the Project throughout the term of the agreement; 2. provide project-related training and documentation; 3. provide ongoing operation of the Work both prior to and after Acceptance by Canada; 4. provide transition-out support on conclusion of the contract however this condition arises.
Service Request	A request for services issued to the Contractor for work within the scope of an authorized TA.
Software Solution	The suite of software products required to meet the requirements as defined in an associated statement of requirements. The Software Solution as proposed may consist of a software product augmented by plug-ins to meet individual functional requirements, or, may consist of an integrated suite of core portal environment and complementary function (products), or other combination of software products that in combination meet the requirements. The Software Solution may in whole or in part provide a solution.

Terms	Meaning
Solution	The sum total of all products and implementation services as contemplated by the requirements set out in the associated Statement of Requirements or Statement of Requirements prepared by Canada for a specific business requirement and provided in accordance with the technical and financial proposals presented by a Bidder in its written response to an ITQ, RFP or similar request.
Subcontractor	An entity with whom a supplier has a direct contractual relationship to perform a portion of the Work pursuant to a contract between the Contractor and Canada, unless the subcontractor merely supplies commercial-off-the-shelf goods to the Contractor.
Successful Bidder	The Bidder selected by Canada through the RFP process and recommended for Contract award
System	A generic term used to mean network and other devices, operating systems, computing platforms, virtualization software and applications or any combination thereof. Its use is context specific.
Task Authorization (TA)	A TA is a structured administrative tool enabling PWGSC or a client to authorize work by a contractor on an "if and when requested" basis in accordance with the conditions of the contract.
User Acceptance Testing	The test phase where the user(s) from the client organization test the application to ensure that it works and satisfies the business needs and is consistent with the requirements as expressed in the application Statement of Requirements.
Work	Means all the activities, services, goods, equipment, matters and things required to be done, delivered or performed by the Contractor under the Contract.

Annex B
Draft Statement of Requirements (SOR)

Regarding

Provision of an Employee Assistance Program Information Management System

For

Employee Assistance Services (EAS) Division within Health Canada (HC)

NOTE: This Draft SOR is a concise version of the anticipated statement of requirements. A detailed version of the SOR will be provided during the solicitation stage of this procurement process.

TABLE OF CONTENTS

1 INTRODUCTION

This Statement of Requirements (SOR) sets out the high-level requirements regarding the provision of an Employee Assistance Program Information Management System to satisfy the needs of the Employee Assistance Services (EAS) division within Health Canada.

EAS division exists within the Specialized Health Services Directorate (SHSD) of the Corporate Services Branch (CSB) of Health Canada and provides 24/7 confidential, professional, bilingual counselling services. EAS has nearly 1,000 private practice counsellors located across the country and supports approximately 1.6 million eligible clients (employees and family members) of more than 80 Federal Departments and Agencies including the Canadian Armed Forces, the Royal Canadian Mounted Police and Veterans. EAS is the largest provider of these services to the Federal Public Service.
The overall objective of this procurement approach is to select a single, qualified provider of an Employee Assistance Program (EAP) Information Management System and associated implementation and support services as required to meet the needs of Employee Assistance Services organization within Health Canada.

Within this SOR:

1. Section 1 provides an overview of the project objectives and scope.
2. Section 2 provides an overview of the current EAS program within Health Canada as background information for this opportunity.
3. Section 3 provides a preliminary high-level scoping of the target EAPIMS environment with emphasis on the overall functional, non-functional and deployment requirements, end-to-end target environment and highlighting those elements provided by Canada and those required to be provided by the Contractor.
4. Section 4 identifies the major preliminary schedule associated with the transition of the current EAS Solution to the provided EAPIMS as provided by the selected Contractor.

1.1 Project Objectives

The project's objectives are to procure and implement an Employee Assistance Program Information Management System that:

1. Provides and delivers a software solution that meets the business functional, non-functional, security and related requirements as set out in this SOR.
2. Deploys and operationalizes the solution within the timelines in the Master Project schedule set out in Section 4 of this SOR.
3. Addresses the challenges exhibited by the current, legacy environment including:

a. Providing high solution availability and performance.
b. Providing ease of use for both novice / infrequent users and experienced users that are using the system on a daily basis in stressful user encounters.
c. Having high quality data from various sources available to users without having to go through significant effort (Data Quality);
d. Having a solution that is easy to work with in terms of changes needed to add, remove or modify fields and values from dropdown lists, etc. to address changes in the work environment (system flexibility);
e. Implementing a solution that can easily be scaled up or down (scalability);
f. Having operational efficiency; and
g. Ensuring Client confidentiality.

The new system will serve five **strategic** purposes:

1. Enable an integrated approach to all of the operational activities that fall within scope of the system, namely:
    a. Intake, referral, case management and quality assurance functions
    b. Management activities, such as case load oversight and risk monitoring that support the functions referred to in item a. above
    c. Appropriate user access protocols to ensure “need to know” access can be established internally via “super user” or “administrator” levels of access and delegation
    d. Supporting secure web based interactions through a dedicated portal with affiliate service providers for scheduling, referral and invoicing
2. Have sufficient flexibility for EAS staff (depending on role delegation) to tailor fields, forms and reports without requiring customized coding;
3. Support near-real-time results-based reporting (broadly: service utilization by department/agency, various demographic data, outcomes evaluations);
4. Allow for improved and user-defined analytics to better inform decision making with regards to where improvements efforts (including both operations and promotional efforts) would be most optimal;
5. Have inherent capacity to scale both vertically (increase in overall business volume and revenue) and horizontally (e.g. increased data analysis and reporting) with the evolution of EAS as a service provider.

With those strategic goals addressed, the EAS’s Service line Managers, Contracted Affiliate Service Providers, Staff Counsellors, Case Management Specialists, and EAS’ Business Office will use the EAPIMS to:

1. Receive, triage and refer (i.e. refer to affiliate counsellors and providers) requests for services from organizational clients and family members.

2. Work with (including: search, access, view, cross-reference, manipulate, make changes, save changes) “case” files for the purposes enabling day-to-day service coordination, administration, monitoring and follow-up (i.e. perform all activities from intake to invoicing via the solution).
3. Enable user-defined Key Performance Indictors (KPIs) to be identified, saved and reported on.
4. Allow for near real-time accounting of affiliate service providers billing and payments to date.
5. Enable managers to monitor caseloads per case management specialist and intake counsellor.
6. Via time based flags, ensure that cases do not go unallocated or become dormant.
7. Capture, access and protect federal government employees’ (and their family members’) personal information.
8. Support effective and efficient coordination of activities and communication among internal stakeholders.
9. Promote consistency and best practices in the delivery of employee assistance program services as well as minimize the administrative burden through built-in service level standards; auto-generation of pre-defined case management tasks; auto-generation of case notes; access to pre-designed template letters and forms; and direct access to EAP guidelines.
10. Safeguard federal government employee information so that only those users of the system with the appropriate authority are authorized to access this information.
11. Easily identify trends that highlight potential issues and gaps, and inform changes to EAS practices and strategies.
12. Monitor and evaluate the performance of EAP through management dashboards and the generation of pre-defined and custom reports from a user’s desktop.

1.2 Scope of Requirements

The Contractor must provide and deliver an integrated EAPIMS and related services where:

1. The EAPIMS must provide and deliver the range of EAP business functionality as set out in this Section 3.2 of this SOR and as clarified through the procurement process.
2. The EAPIMS must be deployed on GC provided infrastructure services as set out in Appendix A to this SOR and as clarified through the procurement process.

3. The services are provided for the detailed design, configuration, integration, deployment, transition-in, ongoing support of the provided EAPIMS and the eventual transition-out to a successor solution or services as set out in Section 3.3 of this SOR and as clarified through the procurement process.
4. The EAPIMS must comply with the security requirements of Canada as set out in ITQ Annexes D, E and F and as clarified through the procurement process.
5. The EAPIMS must comply with the accessibility requirements as set out in GC's Standard on Web Accessibility as set out in Section 3.4 to this SOR and as clarified through the procurement process.

2 THE CURRENT EAS MODEL

2.1 Program Overview

Employee Assistance Services (EAS) within Health Canada delivers the Employee Assistance Program (EAP) and related services to federal public agencies, departments and federally regulated organizations including the Canadian Armed Forces, the Royal Canadian Mounted Police and Veterans.

The lines of service the EAS provides are:

1. Employee Assistance Program (EAP)
2. Specialized Organizational Services (SOS)
3. Informal Conflict Management (ICM)
4. Trauma Management
5. Psycho-Social Emergency Preparedness and Response (PSEPR)
6. Occupational and Critical Incident Stress Management (OCISM)

The Employee Assistance Program (EAP) is one of EAS' service lines. A fully accredited EAP by the Council on Accreditation (COA), it responded to over 77,000 calls and handled nearly 29,200 cases in FY2018-19. It is expected that demand for EAP services will continue to increase in the near future due to the Clerk of the Privy Council's focus on having safe and mentally healthy workplaces and Public Servants taking action as they become more aware of issues related to mental health.

The focus for this EAPIMS procurement is to select and have implemented a new solution that meets EAP's operational needs, streamline processes and take into account the Data Strategy Roadmap of the Federal Public Service.

For that majority of central departments and agencies, Health Canada has a direct role in helping their employees (and their family members) maintain and improve their overall mental health and wellbeing, the direct benefits of which includes: increased resilience to stress and operational stress injuries; improved productivity in the workplace; and reduced absenteeism.

The Policy on Results (effective July 1, 2016) has strengthened the requirements of departments and agencies to define and report on clear outcomes indicators. In addition, stemming from the priorities of the Clerk of the Privy Council, the focus on mental health and wellbeing in the public service (Federal Public Service Workplace Mental Health Strategy, effective November 28, 2016) is front and centre in that departments are required to develop action plans as a means of improving overall mental health in the workplace. With this move toward a whole of government approach to wellness, the ability to monitor and report on results is a minimal operational requirement.

In consideration of the scope of services provided, expected growth moving forward - all occurring within results-based operational and outcomes frameworks - the need for a solution that will meet EAS's current and future needs is of strategic significance.

2.2 Current EAS Enabling Technologies

Currently, numerous business tools are used in support of overall programme delivery. Collectively, these are used to:

- Manage intake and referral for the Employee Assistance Program's 24 hour\7 day 1-800 Crisis and Referral Centre (CRC – 400+ calls / day);
- Perform Case Management activities
- Manage customer contacts including detailed invoicing instructions for all customer organizations;
- Recruit and manage a nationwide network of approximately 1,000 active Service Providers;
- Make up-to-date customer information accessible to EAS Managers (special instructions, client eligibility, services provided, limitations, etc.);
- Follow-up complaints and manage quality assurance issues;
- Generate utilization data that is provided to EAS Organizations;
- Manage key contact information (organizational customers, organizational representatives, affiliate service providers);
- Produce management reports on a regular and/or on an as-needed basis;
- Track needs analysis and Service Request related information; and
- Track financial data.

The key components of the current information system were built and maintained using Lotus Notes. FileMaker, an application development platform, has been used to address some of the Division's needs.

Functionality gaps and evolution in the lines of service has also meant that workarounds and manual processes have been implemented to address numerous needs. The diagram below (Figure 2.2-1) provides a high-level overview of the systems and applications used by EAS for operating the EAP with the following table, Table 2.2-1 providing more detail.

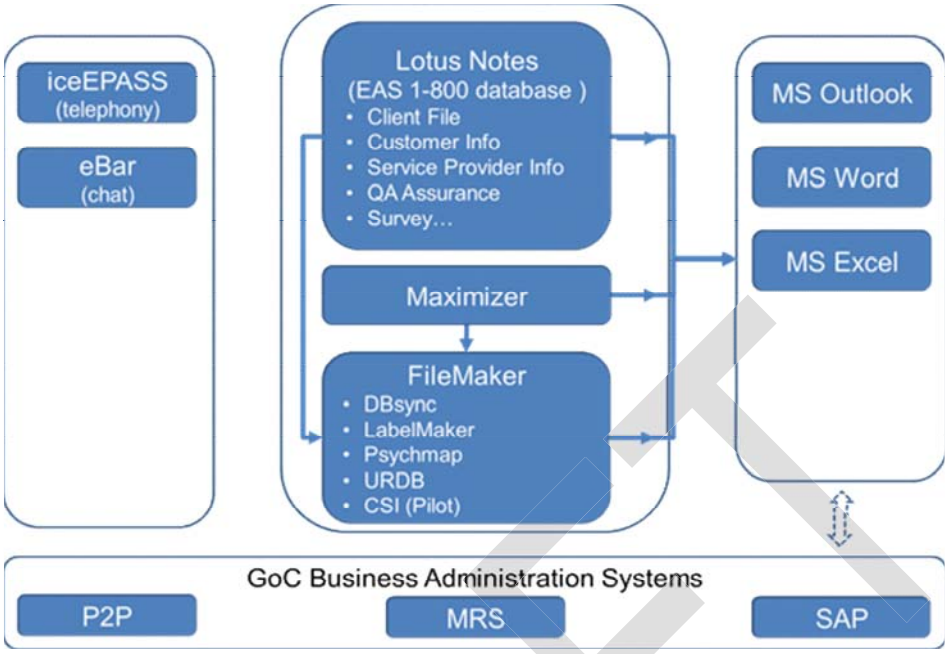

Figure 2.2-1: Current EAS System Diagram

Table 2.2-1: Current EAS Enabling Technologies

System or Interface	Description
Lotus Notes Database	A COTS solution used to create the current version of EAS 1-800 Application for meeting the needs of the Employee Assistance Program run by EAS. Captures and manages client, case, survey, and statistical information pertinent to the EAP program. Data captured in EAS 1-800 feeds into reporting applications created in FileMaker.
Maximizer	A COTS CRM (Customer Relationship Management) solution. Two databases track Service Provider and Organizational Account information. Maximizer is used to output field data to MS Word templates for formatted document outputs and contracts.
DBsync	An application built on the FileMaker platform to compare data from multiple databases containing overlapping datasets for identifying discrepancies and correcting errors in the source data.
LabelMaker	An application built on the FileMaker platform for creating physical file labels. This includes Service Provider billing files (700+ per year) and labels for large mail outs. Labels can be formatted to include specific information such as region, location coding and fiscal year.

System or Interface	Description
PsychMAP	An application built on the FileMaker platform to aid users in locating Service Providers by geolocation (latitude and longitude). For EAP, the data is imported from the Lotus Notes 1-800 database. PsychMAP also serves as the primary Service Provider Management tool for the Specialized Organizational Services (SOS) group.
URDB	An application built on the FileMaker platform to generate client-facing utilisation reports, as well as to process utilisation data for inclusion on a multitude of other reports (Annual Revue and Program Plan, Budget Reports, reports on counselling costs, QA reports, etc.). The application manages saved report configurations per account, batch report generation, and saving of aggregate information.
CSI	An application built on the FileMaker platform to facilitate Service Provider data entry and reporting activities. CSI normalises data entered, ensures that all data is valid before submission, generates invoices based on session information entered, manages extension requests & authorized time per case, and helps track the status of payments. Invoices are generated in HTML format (plain text) so they can be submitted to EAS in a non-proprietary format.
MS Outlook	A COTS solution used for communicating with individuals via e-mail, for tracking tasks and contacts, and for scheduling meetings and presentations.
MS Word	A COTS solution used for creating and editing documents. Examples of documents EAS creates using MS Word: contracts, letter templates, forms, letters, and manual reports.
MS Excel	A COTS solution used to for data analysis and status tracking.
SAP	The Govt. of Canada's financial account system used for entering and tracking financial data (revenues and expenses) and generating payments to Service Providers.
FileMaker	A COTS application development platform used for creating applications in house so processes can be automated, increasing the quality of the final work product and ensuring effective and efficient use of resources.

2.3 Program Stakeholders

There are a range of stakeholders in the delivery of EAS programs and services in addition to those government employees seeking assistance. These range from the portfolio of service providers providing services to employees seeking assistance to the various administrative, management and oversight stakeholders employed in the operation of the programs and services. Figure 2.3-1 illustrates the scope and context of stakeholders and their interaction with the systems and solutions. Tables 2.3-1 and 2.3-2 provide more detail regarding these stakeholders and their functions.

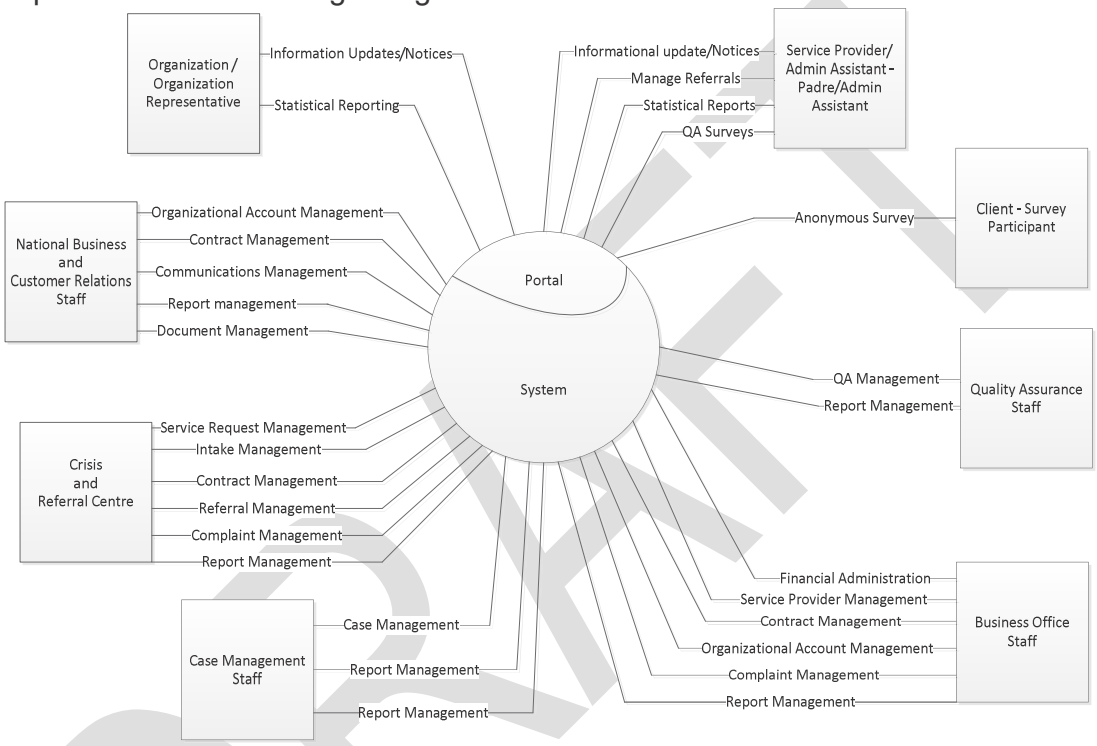

Figure 2.3-1: EAP Stakeholder Business Context Diagram

Table 2.3-1 External EAP Stakeholders

Stakeholder Type	Description	Responsibilities	Approx. # of Stakeholders
Service Provider	A Service Provider is an individual who provides services for EAS Organizational Accounts as well as for EAS directly (e.g. EAS requisitions the Service Provider to develop material, documentation, presentations, etc. on behalf of EAS). Stakeholder would benefit from easier contract management (creation & amendment), time tracking and invoice processing.	Providing services to the client that the entity has been contracted for and staying within the budgeted amount. Submitting required documentation to EAS.	800
Service Provider Admin Assistant	A Service Provider Admin Assistant is an individual who works for a Service Provider. Stakeholder would benefit from easier contract management (creation & amendment), time tracking and invoice processing.	Assisting the Service Provider in meeting their contractual commitments from an administrative perspective.	200
Padre	A Padre is a military chaplain qualified to provide counselling services offered by EAS for military veterans and/or their family. They are treated as “regular” contractors.	Counselling clients who are associated with the military.	30

Stakeholder Type	Description	Responsibilities	Approx. # of Stakeholders
Customer/ Organizational Account	An Organizational Account is a federal entity such as a federal government department or agency, crown corporation or federally regulated organization representing the whole, or a portion of an, Organization with which EAS contracts. Includes the Canadian Armed Forces, the Royal Canadian Mounted Police and Veterans. User does not interact directly with the system.	Encouraging its employees to use EAP services they have contracted for with EAS and prompt payment of fees.	100
Customer Organization Representative	An Organization Representative is a representative of an Organization who has financial signing authority for securing EAP services for their respective organization.	Acting as a key point of contact with the EAS Account Manager and ensuring proper flow of communications between EAS and the representative's organization.	125
Organizational Primary EAP Contact	An Organizational Primary EAP Contact is the primary point of contact within the Organizational Account to liaise with concerning EAP matters. User does not interact directly with the system.	Responsible for proper communication between the EAS Account Manager and stakeholders in the Organizational Account	200
Telephone Interview Service Provider	A Telephone Interview Service Provider is a supplier contracted by EAS to conduct telephone interviews with EAP users on their level of satisfaction with the service they received. EAP users who are contacted have previously agreed to participate in the survey. User does not interact directly with the system.	Conducting telephone interviews with users of EAP services, tabulating the results and disseminating the aggregated information with the EAS team.	1

Stakeholder Type	Description	Responsibilities	Approx. # of Stakeholders
Client	A Client is any person who calls requesting EAP services. The Client may be qualified for access to the EAP based on criteria established for their particular Organization or may be an unqualified caller. The qualified EAP Client is usually an employee or an individual who is related to an employee of a federal government organization - federal government department or agency, crown corporation, federally regulated organization including the Canadian Armed Forces, the Royal Canadian Mounted Police and Veterans. The Client may also be a Survey Participant. Would indirectly benefit from a system that is easy for the CRC counsellor to use as the whole call-in experience would be seamless.	Using the EAP in the manner it was intended.	25,000
Callers	Any person that contacts the EAP.		70,000

Table 2.3-2 Internal EAP Stakeholders

Stakeholder Type	Description	Responsibilities	Approx. # of Stakeholders
Crisis and Referral Center (CRC)			
Crisis and Referral Center (CRC) Logistics Coordinator	Coordinates CRC Counsellor activities. Coordinates and conducts training. Replaces CRC Supervisor when needed. Interested in having a system that is easy to navigate, to train others on, has proper documentation, able to generate management reports.	Coordinating counsellor activities, conducting training sessions and replacing the CRC Supervisor if and when needed.	1
Manager of Counselling Services and Quality Assurance (QA)	Manager of the Case Management team; CRC Supervisor; and QA Supervisor. Receives notice of Trauma incidents via EAS Trauma Group (generic email account). Interested in being able to easily generate different types of management reports and do analysis of different factors. Will want to ensure that the system can handle different types of scenarios and that CRC counsellors have the required information easily available for clients who may already be feeling distressed. Needs to be able to see client files as needed. User of all aspects of the system.	Oversees the management and delivery of counselling services.	1
CRC Supervisor	Supervises the CRC and its operations 24/7; ensuring that the service is offered according to established guidelines, meets quality standards and incorporates clinical supervision. Heavy user of the service delivery/operational components of the system. Interested in having a solution for the CRC Counsellors that is easy to use, provides some built in flows/intelligence yet allows counsellors to easily incorporate special information that may not be included as choices/options in drop down menus yet. Ensures that quality data/information is being	Oversees the operations of the CRC to ensure it meets the set criteria.	1

Stakeholder Type	Description	Responsibilities	Approx. # of Stakeholders
	entered in the system for follow-up, management & tracking purposes.		
CRC Counsellor	First point of contact for an Employee Assistance Program (EAP) Client who may need EAP counselling or other psychosocial services. Key users of the system. Collects information to assess whether counselling or other psychosocial services are needed and responds accordingly. If counselling/psycho-social services are needed, initiate a case and refer the Client to a Service Provider. Some counsellors operate remotely and at times disconnected from the Internet.	Responds to calls from clients takes appropriate next steps and completes relevant documentation for management purposes.	12
CRC Admin Assistant	Key users of the admin functions of the system. Provides EAP Case information to contracted Service Providers, updates Service Provider availability, addresses other relevant informational needs. Enters all Service Providers' extension requests (including their plans) in the system and provides statistical data to support Case Managers. Performs auditing functions to ensure data integrity. Interested in being able to easily update, find and extract required data.	Provides administrative support to the CRC Counsellor and Case Management team.	3
Crisis and Referral Center (CRC) Logistics Coordinator	Coordinates CRC Counsellor activities. Coordinates and conducts training. Replaces CRC Supervisor when needed. Interested in having a system that is easy to navigate, to train others on, has proper documentation, able to generate management reports.	Coordinating counsellor activities, conducting training sessions and replacing the CRC Supervisor if and when needed.	1
Manager of Counselling Services and Quality	Manager of the Case Management team; CRC Supervisor; and QA Supervisor. Receives notice of	Oversees the management and delivery of counselling services.	1

Stakeholder Type	Description	Responsibilities	Approx. # of Stakeholders
Assurance (QA)	Trauma incidents via EAS Trauma Group (generic email account). Interested in being able to easily generate different types of management reports and do analysis of different factors. Will want to ensure that the system can handle different types of scenarios and that CRC counsellors have the required information easily available for clients who may already be feeling distressed. Needs to be able to see client files as needed. User of all aspects of the system.		
CRC Supervisor	Supervises the CRC and its operations 24/7; ensuring that the service is offered according to established guidelines, meets quality standards and incorporates clinical supervision. Heavy user of the service delivery/operational components of the system. Interested in having a solution for the CRC Counsellors that is easy to use, provides some built in flows/intelligence yet allows counsellors to easily incorporate special information that may not be included as choices/options in drop down menus yet. Ensures that quality data/information is being entered in the system for follow-up, management & tracking purposes.	Oversees the operations of the CRC to ensure it meets the set criteria.	1
CRC Counsellor	First point of contact for an Employee Assistance Program (EAP) Client who may need EAP counselling or other psychosocial services. Key users of the system. Collects information to assess whether counselling or other psychosocial services are needed and responds accordingly. If counselling/psycho-social services are needed, initiate a case and refer the Client to a Service Provider.	Responds to calls from clients takes appropriate next steps and completes relevant documentation for management purposes.	12

Stakeholder Type	Description	Responsibilities	Approx. # of Stakeholders
	Some counsellors operate remotely and at times disconnected from the Internet.		
CRC Admin Assistant	Key users of the admin functions of the system. Provides EAP Case information to contracted Service Providers, updates Service Provider availability, addresses other relevant informational needs. Enters all Service Providers' extension requests (including their plans) in the system and provides statistical data to support Case Managers. Performs auditing functions to ensure data integrity. Interested in being able to easily update, find and extract required data.	Provides administrative support to the CRC Counsellor and Case Management team.	3
Case Management (CM)			
Case Management Specialist (CMS)	Grants or denies extensions to Service Providers for additional sessions based upon their request. Coordinates with Service Providers to identify appropriate strategies to follow for proper case management. Supports the business office as it relates to Service Provider payments.	Reviewing requests for case extensions and approving or denying requests based on information provided. Supporting the Business Office by providing supporting documentation for payment purposes.	6
Case Management Administrative Assistant (CMAA)	Performs preliminary verification of extension requests received from Service Providers. Approves standard extension requests and forwards more complicated cases to the Case Management Clerk. Performs data entry for standard extension requests.	Administers requests for counselling extensions and counselling activities.	1
Case Management Clerk (CMC)	Person who distributes extension requests to CMS.	Ensures proper distribution of extension requests and follow-up on	1

Stakeholder Type	Description	Responsibilities	Approx. # of Stakeholders
		outstanding requests.	
Quality Assurance (QA)			
EAP Quality Assurance Supervisor (EQAS)	Interacts with clients, Service Providers and EAP stakeholders. Investigates complaints from clients. Analyzes the results of surveys and periodic reviews. Coordinates and provides bi-weekly orientation sessions to new network counsellors. Provides individual detailed report for each complaint received and enters data in the EAS system. Provides upper management with monthly report on all complaints received for the particular month. Checks "non-compliance" occurrences to ensure they do not become repetitive patterns. Has access to customer Organization's complaints cases (closed and open), quality assurance notes, case management notes, and detailed information about Service Providers.	Reviewing survey results and taking appropriate next steps with the relevant stakeholder to ensure that EAP clients are satisfied with the services received.	1
EAP Quality Assurance Admin Assistant – EQAAA	Administers Quality Assurance processes. Creates an annual report that includes amongst other things "No-Shows", "See Once", number of surveys returned, number of new files created, average delays for first appointment. Enters Voluntary Survey comments. Administers distribution of the Voluntary Survey.	Supports the QA Supervisor by producing appropriate reports and documentation.	1
National Business and Customer Relations			
National Manager Business and Customer Relations	Supervises the activities of the EAP Account Managers. Extracts management reports and documents Organizational Account interactions in detail.	Promotes EAS' services, business development and customer relations.	1
EAS Account Managers (AM)	Liaises with Organizational Accounts to ensure good relations and customer satisfaction, negotiates new contracts and renewals, and	Works with Organizational Accounts representative to	4

Stakeholder Type	Description	Responsibilities	Approx. # of Stakeholders
	promotes all of EAS's service lines on an ongoing basis. Reviews utilization rates, conducts analysis and discusses usage results with Organizational Accounts.	address their Employee Assistance needs including access to an EAP service.	
Regional EAS Account Managers	Same description as EAS Account Managers however working remotely (i.e. working in the regions, not physically located in the National Capital Region).	Works with regional Organizational Accounts representative to address their Employee Assistance needs including access to an EAP service.	2
EAS Admin Assistants to Account Managers (AMAA)	Provides administrative assistance to EAS Account Managers. Carries out day-to-day operational duties related to the work of the EAS Account Managers such as; preparing invoices for distribution, creating letter templates, maintaining reporting templates, monitoring the website and information requests generated through it. Updates various lists. Heavy user.	Supports EAS Account managers by preparing relevant documentation and reports.	2
Business Office (BO)			
Business Office Supervisor	Supervises all aspects of the business office. Coordinates budget planning and reporting, invoicing to Organizational Accounts and SOS customers, payment to EAP and SOS Service Providers. Manages accounts receivable, accounts payable, purchasing, variance reports, financial data entry, contract creation, etc.	Oversees and manages all aspects of the Business Office.	1
Business Office Admin Assistant (BOAA)	Enters information received from Service Providers that send in monthly invoices and statistics, creates call-ups for EAP and SOS services and maintains tracking sheets, and other administrative functions.	Supports the Business Office Supervisor in preparing relevant reports and documentation.	1
Counselling Network	. Negotiates and captures terms of Service Provider's Standing Offer	Screens, hires and manages Service	2

Stakeholder Type	Description	Responsibilities	Approx. # of Stakeholders
Coordinator (CNC)	Agreements (SOA). Manages Service Provider profile information and documents (security screening, proof of education, proof of liability insurance, professional registration, etc.).	Providers in the EAP network.	
Counselling Network Coordinator Admin Assistant (CNCAA)	Creates and modifies SOA for new and existing Service Providers. Creates and maintains Service Provider profiles. Creates call-ups for SOS projects.	Supports the Counselling Network Coordinators by preparing relevant reports and documentation.	1
Data Entry Clerk (DEC)	Verifies data contained within invoices and associated statistical reports received from Service Providers. Follows up with Service Providers when statistical report data is not received.	Verifies and enters data from invoices and other documentation.	7
Client Support Officer (CSO)	Supports the Service Provider accessing the EAS External Portal. Updates the online tutorial as needed. Sends out communications to Service Providers via e-mail.	Supports the Service Providers from an EAS perspective.	1
Management			
Director, Employee Assistance Services	The Director is responsible for all aspects of the EAS Division. Requires access to all data and management reporting.	Managing the EAS division including the operation of the EAP.	1

3 PRELIMINARY TARGET EAPIMS REQUIREMENTS

3.1 Overview

The preliminary **target** EAPIMS deployment model is illustrated in Figure 3.1-1.

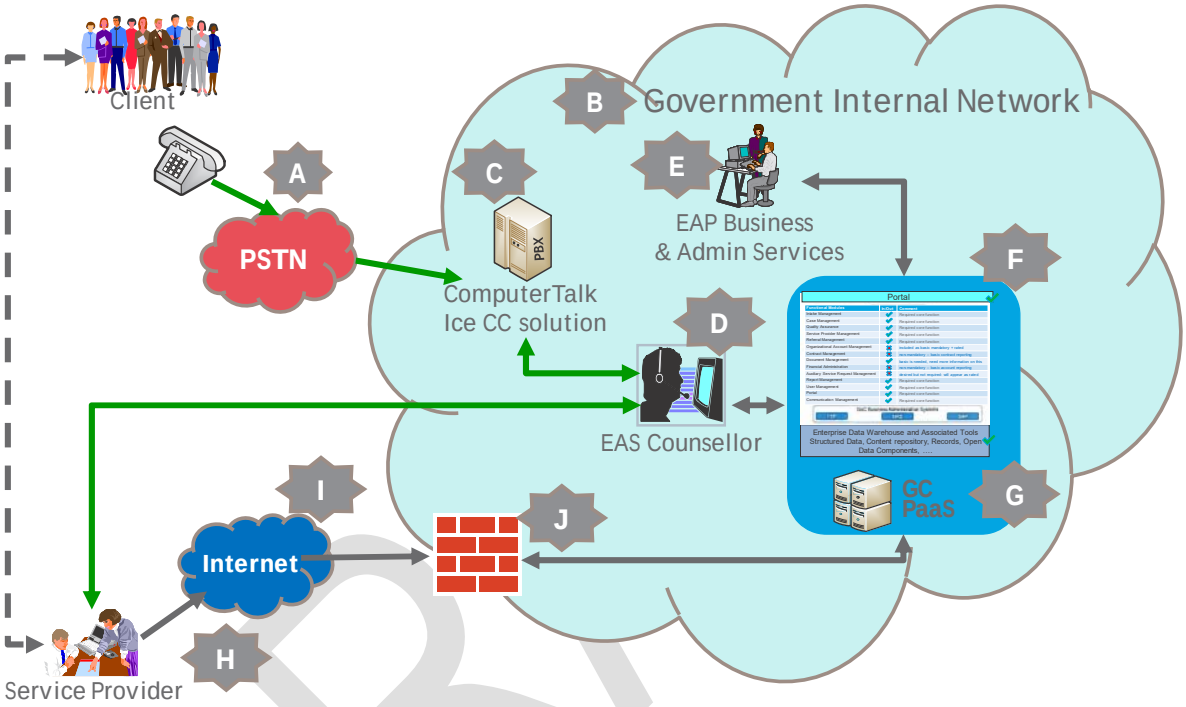

Figure 3.1-1: HC EAPIMS Strawman Target Deployment Model

In this Figure 3.1-1:

A	PSTN	EAS Clients access EAS service through the public switched telephone system and through a web-chat function. For voice, access is through a published set of 1 800 numbers. These numbers terminate in the government provided call centre call management system – currently the ComputerTalk iceEPASS solution configured to meet the specific call flow requirements of the program. The ComputerTalk iceEPASS solution is not integrated with business systems (e.g. to with the CRM platform). In the target model, this independent operation will continue – i.e. there is no requirement for integration between iceEPASS and the EAPIMS.
B		Government of Canada enterprise voice and data network infrastructures used by all internal (to the government) stakeholders and providing secure access to EAS

		applications and data hosted on Government-provided platforms. The government enterprise network provides the security, redundancy, performance, capacity, access and accessibility required to support internal stakeholders.
C	 ComputerTalk Ice CC solution	ComputerTalk iceEPASS contact centre call management solution configured to meet the specific call flow requirements of the program. The iceEPASS platform handles incoming call queues and has no direct integration with backend systems (i.e. there are no screen-pops or other automated call handling functions required).
D	 EAS Counsellor	A HC EAS Counsellor providing the first point of contact for clients requiring access to EAS services. EAS counsellors are equipped with desktop voice and computing devices conformant to HC and GC standards for these devices. All EAS Counsellors are internal to the GC infrastructure. Off-site Counsellors have a GC equipment/devices to allow access to the government network.
E	 EAP Business & Admin Services	EAS Business and administrative users provide quality assurance, case management and administrative services in support of the overall administration of the EAS programs and services. EAS Business and administrative users are equipped with desktop computing devices conformant to HC and GC standards for these devices. All EAS Business and administrative users are internal to the GC infrastructure.
F		The portfolio of EAS business systems required to meet the business needs of the program as set out in this SOR. The portfolio of systems shall be provided in multiple deployment environments on GC provided operating platforms where these deployment environments are as set out in this SOR and include but are not limited to production, staging, “sandbox”/development/test and DR environments.
G		The GC provided platform services configured to provide the performance, capacity, security and related non-functional requirements of the EAPIMS as required to provide and deliver the operational service level objectives. The GC provided platform services will be provided in support of the required deployment environments as set out in this SOR and including but not limited to production, staging, “sandbox”/development/test and Disaster Recovery (DR) environments. The GC provided platform services will conform to the GC Treasury Board (TB) guidelines for platform services in support of Protected B workloads. GC provided platform services will be configured to provide an appropriate level of high-availability and enable the DR

		function to comply with Recovery Point Objective (RPO) and Recovery Time Objective (RTO) as set out in this SOR.
H	 Service Provider	The Service Provider is an external (to the GC) independent provider of Employee Assistance (EA) services. A Service Provider is referred to the Client by the EAS Counsellor. Where appropriate for the care required, a direct interaction occurs between the Client and Service Provider for delivery of the services. All EA services related records and case files are held by the Service Provider. Interaction between the Service Provider and the GC EAS environment are for the purposes of program management and administration.
I		Electronic access to the GC EAS program management and administration regime by external stakeholders, including but not limited to Service Providers, is provided through secure internet access. Does not exist today – part of the "target deployment".
J		Electronic access to the GC EAS program management and administration regime by external stakeholders, including but not limited to Service Providers, is provided through secure internet access controlled by appropriately configured secure firewall services. Does not exist today – part of the target deployment.

3.2 EAPIMS Business Functional Requirements

The integrated EAPIMS must provide and deliver the business functionality to meet the needs of Canada as set out in this SOR. Specifically:

1. The integrated EAPIMS must address the requirements for:
    a. Intake Management as set out in Section 3.2.1;
    b. Case Management as set out in Section 3.2.2;
    c. Quality Assurance as set out in Section 3.2.3;
    d. Service Provider Management as set out in Section 3.2.4;
    e. Referral Management as set out in Section 3.2.5;
    f. Organizational Account Management as set out in Section 3.2.6;
    g. Financial Administration as set out in Section 3.2.9;
    h. Report Management as set out in Section 3.2.11;
    i. User Management as set out in Section 3.2.12;
    j. Portal services as set out in Section 3.2.13;
    k. Communication Management as set out in Section 3.2.14.

3.2.1 Intake Management

Intake Management is the ability to capture, track and manage client's information in order to provide the appropriate service. The process may require immediate counselling, referral to a Service Provider (SP), conducting a needs assessment, and/or referring to a different internal service line.

- Track and manage incoming client calls.
- Associate a call to a Client record, a new or existing case, and any activities relating to the case, such as referrals, delivery of information, or referrals to different service lines.
- Validate client's eligibility for service by accessing related contracts/agreements.
- Assess client using onscreen reference document(s)
- Refer client to Service Provider (see Referral Management).

3.2.2 Case Management

Case management is the collaborative process of assessment, planning and care coordination to meet a client's needs.

- Search clients, case histories, related cases, related payments and all associated notes.
- Manage existing case files, details and case strategies.
- Record decisions and any case related communication with a Service Provider.

3.2.3 Quality Assurance

The role of Quality Assurance is to identify, document, capture and track non-compliance with EAS policies, and client input. It also consists of managing complaints, confidentially capturing and handling complaints in a timely manner, acknowledging the receipt of a complaint and documenting its resolution.

- Service Provider site visits and follow-ups.
- Manage survey templates.
- Capture of survey data.
- Capture non-compliance and client input.
- Complaint can originate from any source – client, service provider, account contact, etc.
- Review, investigate and document.
- Limited user access to complaints.

3.2.4 Service Provider Management

Service Provider (SP) Management oversees the maintenance and upkeep of SP certifications, streamlining hiring efforts and allows for network research and analysis.

- Create and manage Service Provider profile.
- Determine the health of the SP network per service line.
- Access to all relevant Standing Offer Agreements (SOA) – per service lines.

- Create and manage SOA contracts (see Contract Management)
- Geocode office locations(s).
- Manage SP documents (refer to Document Management).

3.2.5 Referral Management

The management of referrals comprises the finding and connecting of the appropriate SP resources to the client or organization as well as the tracking and management of communications leading up to the acceptance/declining of the referral.

- View referrals for which provider has not called back to pick up referral details.
- Capture SP decision relating to the acceptance of the referral.
- Track delays in picking up referral detail and follow-up with Service Provider(s).
- Geolocation search.

3.2.6 Organizational Account Management

Organizational Account Management consists of the continuous evaluation of the Account's requirements and the updating of the Account profile to reflect changes over time. The goal of account management is to promote psycho-social services through direct communication or events, to increase the number of covered individuals and to ensure timely and responsive communications with organizational clients (accounts and prospective accounts).

- Create / update organisations and organizational accounts.
- Manage and generate account related contracts in system.
- Track account related communications.
- Capture orders for promotional items.

3.2.7 Contract Management

Contract management is the process of defining contractual agreements, managing the state of the contract, managing the changes to the contract and generating the contract document.

- Need to support different types of contracts.
- Creation of contracts and amendments. History of contractual agreements is required.
- Manage current dates, amendment to dates, expiration dates and/or other relevant date changes.
- The contract amendment document should outline the changes between the current contract and the previous contract.
- Manage contract statuses.
- Save generated document to document repository.
- Ability to generate contracts in the recipient's language of preference (French and/or English).
- Ability to manage contract templates.
- Create Call-ups request (actual creating of Call-up is done in SAP – see Financial Administration).

3.2.8 Document Management

Document Management is the process of organizing, storing and tracking electronic documents in a central document repository.

- Search document related metadata (such as type of security, expiration dates, document classification, etc.).
- Manage expired documents.
- Document Encryption is required conforming to Communication Security Establishment (CSE) recommended cryptographic algorithm.

3.2.9 Financial Administration

Financial Administration consists of the payment of the amounts owed and the charging of amounts due.

- Validate SP invoice line items against original referral and case management decision (when applicable).
- Creation of new Call-ups and tracking and maintaining of existing call-ups.
- Link each SP invoiced service item(s) to the appropriate call-up(s) associated to the SOA contract(s) that are active on the date(s) of service.
- Track which call-ups were used to pay specific invoices.
- Allow and track adjustments to the original SP invoices.
- Create SP invoice with adjustment notices.
- Track contract value(s) to be charged back to the organisation account/customer.
- Calculate charges.
    - Calculation of the amount to charge the organisation account/customer based on charge interval (defined on the contract or project) and versus amount(s) already charged.
    - For services that are charged per use, the ability to calculate the amount to charge the account/customer based on delivered services.

3.2.10 Service Request Management

Service Request management consists of planning, scheduling, cost control and budget management. It allows the users to manage the delivery of service. It also aids in the tracking of communication and quality assurance activities.

- Assessment and capture of potential customer needs.
- Search mechanism to aid user in determining estimate of service costs.
- Define service delivery details for each service required, location, and date.
- Support the ability to capture and view a multitude of calculated costs for the delivery of a service.
- Define a series of services that fit the customer’s goal and budget.
- Create proposals/quotes with cost estimates for potential customers.
- Create Service Agreement, Interdepartmental Letter of Agreement (ILA), Memorandum of Understanding (MOU) and contracts (see Contract Management).
- Manage date and time specific actions.
- Identify and resolve conflicts between bookings.

3.2.11 Report Management

Report management allows for data research and analysis. It allows pre-defining report parameters, running a collection of standard reports, and producing a high volume of reports with the ability to save the outputs to a document repository, keeping track of the document classification. Reporting should ensure that sensitive data or data that could link to a single individual or cause prejudice to a group remains anonymous or unidentifiable.

- Users can configure reports parameters.
- System needs to track report configurations per organizational account.
- Solution needs to support “power user” to create and edit reports.
- Client related reports needs to be captured in a document repository.
- Ability to manage report templates.
- Output reports in PDF, DOCX and Excel format.
- Batch reporting.
- Generation of complex reports (data originating from multiple data sources– internal and/or external).

3.2.12 User Management

User Management allows creating and managing login credentials for each user as well as allowing individual users to manage their system preferences.

- Each user should be able to edit their user profile and user preferences.
- Aspects of the user profile that relate to access privileges should only be modifiable by a user with appropriate privileges (such as a Power User or System Administrator).

3.2.13 Portal

The purpose of the portal is to provide SP with the ability to create a new profile and submit documentation to keep the profile up-to-date (e.g. updated professional association certificate, liability insurance certificate, etc.) The Portal will also facilitate the communication of referral information to SPs as well as to allow SPs to manage case activities (extension requests) and submit their invoices and statistical forms.

The portal must also support online surveys (note that the survey participants must be anonymous).

3.2.14 Communication Management

Communication management is exclusively defined as the management of communication campaigns.

- Communicate with clients, organizations, etc. for distribution of policy updates, newsletters, request for information, etc. via different communication methods.
- Bring forward system.
- Track responses.

A modernised information system will support EAS in providing first rate service to clients and contribute to the highest standards in client confidentiality. The modernised tool will increase the speed of searches for counsellors to support employees in immediate need, collect additional data to make informed business decisions, and allow EAS employees to be more effective with their time.

3.3 Implementation Services Requirements

The Contractor must provide and deliver the implementation and transition-in services associated with the proposed EAPIMS as required for solution design, configuration, installation, deployment, integration, testing, training and otherwise making ready for use in live production. Required services include but are not limited to:

1. Services for provision of planning and design deliverables for the transition through operations phases of the project.
2. Services to set up the technical infrastructure and initial installation of the core COTS software products required to support the configuration, customization, integration and other efforts as required to implement the initial wave of EAP services.
3. Services as required for the configuration, customization, integration and other efforts as required to implement the initial wave of EAP services and obtain the required authority to operate the EAPIMS in live production.
4. Services required for the onboarding of Stakeholders and migration of operational data from the current EAP environment to the EAPIMS as deployed.

The Contractor must provide and deliver the services associated with the proposed EAPIMS as required for the ongoing day-to-day operation, maintenance and support of the EAPIMS as deployed.

The Contractor may be requested to provide on an as and when requested basis services in support of new EAS initiatives where such services may include but are not limited to EAP project planning, project design, project onboarding, operational services, and infrastructure and integration services.

The Contractor may also be requested to provide, on an as and when requested basis, services related to the provision of ad-hoc EAP services where such services may include but are not limited to enhanced service analytics, support for new or additional contact modalities (e.g. in support of emerging remote and mobile device access), ad-hoc reporting, or other EAS-related service delivery, planning, management or administration services.

Services are required to be provided through a series of tasks authorized by Canada through a structured Task Authorization (TA) process.

3.4 Web Accessibility and Usability Requirements

The Contractor must provide, deliver, enable and support the web accessibility and usability requirements as set out in the following Standards and guidelines.

1) Standard on Web Accessibility: http://tbs-sct.gc.ca/pol/doc-eng.aspx?id=23601 and Web Content Accessibility Guidelines (WCAG) 2.0: http://www.w3.org/TR/WCAG20/
2) Standard on Web Usability: http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?section=text&id=24227
3) Web Experience Toolkit Guideline: http://www.tbs-sct.gc.ca/ws-nw/wa-aw/wet-boew/index-eng.asp
4) Official Languages Act: http://laws.justice.gc.ca/eng/acts/O-3.01/index.html

4. MASTER PROJECT SCHEDULE

The Master Project Schedule identifies the major milestones for business outcomes, deliverables and target dates associated with the transition of the current EAS Solution to the EAPIMS provided by the Contractor and based on a preliminary implementation project plan provided in response to the bid solicitation.

The Master Project Schedule is used to coordinate Contractor-provided deliverables and outcomes with the various government-provided systems and services on which these Contractor materials are dependent (e.g. provision of GC infrastructure and associated access technologies and logistics).

The Master Project Schedule combines various transition activities (e.g. planning, implementation, testing) with the HC's approvals and acceptance processes and the logistics associated with migrating existing employee assistance programs and services to the new EAPIMS.

The Master Project Schedule assumes a start date for the project start-up and planning of no later than October 2020 with a target "go live" date for the transitioned coverage in June 2021.

Table 4.1-1: Master Project Schedule Summary

Major Milestone	Title	Time-frame (M)onths	Outcomes, Deliverables and Key Activities summary
MM-1-CON-0000	Start – project start-up, Planning and Design start	Oct 2020	Project Start (project start-up, Planning and Design Phase based on defined planning deliverables - TA#1)
MM-1-CON-0100	Phase 1 - Detailed Planning and Design Phase Complete	Start + 1M	Detailed planning and design deliverables based on revisions to materials performed by the Contractor during the term of the project start-up and planning Phase 1.
MM-2-CON-0300	Phase 2 implementation and	Start + 5M	Phase 2 installation of EAPIMS on GC provided platforms, configured for Wave 1 EAS business processes and integrated with required GC systems

Major Milestone	Title	Time-frame (M)onths	Outcomes, Deliverables and Key Activities summary
	initial deployment complete		and services and obtaining required approvals to operate (ATO).
MM-3-CON-0500	Phase 3 User Acceptance Testing (UAT) complete Phase 4 Cutover start	Start + 6M	Phase 3 Wave 1 EAS handover to HC for final Phase 4 acceptance testing before cutover to live production.
MM-4-CON-0100	Phase 4 Cutover complete	Start + 9M (June 2021)	Phase 4 cutover and go live of Wave 1 EAS project based on acceptance by Canada (including security, performance and related factors)
MM-5-CON-	Phase 5 Stabilization Period Start	Start + 9M	Monitoring of solution in production to identify and prioritize areas that require change to provide require Wave 1 services at specified service levels. These may include but are not limited to changes to Contractor services, GC provided infrastructure and services.
MM-5-CON-	Phase 5 Stabilization Period Ends	Start + 21M	Finalization of services, service levels and enabling resourcing and infrastructure as required to provide stable EAS services consistent with current services and service levels. Assessment and restructuring of staffing models to improve value for money for Canada.

APPENDIX A TO ANNEX B – GC PROVIDED INFRASTRUCTURE SERVICES

This attachment sets out the scope of IT infrastructure services that can be provided by Canada for the deployment of the EAPIMS. These will reflect SSC hosting services and SSC sanctioned and/or brokered cloud infrastructure services providers that may be available and that meet security requirements for a cloud-hosted solution.

The intent is to ensure appropriate protection of Government of Canada data for solutions hosted in cloud environment.

1. SSC ENTERPRISE DATA CENTRE SERVICE STANDARDS

Availability:

- 24 x 7 x 365, 99.982% of the time

Service Hours:

- 24 x 7 x 365 – On Site

Regular scheduled maintenance:

- The Enterprise Data Centres are designed such that there are no planned maintenance activities that require a complete outage of the Enterprise Data Centres (Barrie, Borden and Gatineau)

External vendor support hours:

- 24 x 7 x 365 – On Site

Mean time to restore:

- 1 hour, 90% of the time

Request fulfillment duration:

Service Offering	Time to Fulfill	Percent of the Time
Facility Planning Consultation	• Acknowledgement will be according to SSC Enterprise Business Intake published process times. • Capacity planning - 15 days once necessary information is provided	80%

Service Offering	Time to Fulfill	Percent of the Time
Data Centre Facility Access	• Planned visit is up to 5 days • Incident response is 1 hour **Exception:** Not all regional data centre facilities have local DCFMS nearby, therefore, other arrangements will be made.	90%
Remote hands (On-site IT Device Support within the Facility)	Planned visit is up to 5 days Incident response is 1 hour **Exception:** Not all regional data centre facilities have local DCFMS nearby, therefore, other arrangements will be made.	90%
IT Hardware Installation (Planning and Installation)	Participation in planning meetings with 5 days advance notice • Install IT devices - 5 to 10 days depending on complexity and volume • Device cabling - 5 to 10 days depending on complexity and volume • Backbone cabling – procurement required, up to 60 days for delivery and installation • Shipping/Receiving - Minimum 2 business day notice and must be scheduled during posted loading dock hours **Exception**: Not all regional data centre facilities have local DCFMS nearby, therefore, other arrangements will be made.	80%

Service Offering	Time to Fulfill	Percent of the Time
IT Hardware Decommission (Planning and Installation)	• Participation in planning meetings with 5 days advance notice • Remove IT devices - maximum 30 days from request **Exception**: Not all regional data centre facilities have local DCFMS nearby, therefore, other arrangements will be made.	90%

Support

Post initial install - ongoing support

SSC Facilities provides 24 x 7 x 365 facility support (where available, see Service Hours) that is dispatched through SSC Enterprise Service Desk (typically as part of a response to an Incident).

Service Offering	Time to Fulfill	Percent of the Time
Facility Planning Consultation	• Acknowledgement will be according to SSC Enterprise Business Intake published process times. • Capacity planning - 15 days once necessary information is provided	80%
Data Centre Facility Access	• Planned visit is up to 5 days • Incident response is 1 hour **Exception:** Not all regional data centre facilities have local DCFMS nearby, therefore, other arrangements will be made.	90%
Remote hands (On-site IT Device Support within the Facility)	Planned visit is up to 5 days Incident response is 1 hour **Exception:** Not all regional data centre facilities have local DCFMS nearby, therefore, other arrangements will be made.	90%

Service Offering	Time to Fulfill	Percent of the Time
IT Hardware Installation (Planning and Installation)	Participation in planning meetings with 5 days advance notice • Install IT devices - 5 to 10 days depending on complexity and volume • Device cabling - 5 to 10 days depending on complexity and volume • Backbone cabling – procurement required, up to 60 days for delivery and installation • Shipping/Receiving - Minimum 2 business day notice and must be scheduled during posted loading dock hours **Exception**: Not all regional data centre facilities have local DCFMS nearby, therefore, other arrangements will be made.	80%
IT Hardware Decommission (Planning and Installation)	• Participation in planning meetings with 5 days advance notice • Remove IT devices - maximum 30 days from request **Exception**: Not all regional data centre facilities have local DCFMS nearby, therefore, other arrangements will be made.	90%

Terms and conditions

- New IT workloads should be installed in the public cloud and subsequently the Enterprise Data Centre facilities as the next priority consideration.
- Migration of workloads to enterprise Data Centre facilities is the preferred option to manage growth and obsolescence. IT growth in legacy Data Centre facilities may be supported if this is the only technical option available AND customer funding is available AND the request aligns with Program Integrity guidelines AND there is existing facility capacity to support the request.

- In the case of lease renewals, the lease renewal term must be arranged for a 1 year period and reviewed on a year by year basis.

2. DATABASE SERVICE STANDARDS

- DB Service is Aligned with SSC Enterprise Data Centre Service Standards

Service Standards	**Target**
Availability	99.5% target (does not include regular scheduled maintenance)
Service Hours	24 x 7 x 365
Regular scheduled maintenance	Monthly scheduled maintenance window (4 hours), aligned with the SSC Enterprise Data Centre scheduled maintenance window
External vendor support hours	24 x 7 x 365
Mean time to restore	4 hours, assuming underlying infrastructure is available and accessible

<table>
<tr><th>Service Standards</th><th>Target</th></tr>
<tr><td>Request fulfillment duration</td><td>Variable based on the level of complexity, quantity, resources and other factors applicable to each individual request, but assuming underlying resources are in place and accessible, here are timeframes for typical simple Requests:

<table>
<tr><th>Service Request</th><th>Fulfillment Duration</th></tr>
<tr><td>Install and Configure a DB instance</td><td>1 business day</td></tr>
<tr><td>Modify existing DB Configuration parameters</td><td>1 business day</td></tr>
<tr><td>Modify existing DB hardware resource parameters (e.g. increase SAN or vCPU)</td><td>1 business day</td></tr>
</table>
</td></tr>
</table>

3. MIDDLEWARE SERVICE STANDARDS

Availability: 24 x 7 x 365, 95% of the time

- **Service hours:** 24 x 7 x 365, hours to be negotiated per environment through an official Service Level Agreement
  - **Standard availability:** 95%, excluding patch work and scheduled maintenance
- **Regular scheduled maintenance:** Mandatory monthly maintenance window is required and negotiated per environment as per Service Level Agreement
- **External vendor support hours:** not applicable**,** SSC provides the partners with support and contacts the vendors when required

Mean time to restore service:

- depends on system complexity and Service Level Agreements

Request fulfillment duration:

- variable based on the level of complexity, quantity, timing, resources and other factors applicable to each requests

ANNEX C

EVALUATION AND QUALIFICATION CRITERIA

1.0 Instructions to Respondents

1.1 Respondents should submit their Responses in accordance with the requirements set out in this Annex.

1.2 In its Response, the Respondent should demonstrate its understanding of the requirements contained in the ITQ and explain how it will meet these requirements. The Respondent should demonstrate its experience and describe its approach for carrying out the Project in a thorough, concise and clear manner.

1.3 The Response should address clearly and in sufficient depth the points that are subject to the Mandatory and Rated Criteria against which the Response will be evaluated. Simply repeating the statement contained in the ITQ is not sufficient.

1.4 If the quantity of reference projects in the Response exceeds the limit stipulated by the submission requirements, projects will be evaluated in the order they are supplied and any extraneous examples will not be evaluated.

1.5 Projects may be referenced in response to more than one submission requirement. However, Respondents should complete one (1) project experience form for each reference to a project (even if the project is referred to more than once) and not cross-reference projects referred to in responses to other sections. For example, if a project is referenced in a Respondent's response to Section C-1 and the Respondent intends to use the same project in its response to Section C-2, the Respondent must complete a separate project experience form for each of Section C-1 and Section C-2.

2.0 ITQ Evaluation Summary and Methodology

2.1 The ITQ will employ a two-step evaluation process: a) a set of general mandatory criteria (11 items) that establish foundational Vendor requirements for this activity, and b) a set of rated measures (Rated Evaluation Criteria) which are derived from the mandatory criteria. The purpose of the mandatory criteria is to ensure that a potential Vendor is suited to address the overall requirement of providing a supported, Commercial Off The Shelf (COTS), EAPIMS system. Following from there, the rated measures are used to enable an objective ranking of organizations that meet all mandatory requirements so as to establish a list of eight organizations which are objectively best positioned to meet Health Canada’s core needs.

2.2 The Mandatory Criteria will be evaluated on a pass/fail basis (i.e. responsive / non-responsive) as indicated in Section 3.1 – Mandatory Technical Criteria. To be responsive, Respondents must clearly detail how they meet the criteria identified in the mandatory requirement. Simply stating that the Respondent complies with the requirement is not sufficient. The Response will fail to meet an Eligible Mandatory Criterion where Canada determines that the information provided is insufficient in detailing how the

Respondent meets a mandatory requirement(s).

2.3 Responses to the Rated Evaluation Criteria will be evaluated in accordance with the applicable weight found in Appendix B - Applicable Weights for Rated Evaluation Criteria.

2.4 Responses will be evaluated in accordance with the criteria and weight factors indicated in 3.2 Rated Technical Criteria and Appendix A to Annex C. These criteria are not evaluated on a pass/fail basis.

2.5 Each reference project provided in relation to the experience assessed in criteria R-x, R-y, will be rated individually against the Rated Evaluation Criteria. The individual scores will then be averaged to arrive at an aggregate score and the applicable weighting will then be applied.

2.6 Once the evaluation has been completed for all Vendor submissions, the eight highest scoring Vendors will be invited to participate in the subsequent procurement.

3.0 Technical Evaluation

3.1 Mandatory Technical Criteria

The Mandatory Criteria listed below will be evaluated on a met/not met (i.e. responsive/non-responsive or compliant/non-compliant) basis.

Where a mandatory criteria requests a Respondent to **'demonstrate':** to be responsive, the technical response must substantiate how the Respondent meets the criteria identified in the mandatory requirement. The substantiation must not simply be a repetition of the requirement(s), but must provide sufficient detail to demonstrate how they will meet the requirements. Simply stating that the Response complies with the requirement is not sufficient. The response will fail to meet a mandatory criterion where Canada determines that the substantiation is insufficient in detailing how the Respondent demonstrates a mandatory requirement(s).

#	Mandatory Criteria	Met (Yes/No)	Page Number(s) in Response
M-1	**Proposed EAPIMS** The Respondent must identify the proposed core EAPIMS that would form the foundation for an HC EAS solution. Specifically, the Respondent must clearly identify the overall structure of the proposed EAPIMS including: 1. Products, modules, components or other licensed software proposed to meet the functional requirements of the EAPIMS as set out in Annex B - Statement of Requirements.		

#	Mandatory Criteria	Met (Yes/No)	Page Number(s) in Response
	2. Dependencies on any underlying commercial software including but not limited to any database, operating system, security or access management dependencies.		
	Response		
M-2	**Proposed EAPIMS** For **each** of the products, modules, components or other licensed software proposed to meet the functional requirements of the EAPIMS as set out in Annex B – Statement of Requirements, the Respondent must identify: 1. The commercial name under which the proposed EAPIMS is sold. 2. The version or release of the proposed EAPIMS. 3. The month and year in which the initial version of the proposed EAPIMS was released. 4. The entity that holds the intellectual property rights to the proposed EAPIMS. **Note:** Where the proposed EAPIMS consists of multiple products integrated to provide an integrated solution to meet this HC requirement then points 1 through 4 must be addressed for each such product.		
	Response		
M-3	**Proposed Solution – Commercial Availability** The proposed core EAPIMS must be commercially available. Respondents must demonstrate compliance by providing product materials demonstrating that the core EAPIMS is commercially available. For the purposes of this ITQ, “commercially available” means that the software or services as proposed is freely available for purchase, has a published product / service definition and pricing structure, and has an ongoing funded development and support investment behind it. In the case where the Solution consists of multiple, independent products, each product proposed must be “commercially available” as defined above. **ALPHA or BETA versions of a product or service do NOT qualify as commercially available.**		
	Response		

#	Mandatory Criteria	Met (Yes/No)	Page Number(s) in Response
M-4	**Respondent Structure** The Respondent must identify the proposed EAPIMS **project** structure by identifying: 1. The Respondent and any Affiliates employed in the provision of the proposed EAPIMS. 2. Any and all providers of core EAPIMS components required for the provision of the EAPIMS as proposed. 3. Any and all providers of professional services proposed by the Respondent to provide and deliver the proposed EAPIMS (e.g. subcontractors engaged by the Respondent for the purposes of solution configuration, integration, customization or support services).		
	Response		
M-5	**Respondent Structure** The Respondent must demonstrate that the Respondent is authorized to provide and deliver the proposed EAPIMS by providing the following: 1. If the Respondent is the Software Publisher for any of the proprietary software products proposed, Canada requires that the Respondent confirm in writing that it is the Software Publisher. Respondent are requested to use the Software Publisher Certification Form included with this ITQ. Although all the contents of the Software Publisher Certification Form are required, using the form itself to provide this information is not mandatory. For Respondents 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 Response being declared non-responsive. or 2. Any Respondent that is not the Software Publisher of all the proprietary software products proposed is required to submit proof of the Software Publisher's authorization, which must be signed by the Software Publisher (not the Respondent). No further consideration will be given to a Respondent who is not the Software Publisher of all of the proprietary software proposed, unless proof of this authorization has been provided to Canada. If the proprietary software proposed by the Respondent originates with multiple Software Publishers, authorization is required from each Software Publisher. Respondents are requested to use the Software Publisher Authorization Form included with this ITQ. Although all the contents of the Software Publisher Authorization Form are required, using the form itself to provide this information is not mandatory. For Respondents/Software Publishers who use an alternate form, it is in Canada's sole discretion to		

#	Mandatory Criteria	Met (Yes/No)	Page Number(s) in Response
	determine whether all the required information has been provided. Alterations to the statements in the form may result in the Response being declared non-responsive. **Notes:** 1. In this ITQ, "Software Publisher" means the owner of the copyright in any software products proposed in the Response, who has the right to license (and authorize others to license/sub-license) its software products. 2. Where the core software of the proposed EAPIMS consists of multiple products integrated to provide an integrated solution to meet this HC requirement then the Respondent must be authorized to provide each such product by providing the required attestations for each product.		
	Response		
M-6	**Proposed Solution – Security** The proposed core EAPIMS must be available to be deployed in a secure operating environment that meets the Government of Canada security requirements. Respondents must demonstrate compliance by attesting that the proposed core EAPIMS is: 1. Available to be deployed: a. on a secure operating platform provided by Canada (e.g. through an internally provided computing and storage platform service or through a GC sanctioned third party provider of secure platform services); OR, b. as an end-to-end, turnkey offering (also known as “Software as a Service”) on a GC sanctioned third party provider of secure platform services. 2. Available to be deployed in a GC-approved computing facility located within the geographic boundaries of Canada. Notes: • The list of GC sanctioned third party provider of secure platform services are available at this web link: https://cloud-broker.canada.ca/s/?language=en_CA		

#	Mandatory Criteria	Met (Yes/No)	Page Number(s) in Response
	• The GC Cloud Service Provider Information Technology Security Assessment Process (ITSM.50.100) is available at this web link: https://cyber.gc.ca/en/guidance/cloud-service-provider-information-technology-security-assessment-process-itsm50100.		
	Response		
M-7	**EAPIMS Deployment References** The Respondent must provide two (2) relevant sample projects by completing the Software Solution Deployment References form (Form C-1, provided in Appendix A to Annex C) for each sample project. Each provided Software Solution Deployment Reference must have been for the deployment of the proposed core EAPIMS or a previous version of the proposed core EAPIMS for an external customer. Each provided Software Solution Deployment Reference must have been in live production for a period of at least 12 months from initial deployment. **Note:** The provided Software Solution Deployment References will be rated as set out in Form C-1		
	Response		
M-8	**Respondent Structure – Roles and Responsibilities** The Respondent must identify the roles and responsibilities of each entity identified in response to M-4 above. The response must clearly identify: 1. The entity/entities with roles and responsibilities for the provision of Core EAPIMS components required for the provision of the EAPIMS as proposed – e.g. the entity that is the software publisher or license holder of the proposed software solution component. 2. The entity/entities responsible for the maintenance of any licensed software as the software publisher or license holder of the proposed software solution component. 3. The entity/entities responsible for the design, configuration, deployment and ongoing support of the proposed EAPIMS as deployed in live production to meet the needs of this EAPIMS.		
	Response		

#	Mandatory Criteria	Met (Yes/No)	Page Number(s) in Response
M-9	**EAPIMS Provider References** The Respondent must provide two (2) relevant sample projects by completing the EAPIMS Implementation Project Services References form (attached as Annex C-2) for each sample project. Each provided EAPIMS Implementation Project Services Reference must have been for the deployment of the proposed core EAPIMS or a previous version of the proposed core EAPIMS. Each provided EAPIMS Implementation Project Services Reference must have incorporated the provision of services by the Respondent organization and include services for the installation, configuration, integration, deployment, transition to live operation and ongoing support of the as-built EAPIMS. **Note:** The provided EAPIMS Implementation Project Services References will be rated as set out in Form C-2.		
	Response		
M-10	**Respondent Profile – Financial Viability** The Respondent must be financially viable to fulfill the requirement. By submitting a proposal in response to this ITQ, any Respondent will have consented to Canada performing its own financial viability assessment of the Respondent. To determine the Respondent's financial viability, Canada will, by written notice to the Respondent, require the submission of financial information as described in the main body of the ITQ Section 4.4: Financial Viability Assessment. Respondents must indicate in the Response below that they acknowledge and accept their consent to Canada performing its own financial viability assessment of the Respondent. Respondents that do not provide such consent or that are determined by Canada not to demonstrate sufficient financial viability will be removed from further consideration.		
	Response **Response – agree to provision**		

#	Mandatory Criteria	Met (Yes/No)	Page Number(s) in Response
M-11	**Proposed Solution - Bilingual Interface and Support** The solution must support both of Canada's official languages (French and English). Respondents should demonstrate compliance by providing samples of materials in French and English that illustrate product multi-language support. Examples of supporting materials include but are not limited to screenshots of user sessions in both official languages (e.g. screenshot of English session, screenshot of French session), user documentation, training or other product materials demonstrating product use in both languages. If the solution is not bilingual as described above, the respondent must provide a detailed roadmap indicating the delays required by the Respondent to produce and deliver a completely bilingual solution.		
	Response		

3.2 Rated Technical Criteria

Responses will be evaluated against the following point-rated technical criteria, using the evaluation factors and weighting indicators specified for each criterion. Responses not meeting the identified minimum weighted scores will be deemed non-responsive.

#	Rated Evaluation Criteria	Scoring Method
R-1	**Respondent Corporate Capability**	
R-1.1	**Understanding of EAS Project Requirements** The Respondent should demonstrate an understanding of the overall Health Canada EAS project requirements and deliverables as set out in Annex B – Statement of Requirements by describing concisely and in its own words: 1. The overall project objectives as set out in Annex B - Statement of Requirements. 2. The target EAPIMS environment as expected by Canada 3. The overall incremental implementation approach and project schedule. 4. The role of Canada in providing infrastructure and services in support of the target environment. 5. The scope of the required EAPIMS in support of the Wave 1 deployments projects. 6. The potential scope of services in response to changes in technology, policy and business requirements over the project lifecycle. 7. The requirements for minimizing risk in the migration and deployment approach adopted. 8. The security requirements associated with the project.	Points will be awarded in the following manner: **5 pts** = Response addresses 7 or more of points 1 through 8 **4 pts** = Response addresses 5 or 6 of points 1 through 8 **3 pts** = Response addresses 4 of points 1 through 8 **2 pts** = Response addresses 3 of points 1 through 8 **1 pt** = Response addresses 2 of points 1 through 8 **0 pts** = Response address less than 2 of points 1 through 8 **Note:** "Addresses a point" means that the Respondent has provided sufficient level of detail to demonstrate the point (e.g. recognition of the requirement to use government provided call management and knowledgebase systems and services) and indicates that they recognize that it is a requirement that needs to be addressed in the scope of the project and identified their assumptions in creating their response. **Responses to this criterion which contain an excessive amount of text copied directly from the ITQ and/or supporting material will not be regarded as indicating an understanding of the proposed Health Canada EAS project requirements and deliverables.**
Response:		
R-1.2	**Respondent Business Maturity - Years** The Respondent should state the number of years for which the Respondent has been providing EAPIMS (as defined in Annex B - Statement of Requirements) in Canada.	Points will be awarded in the following manner: **5 pts** = 7 or more years delivering EAPIMS in Canada **4 pts** = ≥ 5 - < 7 years **3 pts** = ≥ 4 - < 5 years **2 pts** = ≥ 3 - < 4 years **1 pt** = ≥ 2 - <3 years **0 pts** = < 2 years or no comparable response

#	Rated Evaluation Criteria	Scoring Method
Response:		
R-1.3	**Respondent Profile – Core EAPIMS Service Provider Organization** The Respondent should have an existing Business Unit that is focused on the provision of professional services in support of the design, configuration, deployment and ongoing support of EAPIMS (as defined in Annex B - Statement of Requirements) for external clients (i.e. third party organizations not affiliated with the Respondent). The Respondent should demonstrate compliance by identifying: 1. The EAPIMS Business Unit with explicit responsibility for the delivery of EAPIMS and solutions. 2. Where the EAPIMS Business Unit is positioned within the Respondent's corporate structure (e.g. by providing a corporate organization structure which clearly identifies the position of the EAPIMS Business Unit in that structure).	Points will be awarded in the following manner: **5 pts =** where the Respondent has identified a specific Business Unit that has explicit responsibility for the delivery of the EAPIMS as set out in Annex B - Statement of Requirements, where the provision of EAPIMS related services are the core business of the organization, and describes where the EAPIMS Business Unit is positioned within the Respondent's corporate structure **4 pts** = where the Respondent has identified a specific Business Unit that has primary responsibility for the delivery of the EAPIMS as set out in Annex B - Statement of Requirements where the related EAPIMS are **not** the core business of the identified organization (i.e. are part of a portfolio of business areas supported by the organization) and identifies where the EAPIMS Business Unit is positioned within the Respondent's corporate structure **3 pts** = where the Respondent has a Business Unit with resources that deliver EAPIMS to client organizations on an as and when required basis **0 pts =** where the Respondent did not demonstrate an EAPIMS capability
Response:		
R-1.4	**Respondent Profile – Core EAPIMS Provider Services Portfolio** The Respondent should demonstrate the portfolio EAPIMS provided by the Business Unit by listing the services provided. The services should include but not be limited to: 1. Services in support of transition-in including but not limited to solution design, configuration, installation, deployment,	Points will be awarded in the following manner: **5 pts** = where the Respondent has identified the services provided by the Business Unit that includes all of the services listed at points 1 and 2 are core business of the identified organization and demonstrates with a comprehensive level of details that the core services offerings are consistent with the EAPIMS as deployed

#	Rated Evaluation Criteria	Scoring Method
	integration, testing, training and otherwise making ready for use in live production. 2. Services in support of ongoing operations including but not limited to ongoing day-to-day operation, maintenance and support of the EAPIMS as deployed.	**4 pts** = where the Respondent has identified the services provided by the Business Unit that includes all of the services listed at points 1 and 2 are core business of the identified organization and demonstrates with a significant level of details that the core services offerings are consistent with the EAPIMS as deployed **3 pts** = where the Respondent has identified the services provided by the Business Unit that includes all of the services listed at points 1 and 2 are core business of the identified organization and demonstrates with an adequate level of details that the core services offerings are consistent with the EAPIMS as deployed **2 pts** = where the Respondent has identified the services provided by the Business Unit that includes all of the services listed at points 1 and 2 where the EAPIMS related services are not core business of the identified organization and demonstrates with an minimal level of details that the core services offerings are consistent with the EAPIMS as deployed **0 Pts =** where the Respondent did not sufficiently demonstrate an adequate degree of understanding of the requirement or where the Respondent provided no relevant response
Response:		
R-1.5	**<u>Respondent Business Maturity – Service Provider EAPIMS Deployment Projects</u>** The Respondent should list the number of active deployment projects for which the proposed EAPIMS Provider organization has deployed the proposed core EAPIMS into live production. **Note:** an active deployment is a deployment of the proposed core EAPIMS, or a previous version, that is in live production use by a client organization to provide EAS.	Points will be awarded in the following manner: **5 pts** = > 5 or more deployment projects **4 pts** = 4 deployment projects **3 pts** = 3 deployment projects **2 pts** = 2 deployment projects **1 pt** = 1 deployment projects **0 pts** = no deployment projects
Response:		

#	Rated Evaluation Criteria	Scoring Method
R-2	**Proposed Solution**	
R-2.1	**Proposed Solution – Core Solution Functionality** The Respondent should identify the proposed core EAPIMS that would form the foundation for an HC EAS solution. Specifically, the Respondent should identify and describe the core software solution components that in aggregate will provide the solution as deployed to provide: 1. Intake Management as set out in Annex B Section 3.2.1. 2. Case Management as set out in Annex B Section 3.2.2. 3. Quality Assurance as set out in Annex B Section 3.2.3. 4. Service Provider Management as set out in Annex B Section 3.2.4. 5. Referral Management as set out in Annex B Section 3.2.5. 6. Organizational Account Management as set out in Annex B Section 3.2.6. 7. Financial Administration as set out in Annex B Section 3.2.9. 8. Report Management as set out in Annex B Section 3.2.11. 9. User Management as set out in Annex B Section 3.2.12. 10. Portal services as set out in Annex B Section 3.2.13. 11. Communication Management as set out in Annex B Section 3.2.14.	Points will be awarded in the following manner: **5 pts** = Response addresses 10 or more of points 1 through 11 including sample documents demonstrating how point is addressed. **4 pts** = Response addresses 8 or 9 of points 1 through 11 including sample documents demonstrating how point is addressed. **3 pts** = Response addresses 7 of points 1 through 11 including sample documents demonstrating how point is addressed. **2 pts** = Response addresses 6 of points 1 through 11 including sample documents demonstrating how point is addressed , **or** addressed more than 6 points but without including sample documents demonstrating how point is addressed. **1 pt** = Response addresses 4 or 5 of points 1 through 11 including sample documents demonstrating how point is addressed, **or** addressed more than 4 points but without including sample documents demonstrating how point is addressed. **0 pts** = Response addressed less than 4 of points 1 through 11 or provides no relevant response.
Response:		
R-2.2	**Proposed Solution – Solution Architecture** The Respondent should describe the overall EAPIMS architecture. The EAPIMS should be constructed on a standards-based open architecture where a standards-based open architecture is one that:	Points will be awarded in the following manner: **Assess 5** where the Respondent has addressed the requirements in **points 1 through 3** by providing a comprehensive level of detail in the solution blueprint and has tailored its response to the EAPIMS Solution.

#	Rated Evaluation Criteria	Scoring Method
	1. Is implemented using published and publicly available web oriented architecture and "standards" definitions where such definitions include but are not limited to J2EE, .Net and XML standards. 2. Enables each functional element to be implemented on separate hardware platforms and scaled individually (e.g. user access services, EAPIMS application services functions). 3. Is based on a component based system to couple and uncouple solution components and enable maximum usage of existing resources and initial and ongoing flexibility going forward. Usage will include an ever-greening process where no single component being changed, replaced, upgraded or exchanged will bring down the system as a whole.	**Assess 4** where the Respondent has addressed the requirements in **points 1 through 3** by providing a significant level of detail in the solution blueprint and has tailored its response to the EAPIMS Solution. **Assess 3** where the Respondent has addressed the requirements in **points 1 through 3** by providing an adequate level of detail in the solution blueprint and has tailored its response to the EAPIMS Solution. **Assess 2** where the Respondent has minimally addressed the requirements in **points 1 through 3** or has not tailored its response to the EAPIMS Solution. **Assess 0** where the Respondent did not sufficiently demonstrate an adequate degree of understanding of the requirement or where the Respondent provided no relevant response.
Response:		
R-2.3	**Proposed Solution – Deployment Options** The Respondent should set out the available deployment options through which the proposed core EAPIMS can be deployed. The available deployment options include: 1. Public Cloud[1]-based deployment 2. Client On-premises deployment	Points will be awarded in the following manner: **5 pts** = Multiple deployment options including 1 and 2 **4 pts** = Deployment option 1 only **3 pts** = Deployment option 2 only **0 pts** = No deployment option
Response:		

[1] Public cloud – a commercially available offering procured and security-assessed for the use of all government organizations. In this deployment model, the government organizations will securely share tenancy with private companies, non-profits and individuals.

#	Rated Evaluation Criteria	Scoring Method
R-3	**Security and Accessibility**	
R-3.1	**Project Security – Security Policy** The Respondent should demonstrate that it has a comprehensive security policy that is aligned with the security requirements of this Health Canada EAS initiative. The Respondent should demonstrate that the proposed security policy addresses: 1. The requirement that only resources who have the security clearance to perform a task are authorized to access protected information, assets or site(s). 2. The requirement to ensure that the security policy is applied throughout the entire Respondent Team including all subcontractors. **The security policy of subcontracted organizations will not be accepted for evaluation purposes in response to this criterion.**	Points will be awarded in the following manner: **5 pts** = Response has addressed the requirements in points 1 and 2 and has tailored its response to the Health Canada EAS Project **3 pts** = Response has addressed the requirements in one of points 1 or 2, and has tailored its response to the Health Canada EAS Project **2 pts** = Response addressed the requirements in one of points 1 or 2 and has **not** tailored its response to the Health Canada EAS Project. **0 pts** = Response addresses neither points
Response:		
R-3.2	**Accessibility – WCAG 2.1 AA Guidelines** The Respondent should demonstrate how and at what level their core EAPIMS solution conforms to World Wide Web Consortium (WC) WCAG 2.1 AA guidelines set out by GC's Standard on Web Accessibility. **The Bidder should describe in detail how ensuring accessibility is built into their proposed solution from the standpoint of their release cycle.**	Points will be awarded in the following manner: **5 pts =** The Solution meets WCAG 2.1 AA or higher. **4 pts =** The Solution meets WCAG 2.0 AA with an actionable plan or product release cycle to move to WCAG 2.1 AA or higher. **3 pts =** The Solution partially meets WCAG 2.0 AA or higher with an actionable plan or product release cycle to move to WCAG 2.0 AA or higher **0 pts =** The Solution does not meets WCAG 2.0 AA minimum requirements or there is no process to complete an assessment.
Response:		

Appendix A to Annex C: Project References Forms

This Annex to the Rated Requirements provides the templates for project references:

1. Form C-1 - Previous Software Solution Deployment References – 2 reference projects are required in response to Mandatory M-7.
2. Form C-2 - EAPIMS Implementation Project Services References – 2 reference projects are required in response to Rated M-9

Respondents may use the same reference project in response to each of these requirements. Respondents must ensure that the responses are complete and provide the required completed reference forms.

For clarity, although the same project may be used in each case, each set of reference projects has specific focus and have different embedded criteria.

The Client Reference Contact Person identified in the Client Reference must be able to unambiguously confirm that the Respondent, or its Affiliate(s), provided the services as set out in the Client Reference Template. For clarity, where the provided Client Reference Contact Person is unable to unambiguously confirm that the Respondent, or its Affiliate(s), provided the services (e.g. by indicating a lack of knowledge or authority to provide such unambiguous confirmation, or, to imply such lack of knowledge by denying that the Respondent provided services), then Canada will interpret such inability to provide an unambiguous response as being a failure to confirm compliance and will assess the proposal as being non-compliant with the requirements.

The onus is on the Respondent to ensure that the Client Reference Contact Person identified in the Client Reference is able to unambiguously confirm or deny that the Respondent, or its Affiliate(s), provided the services as set out in the Client Reference Template.

Form C-1 Previous Software Solution Deployment References

Instructions for completion:

1. Two (2) relevant sample projects must be provided.
2. A separate Software Solution Deployment References form must be completed for each sample project.
3. Responses will be used to rank references provided in response to M-7 (EAPIMS Deployment References).

Reference 1

Respondent	
Client	
Contact Name	
Contact Title	
Telephone Number	
Project Name	
Brief Overview of the Project	
Project Timeframe	

Previous Software Solution Deployment References – Reference 1				
#	**Criteria**	**Weight**	**Scoring Method**	**Response**
1	The Respondent should identify that the core EAPIMS provided, deployed and operating in the reference project is using the proposed software modules and release levels.	25%	Points will be awarded in the following manner: **5 pts** = the core EAPIMS provided and deployed in the reference project is operating using the proposed software modules and release levels **4 pts** = the core EAPIMS provided and deployed in the reference project is operating using the proposed software modules at release levels that are no more than 1 major release prior to the current release level	

Previous Software Solution Deployment References – Reference 1				
#	Criteria	Weight	Scoring Method	Response
			3 pts = the core EAPIMS provided and deployed in the reference project is operating using the proposed software modules at release levels that are no more than 2 major release prior to the current release level **2 pts** = the core EAPIMS provided and deployed in the reference project is operating using the proposed software modules at release levels that are more than 2 major release prior to the current release level **0 pts** = the core EAPIMS provided and deployed in the reference project is not operating using the proposed software modules or no comparable response	
2	The Respondent should identify date at which the preference project went into live production with the EAPIMS. For clarity, the EAPIMS went into live production when the following functionality / modules are in live production: 1. Intake Management as set out in Annex B Section 3.2.1. 2. Case Management as set out in Annex B Section 3.2.2. 3. Quality Assurance as set out in Annex B Section 3.2.3; 4. Service Provider Management as set out in Annex B Section 3.2.4. 5. Referral Management as set out in Annex B Section 3.2.5. 6. Organizational Account Management as set out in Annex B Section 3.2.6. 7. Report Management as set out in Annex B Section 3.2.11.	10%	Points will be awarded in the following manner: **5 pts** = ≥ 36 months prior to the closing date of the ITQ **4 pts** = < 36 months - ≥ 24 months prior to the closing date of the ITQ **3 pts** = < 24 months - ≥ 12 months prior to the closing date of the ITQ **2 pts** = < 12 months prior to the closing date of the ITQ **0 pts** = not in live production or no comparable response	
3	The Respondent should identify the languages supported in the reference project where supported languages should include English and French.	15%	Points will be awarded in the following manner: **5 pts** = the languages supported in the reference project include English and Canadian French **4 pts** the languages supported in the reference project	

Previous Software Solution Deployment References – Reference 1				
#	Criteria	Weight	Scoring Method	Response
			include English and French **2 pts =** the languages supported in the reference project include English or French but not both **0 pts** = the languages supported in the reference project include neither English nor French or no comparable response	
4	The Respondent should identify the organization that provided the implementation services in support of the reference Project.	10%	Points will be awarded in the following manner: **5 pts** = the solution provider proposed for this HC project is the organization that provided the implementation services in support of the reference Project **0 pts** = the solution provider proposed for this HC project is not the organization that provided the implementation services in support of the reference Project or no comparable response	
5	The Respondent should identify the organization that provided ongoing operational support services in support of the reference Project.	10%	Points will be awarded in the following manner: **5 pts** = the solution provider proposed for this HC project is the organization that provided the ongoing operational support services in support of the reference Project **0 pts** = the solution provider proposed for this HC project is not the organization that provided the ongoing operational support services in support of the reference Project or no comparable response	
6	The Reference project should incorporate the deployment of 1. Intake Management as set out in Annex B Section 3.2.1. 2. Case Management as set out in Annex B Section 3.2.2. 3. Quality Assurance as set out in Annex B Section 3.2.3. 4. Service Provider Management as set out in Annex B Section 3.2.4. 5. Referral Management as set out in Annex B Section 3.2.5. 6. Organizational Account Management as set out in Annex B Section 3.2.6. 7. Financial Administration as set out in Annex	20%	Points will be awarded in the following manner: **5 pts** = Referenced project incorporated deployment of 10 or more of points 1 through 11 **4 pts** = Referenced project incorporated deployment of 8 or 9 of points 1 through 11 **3 pts** = Referenced project incorporated deployment of 7 of points 1 through 11 **2 pts** = Referenced project incorporated deployment of 6 of points 1 through 11 **1 pt** = Referenced project incorporated deployment of 4 or 5 of points 1 through 11 **0 pts** = Referenced project incorporated deployment of less than 4 of points 1 through 11 or provides no relevant response	

Previous Software Solution Deployment References – Reference 1				
#	Criteria	Weight	Scoring Method	Response
	B Section 3.2.9. 8. Report Management as set out in Annex B Section 3.2.11. 9. User Management as set out in Annex B Section 3.2.12. 10. Portal services as set out in Annex B Section 3.2.13. 11. Communication Management as set out in Annex B Section 3.2.14.			
7	The Respondent should identify the number of cases* handled annually by the deployed EAPIMS. *A “case” is an individual referral of an eligible EAP client to an accredited private practice counsellor	10%	Points will be awarded in the following manner: **5 pts** = ≥ 20,000 cases annually **4 pts** = ≥ 10,00l0 - < 20,000 cases annually **3 pts** = ≥ 5,000 - < 10,000 cases annually **2 pts** = ≥ 3,000 - < 5,000 cases annually **1 pt** = ≥ 1,000 - < 3,000 cases annually **0 pts** = < 1,000 cases annually or no comparable response	

Reference 2

Respondent	
Client	
Contact Name	
Contact Title	
Telephone Number	
Project Name	
Brief Overview of the Project	
Project Timeframe	

Previous Software Solution Deployment References – Reference 2				
#	**Criteria**	**Weight**	**Scoring Method**	**Response**
1	The Respondent should identify that the core EAPIMS provided, deployed and operating in the reference project is using the proposed software modules and release levels.	25%	Points will be awarded in the following manner: **5 pts** = the core EAPIMS provided and deployed in the reference project is operating using the proposed software modules and release levels **4 pts** = the core EAPIMS provided and deployed in the reference project is operating using the proposed software modules at release levels that are no more than 1 major release prior to the current release level	

Previous Software Solution Deployment References – Reference 2				
#	Criteria	Weight	Scoring Method	Response
			3 pts = the core EAPIMS provided and deployed in the reference project is operating using the proposed software modules at release levels that are no more than 2 major release prior to the current release level **2 pts** = the core EAPIMS provided and deployed in the reference project is operating using the proposed software modules at release levels that are more than 2 major release prior to the current release level **0 pts** = the core EAPIMS provided and deployed in the reference project is not operating using the proposed software modules or no comparable response	
2	The Respondent should identify date at which the preference project went into live production with the EAPIMS. For clarity, the EAPIMS went into live production when the following functionality / modules are in live production: 1. Intake Management as set out in Annex B Section 3.2.1. 2. Case Management as set out in Annex B Section 3.2.2. 3. Quality Assurance as set out in Annex B Section 3.2.3; 4. Service Provider Management as set out in Annex B Section 3.2.4. 5. Referral Management as set out in Annex B Section 3.2.5. 6. Organizational Account Management as set out in Annex B Section 3.2.6. 7. Report Management as set out in Annex B Section 3.2.11.	10%	Points will be awarded in the following manner: **5 pts** = ≥ 36 months prior to the closing date of the ITQ **4 pts** = < 36 months - ≥ 24 months prior to the closing date of the ITQ **3 pts** = < 24 months - ≥ 12 months prior to the closing date of the ITQ **2 pts** = < 12 months prior to the closing date of the ITQ **0 pts** = not in live production or no comparable response	
3	The Respondent should identify the languages supported in the reference project where supported languages should include English and French.	15%	Points will be awarded in the following manner: **5 pts** = the languages supported in the reference project include English and Canadian French **4 pts** the languages supported in the reference project	

Previous Software Solution Deployment References – Reference 2				
#	Criteria	Weight	Scoring Method	Response
			include English and French **2 pts =** the languages supported in the reference project include English or French but not both **0 pts** = the languages supported in the reference project include neither English nor French or no comparable response	
4	The Respondent should identify the organization that provided the implementation services in support of the reference Project.	10%	Points will be awarded in the following manner: **5 pts** = the solution provider proposed for this HC project is the organization that provided the implementation services in support of the reference Project **0 pts** = the solution provider proposed for this HC project is not the organization that provided the implementation services in support of the reference Project or no comparable response	
5	The Respondent should identify the organization that provided ongoing operational support services in support of the reference Project.	10%	Points will be awarded in the following manner: **5 pts** = the solution provider proposed for this HC project is the organization that provided the ongoing operational support services in support of the reference Project **0 pts** = the solution provider proposed for this HC project is not the organization that provided the ongoing operational support services in support of the reference Project or no comparable response	
6	The Reference project should incorporate the deployment of 1. Intake Management as set out in Annex B Section 3.2.1. 2. Case Management as set out in Annex B Section 3.2.2. 3. Quality Assurance as set out in Annex B Section 3.2.3. 4. Service Provider Management as set out in Annex B Section 3.2.4. 5. Referral Management as set out in Annex B Section 3.2.5. 6. Organizational Account Management as set out in Annex B Section 3.2.6. 7. Financial Administration as set out in Annex	20%	Points will be awarded in the following manner: **5 pts** = Referenced project incorporated deployment of 10 or more of points 1 through 11 **4 pts** = Referenced project incorporated deployment of 8 or 9 of points 1 through 11 **3 pts** = Referenced project incorporated deployment of 7 of points 1 through 11 **2 pts** = Referenced project incorporated deployment of 6 of points 1 through 11 **1 pt** = Referenced project incorporated deployment of 4 or 5 of points 1 through 11 **0 pts** = Referenced project incorporated deployment of less than 4 of points 1 through 11 or provides no relevant response	

Previous Software Solution Deployment References – Reference 2				
#	Criteria	Weight	Scoring Method	Response
	B Section 3.2.9. 8. Report Management as set out in Annex B Section 3.2.11. 9. User Management as set out in Annex B Section 3.2.12. 10. Portal services as set out in Annex B Section 3.2.13. 11. Communication Management as set out in Annex B Section 3.2.14.			
7	The Respondent should identify the number of cases* handled annually by the deployed EAPIMS. *A “case” is an individual referral of an eligible EAP client to an accredited private practice counsellor	10%	Points will be awarded in the following manner: **5 pts** = ≥ 20,000 cases annually **4 pts** = ≥ 10,00l0 - < 20,000 cases annually **3 pts** = ≥ 5,000 - < 10,000 cases annually **2 pts** = ≥ 3,000 - < 5,000 cases annually **1 pt** = ≥ 1,000 - < 3,000 cases annually **0 pts** = < 1,000 cases annually or no comparable response	

Form C-2 EAPIMS Implementation Project Services References

Instructions for completion:

1. Two (2) relevant sample projects must be provided.
2. A separate EAPIMS Implementation Project Services References form must be completed for each sample project.
3. Responses will be used to rank M-9 References (EAPIMS Provider References).

Reference 1

Respondent	
Client	
Contact Name	
Contact Title	
Telephone Number	
Project Name	
Brief Overview of the Project	
Project Timeframe	

EAPIMS Implementation Project Services References – Reference 1				
#	Criteria	Weight	Scoring Method	Response
1	The Respondent should identify the core EAPIMS provided and deployed in the reference project including the proposed software modules and release levels.	15%	Points will be awarded in the following manner: **5 pts** = the core EAPIMS provided and deployed in the reference project is operating using the proposed software modules and release levels **4 pts** = the core EAPIMS provided and deployed in the reference project is operating using the proposed software modules at release levels that are no more than 1 major release prior to the current release level **3 pts =** the core EAPIMS provided and deployed in the reference project is operating using the proposed software modules at release levels that are no more than 2 major release prior to the current release level **2 pts** = the core EAPIMS provided and deployed in the reference project is operating using the proposed software modules at release levels that are more than 2 major release prior to the current release level **0 pts** = the core EAPIMS provided and deployed in the reference project is not operating using the proposed software modules or no comparable response	
2	The Respondent should identify date at which the preference project went into live production with the EAPIMS. For clarity, the EAPIMS went into live production when the following functionality / modules are in live production: 1. Intake Management as set out in Annex B Section 3.2.1. 2. Case Management as set out in Annex B Section 3.2.2. 3. Quality Assurance as set out in Annex B Section 3.2.3. 4. Service Provider Management as set out in Annex B Section 3.2.4. 5. Referral Management as set out in Annex B	15%	Points will be awarded in the following manner: **5 pts** = > 36 months prior to the closing date of the ITQ **4 pts** = < 36 months - > 24 months prior to the closing date of the ITQ **3 pts** = < 24 months - > 12 months prior to the closing date of the ITQ **2 pts** = < 12 months prior to the closing date of the ITQ **0 pts** = not in live production or no comparable response	

EAPIMS Implementation Project Services References – Reference 1				
#	Criteria	Weight	Scoring Method	Response
	Section 3.2.5. 6. Organizational Account Management as set out in Annex B Section 3.2.6. 7. Report Management as set out in Annex B Section 3.2.11.			
3	The Respondent should identify the languages supported in the reference project where supported languages should include English and French.	20%	Points will be awarded in the following manner: **5 pts** = the languages supported in the reference project include English and Canadian French **4 pts** = the languages supported in the reference project include English and French **2 pts =** the languages supported in the reference project include English or French but not both **0 pts** = the languages supported in the reference project include neither English or French or no comparable response	
4	The Respondent should identify the organization that provided the implementation services in support of the reference Project.	25%	Points will be awarded in the following manner: **5 pts** = the solution provider proposed for this HC project is the organization that provided the implementation services in support of the reference Project **0 pts** = the solution provider proposed for this HC project is not the organization that provided the implementation services in support of the reference Project or no comparable response	
5	The Respondent should identify the organization that provided ongoing operational support services in support of the reference Project.	25%	Points will be awarded in the following manner: **5 pts** = the solution provider proposed for this HC project is the organization that provided the ongoing operational support services in support of the reference Project **0 pts** = the solution provider proposed for this HC project is not the organization that provided the ongoing operational support services in support of the reference Project or no comparable response	

Reference 2

Respondent	
Client	
Contact Name	
Contact Title	
Telephone Number	
Project Name	
Brief Overview of the Project	
Project Timeframe	

EAPIMS Implementation Project Services References – Reference 2				
#	**Criteria**	**Weight**	**Scoring Method**	**Response**
1	The Respondent should identify the core EAPIMS provided and deployed in the reference project including the proposed software modules and release levels.	15%	Points will be awarded in the following manner: **5 pts** = the core EAPIMS provided and deployed in the reference project is operating using the proposed software modules and release levels **4 pts** = the core EAPIMS provided and deployed in the reference project is operating using the proposed software modules at release levels that are no more than 1 major release prior to the current release level **3 pts =** the core EAPIMS provided and deployed in the reference project is operating using the proposed software modules at release levels that are no more than 2 major release prior to the current release level **2 pts** = the core EAPIMS provided and deployed in the reference project is operating using the proposed software modules at release levels that are more than 2 major release prior to the current release level **0 pts** = the core EAPIMS provided and deployed in the reference project is not operating using the proposed software modules or no comparable response	
2	The Respondent should identify date at which the preference project went into live production with the EAPIMS. For clarity, the EAPIMS went into live production when the following functionality / modules are in live production: 1. Intake Management as set out in Annex B Section 3.2.1. 2. Case Management as set out in Annex B Section 3.2.2. 3. Quality Assurance as set out in Annex B Section 3.2.3. 4. Service Provider Management as set out in Annex B Section 3.2.4. 5. Referral Management as set out in Annex B	15%	Points will be awarded in the following manner: **5 pts** = > 36 months prior to the closing date of the ITQ **4 pts** = < 36 months - > 24 months prior to the closing date of the ITQ **3 pts** = < 24 months - > 12 months prior to the closing date of the ITQ **2 pts** = < 12 months prior to the closing date of the ITQ **0 pts** = not in live production or no comparable response	

EAPIMS Implementation Project Services References – Reference 2				
#	**Criteria**	**Weight**	**Scoring Method**	**Response**
	Section 3.2.5. 6. Organizational Account Management as set out in Annex B Section 3.2.6. 7. Report Management as set out in Annex B Section 3.2.11.			
3	The Respondent should identify the languages supported in the reference project where supported languages should include English and French.	20%	Points will be awarded in the following manner: **5 pts** = the languages supported in the reference project include English and Canadian French **4 pts** = the languages supported in the reference project include English and French **2 pts =** the languages supported in the reference project include English or French but not both **0 pts** = the languages supported in the reference project include neither English or French or no comparable response	
4	The Respondent should identify the organization that provided the implementation services in support of the reference Project.	25%	Points will be awarded in the following manner: **5 pts** = the solution provider proposed for this HC project is the organization that provided the implementation services in support of the reference Project **0 pts** = the solution provider proposed for this HC project is not the organization that provided the implementation services in support of the reference Project or no comparable response	
5	The Respondent should identify the organization that provided ongoing operational support services in support of the reference Project.	25%	Points will be awarded in the following manner: **5 pts** = the solution provider proposed for this HC project is the organization that provided the ongoing operational support services in support of the reference Project **0 pts** = the solution provider proposed for this HC project is not the organization that provided the ongoing operational support services in support of the reference Project or no comparable response	

Appendix B to Annex C: Applicable Weights for Rated Evaluation Criteria

ITQ RATED REQUIREMENTS		
Hierarchy	**Criteria**	**Overall Weight**
R-1	**Respondent - Corporate Capability**	**30%**
R-1.1	Understanding of EAS Project Requirements	3%
R-1.2	Respondent Business Maturity - Years	4.5%
R-1.3	Respondent Profile – Core EAPIMS Provider Organization	4.5%
R-1.4	Respondent Profile – Core EAP Service Provider Services Portfolio	9%
R-1.5	Respondent Business Maturity – Service Provider EAPIMS Deployment Projects	9%
R-2	**Proposed EAP Software Solution**	**40%**
R-2.1	Proposed Solution – Core Solution Functionality	16%
R-2.2	Proposed Solution – Solution Architecture	12%
R-2.3	Proposed Solution – Deployment Options	12%
R-3	**Security and Accessibility**	**10%**
R-3.1	Project Security – Security Policy	5%
R-3.2	Accessibility	5%
R-4	**References**	**20%**
R-4.1	Annex C-1 Previous Software Solution Deployment Reference #1	5%
R-4.2	Annex C-1 Previous Software Solution Deployment Reference #2	5%
R-4.3	Annex C-2 EAPIMS Implementation Project Services Reference #1	5%
R-4.4	Annex C-2 EAPIMS Implementation Project Services Reference #2	5%

ANNEX D

DRAFT SECURITY REQUIREMENTS APPLICABLE TO ON-PREMISES SOLUTIONS AT THE RFP STAGE AND ANY RESULTING CONTRACT

Note: The requirements address some, but not necessarily all of the requirements which Canada intends to address in the RFP. Additional security requirements may be included in a subsequent phases of this procurement process. Canada is including these requirements in this ITQ to provide respondents advance notice of some of the requirements that are likely to be included in the associated RFP.

1. Before award of a contract, the following conditions must be met:

   (a) the Bidder must hold a valid organization security clearance as indicated in below;

   (b) the Bidder's proposed individuals requiring access to classified or protected information, assets or sensitive work sites must meet the security requirements as indicated below;

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

2. In the case of a joint venture bidder, each member of the joint venture must meet the security requirements.

3. 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.

4. For additional information on security requirements, Bidders should refer to the Contract Security Program of Public Works and Government Services Canada (http://www.tpsgc-pwgsc.gc.ca/esc-src/introduction-eng.html) website.

5. Foreign bidders must be from a country where there is an existing bi-lateral industrial security agreement with Canada that stipulates security equivalencies. Foreign bidders (including U.S.) should contact the Contracting Authority to obtain the security requirements terms that will apply to the bid solicitation and the resulting contract.

SECURITY REQUIREMENT FOR CANADIAN SUPPLIER:

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

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

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

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

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

   (a) Security Requirements Check List and security guide (if applicable), attached at Annex E;
   (b) Industrial Security Manual (Latest Edition)

ANNEX E

SECURITY REQUIREMENTS CHECK LIST (SRCL)

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat: HT300-193651

Security Classification / Classification de sécurité

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

PART A - CONTRACT INFORMATION / PARTIE A - INFORMATION CONTRACTUELLE

1. Originating Government Department or Organization / Ministère ou organisme gouvernemental d'origine: Health Canada

2. Branch or Directorate / Direction générale ou Direction: CSB / Specialized Health Services Directorate / EAS

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

Invitation To Qualify (ITQ) for a ready to use Commercial-Off-The-Shelf (COTS) software that fits the business needs of the Employee Assistance Services (EAS) group.

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
Access to development servers limited or brokered by Shared Services Canada (SSC) for installation of Employee Assistance Program Info. Mgmt. System (EAPIMS) software for configuration and testing purposes.

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

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

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

Canada	NATO / OTAN	Foreign / Étranger
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) [ ]

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat: HT300-193651

Security Classification / Classification de sécurité

PART A (continued) / PARTIE A (suite)

6. 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 :

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?

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
HT300-193651
Security Classification / Classification de sécurité

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

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

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

SUMMARY CHART / TABLEAU RÉCAPITULATIF

Category / Catégorie	PROTECTED / PROTÉGÉ			CLASSIFIED / CLASSIFIÉ			NATO				COMSEC					
	A	B	C	CONFIDENTIAL / CONFIDENTIEL	SECRET	TOP SECRET / TRÈS SECRET	NATO RESTRICTED / NATO DIFFUSION RESTREINTE	NATO CONFIDENTIAL / NATO CONFIDENTIEL	NATO SECRET	COSMIC TOP SECRET / COSMO TRÈS SECRET	PROTECTED / PROTÉGÉ A	PROTECTED / PROTÉGÉ B	PROTECTED / PROTÉGÉ C	CONFIDENTIAL / CONFIDENTIEL	SECRET	TOP SECRET / TRÈS SECRET
Information / Assets / Renseignements / Biens	✓	✓														
Production																
IT Media / Support TI	✓	✓														
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	
HT300-193651	
Security Classification / Classification de sécurité	

PART D - AUTHORIZATION / PARTIE D - AUTORISATION

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

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature
Nishad Datoo	Project Manager	N. Datoo

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date
(613) 949-6257		nishad.datoo@canada.ca	Jan. 27, 2020

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

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature
SONIA LAROSE	Sec. Contract Coord.	Larose

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date
613-954-1775		Sonia.larose@canada.ca	2020-01-28

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

16. Procurement Officer / Agent d'approvisionnement

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

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

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

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

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

ANNEX F

DRAFT MINIMUM SECURITY REQUIREMENTS APPLICABLE TO SAAS SOLUTIONS AT THE RFP STAGE AND ANY RESULTING CONTRACT

(a) Annex F sets the minimum security requirements that must be met in order to demonstrate security compliance for the provision of EAPIMS using SaaS Solution at the RFP stage. These requirements address some, but not necessarily all of the requirements which Canada intends to address in the RFP. Additional security requirements may be included in subsequent phases of this procurement process. Canada is including these requirements in this ITQ to provide respondents advance notice of some of the requirements that are likely to be included in the associated RFP.

(b) The Annex is divided in 5 schedules as follows:

- Schedule A - Industrial Security Program for Cloud Protected B Requirements
- Schedule B - Protected B Data Security Compliance Requirements
- Schedule C - Privacy Obligations
- Schedule D - Security Obligations
- Schedule E - Supply Chain Integrity Process

Schedule A – Industrial Security Program for Cloud Protected B Requirements

1. Before award of a contract the following conditions must be met:

   (a) the Contractor must hold a valid organization security clearance as indicated in below;

   (b) the Contractor proposed individuals requiring access to classified or protected information, assets or sensitive work sites must meet the security requirements as indicated below;

   (c) the Contractor must provide the name of all individuals who will require access to classified or protected information, assets or sensitive work sites.

2. In the case of a joint venture Contractor, each member of the joint venture must meet the security requirements.

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

4. For additional information on security requirements, Contractor should refer to the Contract Security Program of Public Works and Government Services Canada (http://www.tpsgc-pwgsc.gc.ca/esc-src/introduction-eng.html) website.

A.1 Security requirements for Canadian Contractor

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

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

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

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

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

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

   (b) Industrial Security Manual (Latest Edition);

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

A.2 Security requirements for foreign contractor

The Canadian Designated Security Authority (Canadian DSA) for industrial security matters in Canada is the Industrial Security Sector (ISS), Public Works and Government Services Canada (PWGSC), administered by International Industrial Security Directorate (IISD), PWGSC. The Canadian DSA is the authority for confirming Contractor/Subcontractor compliance with the security requirements for foreign Contractor/Subcontractor. The following security requirements apply to the foreign Contractor/Subcontractor incorporated or authorized to do business in a jurisdiction other than Canada and delivering/performing outside of Canada the Work described in the Cloud Solutions, in addition to the Privacy Requirements and Security Requirements detailed in Schedule C and Schedule D respectively.

1. The Foreign recipient Contractor/Subcontractor 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 has international bilateral security instruments with the countries listed on the following PWGSC website: http://www.tpsgc-pwgsc.gc.ca/esc-src/international-eng.html.

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

   (a) The Foreign recipient Contractor/Subcontractor must provide proof that they are incorporated or authorized to do business in their jurisdiction.
   (b) The Foreign recipient Contractor/Subcontractor must not begin providing the 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/Subcontractor in an Attestation Form, to provide confirmation of compliance and authorization for services to be performed.
   (c) The Foreign recipient Contractor/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/Subcontractor 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.

   (d) The Foreign recipient Contractor/Subcontractor must not grant access to CANADA PROTECTED information/assets, except to personnel who have been screened in accordance with the definition and practices in the Treasury Board Standard on Security Screening (https://www.tbssct.gc.ca/pol/doc-eng.aspx?id=28115), or use acceptable equivalent measures established by the Contractor/Subcontractor in their publicly available documentation, and as agreed to by Canada.

3. **Canada protected** information/assets, provided to the foreign recipient Contractor/Subcontractor or produced by the Foreign recipient Contractor/Subcontractor, must:

   (a) not be disclosed to another government, person or firm, or representative thereof not directly related to the performance of the contract / subcontract, without the prior written consent of Canada. Such consent must be sought from its national DPA, the Contracting Authority (in collaboration with the Canadian DSA); and
   (b) not be used for any purpose other than for the performance of the contract/subcontract without the prior written approval Canada. This approval must be obtained by contacting its national DPA, the Contracting Authority (in collaboration with the Canadian DSA).

4. 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.

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

6. The Foreign recipient Contractor/Subcontractor must, at all times during the performance of the contract/subcontract hold an equivalence to an approved Document Safeguarding Capability (DSC) at the level of establish by the contracts/subcontract.

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

8. The Foreign recipient Contractor/Subcontractor must comply with the provisions of the Security Requirements Check List attached at Annex E for Cloud Protected B requirements.

9. Canada has the right to reject any request made separate and apart from the authorization in this Contract in connection with the Contractor/Subcontractor delivering Services 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.

Schedule B – Protected B Data Security Compliance Requirements

The following twenty (20) Security requirements must be met in order to demonstrate security compliance (**Up to and including Protected B Data).**

Table 1. Requirements for Security Compliance (up to and including Protected B data)

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance
M1	**Roles and Responsibilities for Security**	The Supplier must clearly delineate the roles and responsibilities for the security controls and features of the Services between the Supplier (any Supplier Sub-processors, as applicable) and Canada.	In the document, the Supplier must include, at a minimum, the parties' 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.
M2	**Master / Root Account Management**	The Supplier of the proposed Commercially Available Software as a Service must have the ability to protect the confidentiality, integrity and availability of GC Master Account information and credentials used to establish the GC cloud environment. This includes ensuring that credentials remain within the geographic boundaries of Canada.	The Supplier must demonstrate compliance by providing documentation outlining the Commercially Available Software as a Service's ability to protect the confidentiality, integrity and availability of GC Master Account information and credentials used to establish the GC cloud environment. 1) To be considered compliant, the provided documentation must include: 2) a) System documentation or white paper that outlines the policies, processes and procedures used to protect the confidentiality, integrity and availability of GC Master Account information and credentials used to establish the GC cloud environment. 3) The substantiation required for the Master / Root Account Management, the documentation cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Supplier of the proposed Commercially Available Software as a Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. The Suppliers must indicate where in response the reference material can be found, including the title of the document, and the page and paragraph numbers. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the response, it is requested that Suppliers indicate where in response the reference material can be found, including the title of the document, and the page and paragraph numbers.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance
M3	**Data Protection Isolation**	The proposed Services must provide the GC the ability to isolate data in Canada in an approved data center. For the purposes of this solicitation, an Approved Data Centre is defined as the following: a) A data center that is geographically located in Canada; and b) A data centre that meets all security requirements and certifications identified. Data Center Facilities Requirements: The Supplier of the proposed Commercially Available Software as a Service must ensure that security measures are implemented for the protection of IT facilities and information system assets on which Canada data is stored and processed against all forms of tampering, loss, damage, and seizure, and that is based on a prevent- detect-respond-recover approach to physical security. Physical protection measures must be applied in accordance with, or use an adequate risk-based approach aligned with the physical and environmental protection (PE), maintenance (MA), and media protection (MP) security controls outlined in ITSG-33 Government of Canada Security Control Profile for Cloud-Based GC IT Services for PBMM and the practices in the Royal Canadian Mounted Police (RCMP) guidance and standards on physical security. This includes, at a minimum a) sufficient redundancy and recovery capabilities within and between its IT facilities including being geographically disparate such that the loss of one data center does not prohibit recovery of data within the prescribed Service Level Agreement; b) proper handling of IT media;	The Supplier must provide documentation that demonstrates how the Supplier of the proposed Services complies with the requirements in the Data Center Facilities Requirements To be considered compliant, the provided documentation must include: a) system documentation or technical documentation outlining and detailing the security measures including policies, processes and procedures that are implemented for the protection of IT facilities and information system assets on which GC data is stored and processed against all forms of tampering, loss, damage, and seizure, and that is based on a prevent- detect-respond-recover approach to physical security. The substantiation required for Data Center Facilities Requirements - , the documentation cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Commercially Available Software as a Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. The Suppliers must indicate where in response the reference material can be found, including the title of the document, and the page and paragraph numbers. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the response, it is requested that Suppliers indicate where in response the reference material can be found, including the title of the document, and the page and paragraph numbers.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance
		c) controlled maintenance of 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 its information system assets to authorized employees and contractors 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) maintaining audit logs of physical access; h) controlling and managing physical access devices; i) enforcing safeguarding measures for Canada data at alternate work sites (e.g., telework sites); and j) recording and monitoring all physical access to data center facilities and all logical access to information system components hosting Canada's data using a combination of access logs and video surveillance in all sensitive areas and intrusion detection mechanisms.	
M4	**Data Segregation**	The Supplier must, for both Tiers, implement controls to ensure appropriate isolation of resources such that Information Assets are not co-mingled with other tenant data, while in use, storage or transit, and throughout all aspects of the Supplier's Service's and Supplier Infrastructure's functionality and system administration. This includes implementing access controls and enforcing appropriate logical or physical segregation to support: (a) The separation between Supplier's internal administration from resources used by its customers; and (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.	The Supplier must provide documentation that demonstrates how the Supplier of the proposed Services complies with the requirements.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance
M5	**Data Protection**	The Supplier of the proposed Commercially Available Software as a Services must have the ability or the Government of Canada to store and protect its information at rest, including data in backups or maintained for redundancy purposes within the geographic boundaries of Canada. This includes: a) Identifying and providing the Government of Canada with an up-to-date list of physical locations including city which may contain Canada's data in Canada for each data centre that will be used to provide Services. b) Identifying which portions of the Services are delivered from outside of Canada including all locations where data is stored and processed and where they manage the service from. c) ensuring the infeasibility of finding a specific customer's data on physical media; and d) Employing encryption to ensure that no data is written to a disk in an unencrypted form. Suppliers please note: Suppliers are advised that subsequent procurement Streams may require the Supplier of the proposed Commercially Available Software as a Service to notify Canada when there are updates to the list of physical locations which may contain Canada's data.	The Supplier must demonstrate compliance by providing documentation outlining proposed Commercially Available Software as a Service's ability to isolate data in Canada in an approved data center. To be considered compliant, the provided documentation must include the following: a) Screen shots of the available data center where Canadian data centers are on the availability list; and b) A list or map indicating where geographically the data centers are located in Canada. The substantiation required for this criteria cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Commercially Available Software as a Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Submission, it is requested that Suppliers indicate where in response the reference material can be found, including the title of the document, and the page and paragraph numbers.
M6	**Data Center Facilities**	The Supplier of the proposed Commercially Available Software as a Service must ensure that security measures are implemented for the protection of IT facilities and information system assets on which GC data is stored and processed against all forms of tampering, loss, damage, and seizure, and that is based on a prevent- detect-respond-recover approach to physical security. Physical protection measures must be applied in accordance with, or use an adequate risk-based approach aligned with the physical aligned with the	The Supplier must provide documentation that demonstrates how the Supplier of the proposed Services complies with the requirements in the Data Center Facilities Requirements. To be considered compliant, the provided documentation must include: a) system documentation or technical documentation outlining and detailing the security measures including policies, processes and procedures that are implemented for the protection of IT facilities and information system assets on which Canada data is stored and processed against all forms of tampering, loss, damage, and seizure, and

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance
		physical security controls and the practices in the Treasury Board Operational Security Standard on Physical Security (http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12329) . The security measures required under this include, at a minimum; a) sufficient redundancy and recovery capabilities within and between its IT facilities including being geographically disparate such that the loss of one data center does not prohibit recovery of data within the prescribed Service Level Agreement; b) proper handling of IT media; c) controlled maintenance of 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 its information system assets to authorized employees and contractors 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) maintaining audit logs of physical access; h) controlling and managing physical access devices; i) enforcing safeguarding measures for GC data at alternate work sites (e.g., telework sites); and j) recording and monitoring all physical access to data center facilities and all logical access to information system components hosting Canada's data using a combination of access logs and video surveillance in all sensitive areas and intrusion detection mechanisms.	that is based on a prevent- detect-respond-recover approach to physical security. The substantiation required for Data Center Facilities Requirements, the documentation cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Commercially Available Software as a Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the response, it is requested that Suppliers indicate where in response the reference material can be found, including the title of the document, and the page and paragraph numbers.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance
M7	**Personnel Security**	The Supplier of the proposed Commercially Available Software as a Services must implement security measures that grant and maintain the required level of security screening for its respective personnel, as well as the personnel of any subcontractor personnel pursuant to their access privileges to information system assets on which Canada's Data is stored and processed. Screening measures must be applied in accordance with the definition and practices in the Treasury Board Standard on Security Screening (https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=28115) , or use an acceptable equivalent agreed to by Canada. This includes, at a minimum: a Personnel Security) description of the employee and subcontractor positions that require access to Canada's Data or have the ability to affect the confidentiality, integrity or availability of the Services; b) process for ensuring that employees and contractors understand, are aware, and fulfil, their responsibilities for information security, and are suitable for the roles for which they are considered; c) process for security awareness and training as part of employment on boarding and when employee and subcontractor roles change; d) process that is enforced when an employee or subcontractor changes their role or when employment is terminated; and e) approach for detecting potential malicious insiders and controls implemented to mitigate the risk of access to GC data and/or effect on the reliability of cloud services hosting GC assets and data	The Supplier must provide documentation that demonstrates how the Supplier of the proposed Services complies with the requirements in the Personnel Security Requirements. To be considered compliant, the provided documentation must include: a) system documentation or technical documentation outlining and detailing the security measures including the policies, processes and procedures that are used to grant and maintain the required level of security screening for the Supplier and subcontractor personnel pursuant to their access privileges to information system assets on which Canada's Data is stored and processed. The substantiation required in the Personnel Security Requirements, the documentation cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Supplier of the proposed Commercially Available Software as a Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. The Suppliers must indicate where in response the reference material can be found, including the title of the document, and the page and paragraph numbers. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the response, it is requested that Suppliers indicate where in response the reference material can be found, including the title of the document, and the page and paragraph numbers.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance
M8	**Third Party Assurance**	The Supplier of the proposed Commercially Available Software as a Service must be designed and developed to ensure the security of their proposed Commercially Available Software as a Service, including, implementing information security policies, procedures, and security controls. The Supplier of the proposed Commercially Available Software as a Service must also comply with the security requirements selected in the GC Security Control Profile for Cloud-Based GC IT Services for Protected B, Medium Integrity and Medium Availability (PBMM) for the scope of the proposed Commercially Available Software as a Service provided. Compliance will be validated and verified through the Canadian Centre for Cyber Security (CCCS) Cloud Service Provider (CSP) Information Technology (IT) Security Assessment Process (ITSM.50.100) (https://cyber.gc.ca/en/guidance/cloud-service-provider-information-technology-security-assessment-process-itsm50100) . Any Supplier that has participated in the process must provide documentation to confirm that they have completed the on-boarding process with (i) a copy of the most recent completed assessment report provided by CCCS; and (ii) a copy of the most recent summary report provided by CCCS. This will accelerate the qualification process and at the same doesn't require the Supplier to demonstrate the compliance To initiate the on-boarding process, the Supplier should contact the CCCS Client Services to receive a copy of the onboarding submission form and any additional information related to the CSP IT Assessment Program.	The Supplier must demonstrate how the Supplier of the proposed Commercially Available Software as a Service complies with the requirements in the Third Party Assurance Requirements. Compliance must be demonstrated through the mapping of security controls to the applicable industry certifications identified below, and validated through independent third party assessments. The Supplier must provide each of the following industry certifications to demonstrate compliance: 1) ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems – Requirements; and 2) ISO/IEC 27017:2015 Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services; and 3) AICPA Service Organization Control (SOC) 2 Type II for the trust principles of security, availability, processing integrity, and confidentiality. Each certification or assessment report must: a) Be valid as of the Submission date; b) Identify the legal business name of the proposed Commercially Available Software as a Service and Cloud Service Provider; c) Identify the current certification date and/or status; d) Identify the list of Assets, Supplier Infrastructure, and Service Locations within the scope of the certification report. e) The scope of the report must map to locations and services offered by the proposed Commercially Available Software as a Service. 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; and f) Be issued from an independent third party qualified under AICPA or CPA Canada, and/or ISO certification regime and that conforms to ISO/IEC 17020 quality system standard. The Supplier can provide additional supplementary evidence from system security plans, information system design, information system architecture, or documents that provide a comprehensive system

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance
			description, such as assessment of its Services against the Cloud Security Alliance (CSA) Cloud Control's Matrix (CCM) version 3.01 or subsequent version, to support the claims from the above certifications, in order to demonstrate compliance to the GC Security Control Profile for Cloud-Based GC IT Services for Protected B, Medium Integrity and Medium Availability (PBMM). Please note • Certifications must be provided for all portions of the proposed Service. • Certifications must be accompanied by assessment reports.
M9	**IT Security Assessment Program**	The Supplier must demonstrate compliance with the security requirements selected in the GC Security Control Profile for Cloud-Based GC IT Services available (https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/cloud-computing/government-canada-security-control-profile-cloud-based-it-services.html) for the scope of the Services provided by the Supplier in the IT Security Assessment Program.	The Supplier must demonstrate compliance with the security requirements selected in the GC Security Control Profile for Cloud-Based GC IT Services available (https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/cloud-computing/government-canada-security-control-profile-cloud-based-it-services.html) for the scope of the Services provided by the Supplier in the IT Security Assessment Program. Compliance must be demonstrated through the mapping of security controls to the applicable industry certifications identified below, and validated through independent third party assessments. Mapping of the Security Controls must a included; GC Security Control Profile for Cloud-Based GC IT Services , and Industry Certification in Third-Party Assurance detailed under M8.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance
M10	**Supply Chain Management**	The Supplier must provide a third-party supplier list containing information on any third parties (e.g. subsidiaries, subcontractors, etc.) that would provide Canada with the proposed Commercially Available Software as a Service. For the purposes of this requirement, a company who is merely a supplier of goods to the Supplier of the proposed Commercially Available Software as a Service, but who does not perform any portion of the supply chain that could provide Canada with the proposed Commercially Available Software as a Service, is not considered to be a third party. Third party examples would include, for example, technicians who might be deployed or maintain the Commercially Available Software as a Services of the Supplier has been proposed by the Supplier. Please note: Suppliers are advised that subsequent procurement Streams may require the Supplier to notify Canada regularly when there are updates to the list of third-party suppliers.	The Supplier must provide documentation that lists information on any third parties that could be used to perform any part of the supply chain that would provide Canada with the proposed Commercially Available Software as a Service whether they would be (i) subcontractors to the Supplier, or (ii) subcontractors to subcontractors of the Supplier down the chain, OR (iii) any subsidiaries. If the Supplier does not use any third parties to perform any part of the supply chain that could provide Canada with the proposed Commercially Available Software as a Service, the Supplier is requested to indicate this in their response to this requirement. The Suppliers must indicate where in response the reference material can be found, including the title of the document, and the page and paragraph numbers.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance
M11	**Supply Chain Risk Management**	The Supplier of the proposed Commercially Available Software as a Services 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 Services. This includes, but is not limited to 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.	The Supplier must demonstrate how the Supplier of the proposed Commercially Available Software as a Service complies with the requirements in the Supply Chain Risk Management Requirements as documented under the Supplier Information Technology Security Assessment program. To be considered compliant, the provided documentation must demonstrate that the Commercially Available Software as a Service supply chain risk management approach aligns with one of the following best practices. 1. ISO/IEC 27036 Information technology -- Security techniques -- Information security for supplier relationships (Parts 1 to 4); or 2. NIST Special Publication 800-161 - Supply Chain Risk Management Practices for Federal Information Systems and Organizations; or 3. ITSG-33 security control for SA-12 and SA-12(2) where the organized defined security safeguards is documented in a Supply Chain Risk Management (SCRM) plan. The SCRM Plan must describe the Supplier's approach to SCRM and demonstrate how the Suppliers of the proposed Commercially Available Software as a Service will reduce and mitigate supply chain risks. The SCRM Plan must be independently assessed and validated by an independent third party certified under AICPA or CPA Canada, and/or ISO certification regime. The Suppliers must indicate where in response the reference material can be found, including the title of the document, and the page and paragraph numbers.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance
M12	**Privacy**	The Supplier of the proposed Commercially Available Software as a Service must demonstrate that it is compliant with the privacy policies, procedures, and provisions that meet the following industry certification: a) ISO/IEC 27018:2014 Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors. Please note: Suppliers are advised that subsequent procurement Streams may require the Supplier to confirm to Canada on a regular basis that the proposed Commercially Available Software as a Service meets the above certification, and that the certification is valid for the full term of the procurement vehicle.	To demonstrate compliance to the certification, the Supplier must provide: a) A copy of the Commercially Available Software as a Service and Cloud Service Provider most recent and ISO 27018 certification documents, which must have been issued within 12 months prior to the Submission date; and b) A copy of the ISO 27018 assessment report for their current Commercially Available Software as a Services and Cloud Service Provider. The Suppliers must indicate where in response the reference material can be found, including the title of the document, and the page and paragraph numbers.
M13	**Privacy by Design**	The Supplier must demonstrate that it: (a) Implements a software development lifecycle that conforms to ISO 27032 and implements privacy by design; (b) Is compliant with the Privacy Management Framework and policy requirements that are specified in the ISO Standard 29100; and (c) (Adheres to the privacy by design 7 foundational principles (see https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf).	The Supplier must provide documentation that demonstrates how the Supplier of the proposed Services complies with the requirements. The Suppliers must indicate where in response the reference material can be found, including the title of the document, and the page and paragraph numbers.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance
M14	**Privileged Access Management**	The Supplier of the proposed Commercially Available Software as a Service must provide system documentation that demonstrates how to the Software as a service is able to meet the following security requirements Privileged Access Management Requirements: (a) Manage and monitor privileged access to the Solution, including the underlying infrastructure, 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; (b) Restrict and minimize access to the Services and Canada's Information Assets to only authorized devices and End Users with an explicit need to have access; (c) Enforce and audit authorizations for access to the Services and Information Assets; (d) Constrain all access to service interfaces that host Assets and Information Assets to uniquely identified, authenticated and authorized End Users, devices, and processes (or services); (e) Implement password policies to protect credentials from compromise by either on-line 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 credentials, and (iii) access to and exfiltration from the password database, in accordance with CSE's ITSP.30.031 V2 (or subsequent versions) (https://www.cse-cst.gc.ca/en/node/1842/html/26717); (f) Implement multi-factor authentication mechanisms to authenticate (Tier 2 only) End Users with privileged access, in accordance with CSE's ITSP.30.031 V2 (or subsequent versions) (https://www.cse-cst.gc.ca/en/node/1842/html/26717); (g) Implement role-based access control mechanisms to assign privileges which form the basis to enforce access to Assets and Information Assets;	The Supplier must demonstrate compliance by providing documentation outlining the Commercially Available Software as a Service's ability to meet the security requirements related to the Privileged Access Management Requirements: To be considered compliant, the provided documentation must include: a) System documentation or white paper that outlines the policies, processes and procedures used to manage privileged access management. The substantiation required for the Privileged Access Management , the documentation cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Supplier of the proposed Commercially Available Software as a Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the response, it is requested that Suppliers indicate where in Submission the reference material can be found, including the title of the document, and the page and paragraph numbers.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance
		(h) 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; (i) Adhere to the principles of least privilege and need-to-know when granting access to the Services and Assets and Information Assets; (j) Access controls on objects in storage and granular authorization policies to allow or limit access (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 Services and Supplier Infrastructure; (l) Implement an automated process to periodically audit, at a minimum, account creation, modification, enabling, disabling, and removal actions; and (m) Upon the termination of employment, terminate or revoke authenticators and access credentials associated with any Services Personnel.	
M15	**Federation of Identity**	**Federation of Identity** The Supplier must have the ability for Canada to support federated identity integration including: (a) Implement multi-factor authentication mechanisms to authenticate End Users with privileged access, in accordance with CSE's ITSP.30.031 V2 (or subsequent versions) (https://www.cse-cst.gc.ca/en/node/1842/html/26717); (b) Support for Security Assertion Markup Language (SAML) 2.0 and OpenID Connect 1.0 where the End User credentials and authentication to cloud services are under the sole control of Canada; and	The Supplier must provide documentation that demonstrates how the Supplier of the proposed Services complies with the requirements in the Federation of Identity. To be considered compliant, the provided documentation must include: a) System documentation or technical documentation outlining and detailing the security measures including policies, processes and procedures that are implemented for the protection of Federation of Identity. The substantiation required for in the Federation of Identity cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Commercially Available Software as a Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. The

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance
		(c) 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).	Suppliers must indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Submission, it is requested that Suppliers indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers.
M16	**Endpoint Protection**	**Endpoint Protection** The Supplier must implement, manage, and monitor security-hardened endpoints to prevent against 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.	The Supplier must provide documentation that demonstrates how the Supplier of the proposed Services complies with the requirements in the Endpoint Protection. To be considered compliant, the provided documentation must include: a) System documentation or technical documentation outlining and detailing the security measures including policies, processes and procedures that are implemented for Endpoint Protection. The substantiation required for in the Endpoint Protection the documentation cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Commercially Available Software as a Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. The Suppliers must indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Submission, it is requested that Suppliers indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance
M17	**Secure Development**	**Secure Development** The Supplier 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 (i) NIST, (ii) ISO, (iii) ITSG-33, (iv) SAFECode, or (v) Open Web Application Security Project (OWASP) standards such as Application Security Verification Standard (ASVS) or an equivalent standard approved by Canada in writing.	The Supplier must provide documentation that demonstrates how the Supplier of the proposed Services complies with the requirements in the Secure Development. To be considered compliant, the provided documentation must include: a) System documentation or technical documentation outlining and detailing the security measures including policies, processes and procedures that are implemented for the Secure Development. The substantiation required for in the Secure Development, the documentation cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Commercially Available Software as a Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. The Suppliers must indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Submission, it is requested that Suppliers indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers.
M18	**Supplier Remote Management**	**Supplier Remote Management** The Supplier must manage and monitor remote administration of the Supplier's 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 CSE's ITSP.30.031 V2 (or subsequent versions) (https://www.cse-cst.gc.ca/en/node/1842/html/26717); (b) Employ a CSEC Approved Cryptographic Algorithmscryptographic mechanisms to protect the confidentiality of remote access sessions; (c) Route all remote access through controlled, monitored, and audited access control points;	The Supplier must provide documentation that demonstrates how the Supplier of the proposed Services complies with the requirements in the Supplier Remote Management. To be considered compliant, the provided documentation must include: a) system documentation or technical documentation outlining and detailing the security measures including policies, processes and procedures that are implemented for the Supplier Remote Management The substantiation required for in the Supplier Remote Management, the documentation cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Commercially Available Software as a Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. The Suppliers must indicate where in the

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance
		(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.	Submission the reference material can be found, including the title of the document, and the page and paragraph numbers. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Submission, it is requested that Suppliers indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers.
M19	**Information Spillage**	**Information Spillage** (1) The Supplier 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 Supplier'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. (d) The supplier will confirm a point of contact, proper procedures and an agreed upon secure	The Supplier must provide documentation that demonstrates how the Supplier of the proposed Services complies with the requirements in Information Spillage. To be considered compliant, the provided documentation must include: a) System documentation or technical documentation outlining and detailing the security measures including policies, processes and procedures that are implemented for the protection of Information Spillage. The substantiation required for in the Information Spillage, the documentation cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Commercially Available Software as a Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. The Suppliers must indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Submission, it is requested that Suppliers indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance
		form of communication to provide assistance where practicable for customer administrators. (2) Upon request of Canada, the Supplier must provide a document that describes the Supplier's Information Spillage Response Process. "Information Spillage (1) The Supplier must provide Canada with a document that outlines the process it follows to respond to an Information Spillage Incident. The process must be aligned with: (i) ITSG-33 Security Control for IR-9 Information Spillage Submission; or (ii) another best practice of Leading Service Providers approved by Canada in writing. Notwithstanding the foregoing, the Supplier's Information Spillage process must include, at a minimum: (a) A process for identifying the specific Information Asset that is involved in an Asset's or System's contamination; (b) A process to isolate and eradicate a contaminated Asset or System; and (c) A process for identifying Assets or Systems that may have been subsequently contaminated and any other actions performed to prevent further contamination. (2) The Supplier must provide an up-to-date information spillage process to Canada on an annual basis, or promptly following any Change to the Supplier's information spillage process.	

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance
M20	Cryptographic Protection	**Cryptographic Protection** The Supplier must provide Canada with a document that outlines the process it follows to respond to an Information Cryptographic Protection. (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 key sizes and crypto periods; (b) Use cryptographic algorithms and cryptographic key sizes and crypto periods that have been validated by the Cryptographic Algorithm Validation Program (http://csrc.nist.gov/groups/STM/cavp/), and are specified in ITSP.40.111 Cryptographic Algorithms for Unclassified, Protected A, and Protected B Information, or subsequent versions (https://cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-and-protected-b-information-itsp40111); (c) Ensure that FIPS 140 validated cryptography is employed when encryption is required, and is implemented, configured, and operated in a Cryptographic Module, validated by the Cryptographic Module Validation Program (https://www.cse-cst.gc.ca/en/group-groupe/crypto-module-validation-program), in an either approved or an allowed mode to provide a high degree of certainty that the FIPS 140-2 validated cryptographic module is providing the expected security services in the expected manner; and (d) Ensure that any FIPS 140-2 modules in use have an active, current, and valid certification. FIPS 140 compliant/validated products will have certificate numbers.	The Supplier must provide documentation that demonstrates how the Supplier of the proposed Services complies with the requirements in Cryptographic Protection To be considered compliant, the provided documentation must include: a) system documentation or technical documentation outlining and detailing the security measures including policies, processes and procedures that are implemented for Cryptographic Protection The substantiation required for in the Cryptographic Protection, the documentation cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Commercially Available Software as a Service meets the requirement. Suppliers can provide screen captures and technical or end-user documentation to supplement their responses. The Suppliers must indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers. Where Canada determines that the substantiation is not complete, the Supplier will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Submission, it is requested that Suppliers indicate where in the Submission the reference material can be found, including the title of the document, and the page and paragraph numbers.

Schedule C – Privacy Obligations

1. General

The EAPIMS will not be used to store or manage clinical or other medical data that can be identified with a specific individual. Only reporting and statistical data required for the management and administration of the program will be retained in the EAPIMS environment. All clinical or other medical data will be held solely by the clinical practitioners who are providing services and to whom program clients have been referred.

(a) Purpose

The purpose of this Schedule is to set forth the obligations of the Supplier relating to the proper management of Assets and Information Assets, in order to protect such Assets and Information Assets from unauthorized modification, access or exfiltration, all in accordance with the Contract, this Schedule, the Supplier's Specific Privacy Measures, and Canada's Privacy Policies (collectively, the "**Privacy Obligations**").

(b) Flow-Down of Privacy Obligations

The obligations of the Supplier contained in these Privacy Obligations must be flowed down by the Supplier to Supplier Sub-processors, to the extent applicable to each Supplier Sub-processor, given the nature of the services provided by it to the Supplier.

(c) Change Management

The Supplier must, throughout the Contract, take all steps required, through the Change Management Procedures, to update and maintain the Privacy Requirements as needed to comply with the privacy practices of industry standards, provided that if these Changes can reasonably be accommodated with no additional resources, the Supplier must perform such Changes at no additional cost to Canada (i.e. via a zero cost Change Order).

The Supplier must advise Canada of all improvements that affect the Services in this Contract, including technological, administrative or other types of improvements. The Supplier agrees to offer all improvements it is offering to its customers at large as part of its standard service offering at no additional cost to Canada.

2. Acknowledgments

The parties acknowledge that:

(a) All Assets and Information Assets are subject to these Privacy Obligations.

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

(c) The Supplier must not have or attempt to gain custody of any Information Asset, nor permit any Services Personnel to access any Information Asset prior to the implementation of the Privacy Requirements as required under this Schedule on or before the **[Go Live Date]**.

3. Protecting Information Assets

(a) Canada's Data including all Personal Information (PI) will be used or otherwise processed only to provide Canada the Services including purposes compatible with providing those services. The Supplier must not use or otherwise process Canada's Data or derive information from it for any advertising or similar commercial purposes. As between the parties, Canada retains all right, title and interest in and to Customer Data. The Supplier acquires no rights in Customer Data, other than the rights Customer grants to the Supplier to provide the Services to Customer.

4. Third-Party Assurance: Certifications

(a) The Supplier must ensure that in respect of any personal information that it may host, store or process, on all Assets, Supplier Infrastructure (including any IaaS, PaaS or SaaS Service provided to Canada) and Service Locations conform to the following industry certifications:

(i) ISO/IEC 27018:2014 Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors – Certification achieved by an accredited certification body.

(b) The Supplier must demonstrate compliance to this certifications by providing independent third party assessment reports or certifications for all portions of the Service.

(c) Each certification provided must: (i) identify the legal business name of the Supplier or applicable Supplier Sub-processor; (ii) identify the Supplier's or Supplier Sub-processor's including Cloud Service Provider certification date and the status of that certification; (iii) identify the list of Assets, Supplier Infrastructure, and Service Locations 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.

(d) Each ISO certification provided under this section must be valid throughout the contract, within the 12 months prior to the start of the contract. Certifications must be accompanied by supporting ISO assessment reports.

(e) The Supplier must maintain the currency of its certification to the standards described in Subsection 5(1) throughout the contract. The Supplier must provide, at least annually, and promptly upon the request of the Canada, all reports or records that may be reasonably required to demonstrate that the Supplier's certifications remain current, and is valid for the duration of the contract.

5. Privacy Compliance

(a) The Supplier must demonstrate through third party assessment reports and audit reports that it:

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

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

(b) This applies to all information, data and metadata in the Suppliers possession or under its care acquired pursuant to, or arises in any other way out of 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.

6. Auditing Compliance

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

(b) Within 30 days of contract award, the Contractor must engage a third party to conduct a privacy audit or provide evidence to confirm that it does not generate, collect, use, store or disclose any additional personal information as defined by Canada, other than Customer data as defined by the Contractor and does not specifically have PII in Support Data (collected in logs (e.g., telemetry data such as email message headers and content).

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

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

(ii) 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

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

(d) Each audit will result in the generation of an audit report that must be shared with Canada. The audit report must clearly disclose any material findings by the auditor. The Supplier must promptly remediate issues raised in any audit report to the satisfaction of the auditor, and must (i) provide Canada with the plan to correct any negative findings arising from such reports and (ii) provide implementation progress reports to Canada upon request within ten Federal Government Working Days.

(e) Upon request of Canada, additional supplementary evidence from the Supplier, including System security plans, designs, or architecture documents that provide a comprehensive System description, may be provided by the Supplier or a Supplier Sub-processor to supplement the certification and audit reports described in this in order to demonstrate the Supplier's compliance with the required industry certifications.

7. Privacy by Design

The Supplier must demonstrate that it:

(a) Implements a software development lifecycle that conforms to ISO 27032 and implements privacy by design; and

(b) Is compliant with the Privacy Management Framework and policy requirements that are specified in the ISO Standard 29100; and

(c) Adheres to the privacy by design 7 foundational principles (see https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf).

8. Data Ownership and Privacy Requests

(a) Customer Data including all Personal Information (PI) will be used or otherwise processed only to provide Customer the Cloud Service including purposes compatible with providing those services. The Contractor must not use or otherwise process Customer Data or derive information from it for any advertising or similar commercial purposes. As between the parties, Customer retains all right, title and interest in and to Customer Data. The Contractor acquires no rights in Customer Data, other than the rights Customer grants to the Contractor to provide the Cloud Service to the Customer.

(b) All data that it stores, hosts or processes on behalf of Canada remains the property of Canada. When requested by the Contracting

Authority, the Contractor must provide Personal Information records within two Federal Government Working Days (or five Federal Government Working Days if it must be retrieved from offsite backup/replication) in a Word or Excel document.

9. Privacy Officer

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

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

(a) The Supplier must support Canada in creating a privacy impact assessment in accordance with the Treasury Board Directive on Privacy Impact Assessment, by assisting the Canada with the supporting documentation including a foundational PIA for Canada provided by the Supplier. The Supplier agrees to provide this support within five to ten working days of a request or within a mutually agreed upon timeframe depending on the complexity of the request by the Canada.

11. Privacy Breach

(a) The Supplier must alert and promptly notify the Technical Authority (via phone and email) of any compromise, breach or of any evidence that leads the Cloud Service Provider to reasonably believe that risk of compromise, or a 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 within the Cloud Service Provider's service level commitments.

(b) If the Supplier becomes aware of a 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 Supplier (each a "Security Incident"), the Supplier 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 reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

(c) The Supplier must:

(i) 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, and the procedure for recovering data; and

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

12. Ownership of Personal Information and Records

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

13. Use of Personal Information

(a) The foreign recipient **Contractor/Subcontractor** agrees to create, collect, receive, manage, access, use, retain and dispose of the Personal Information and the Records only to perform the Work in accordance with the **contract/subcontract**.

14. Collection of Personal Information

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

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

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

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

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

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

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

(b) The foreign recipient **Contractor/Subcontractor** and their respective employees must identify themselves to the individuals from

whom they are collecting Personal Information and must provide those individuals with a way to verify that they are authorized to collect the Personal Information under a Contract with Canada.

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

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

15. Maintaining the Accuracy, Privacy, and Integrity of Personal Information

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

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

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

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

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

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

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

(g) include a notation on any Record(s) that an individual has requested be corrected if the foreign recipient

Contractor/Subcontractor has decided not to make the correction for any reason. Whenever this occurs, the foreign recipient **Contractor/Subcontractor** must immediately advise the Contracting Authority of the details of the requested correction and the reasons for the foreign recipient **Contractor's/Subcontractor's** decision not to make it. If directed by the Contracting Authority to make the correction, the Contractor must do so;

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

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

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

16. Safeguarding Personal Information

The foreign recipient **Contractor/Subcontractor** must safeguard the Personal Information at all times by taking all measures reasonably necessary to secure it and protect its integrity and confidentiality. To do so, at a minimum, the foreign recipient **Contractor/Subcontractor** must:

(a) store the Personal Information electronically so that a password (or a similar access control mechanism, such as biometric access) is required to access the system or database in which the Personal Information is stored;

(b) ensure that passwords or other access controls are provided only to individuals who require access to the Personal Information to perform the Work;

(c) not outsource the electronic storage of Personal Information to a third party (including an affiliate) unless the Canadian DSA has first consented in writing;

(d) safeguard any database or computer system on which the Personal Information is stored from external access using methods that are generally used, from time to time, by prudent public and private sector organizations in Canada in order to protect highly secure or sensitive information;

(e) maintain a secure back-up copy of all Records, updated at least weekly;

(f) implement any reasonable security or protection measures requested by Canada from time to time; and

(g) notify the Contracting Authority and the Canadian DSA immediately of any security breaches; for example, any time an unauthorized individual accesses any Personal Information.

17. Statutory Obligations

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

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

18. Legal Requirement to Disclose Personal Information

(a) Before disclosing any of the Personal Information pursuant to any applicable legislation, regulation, or an order of any court, tribunal or administrative body with jurisdiction, the foreign recipient **Contractor/Subcontractor** must immediately notify the Contracting Authority, in order to provide the Contracting Authority with an opportunity to participate in any relevant proceedings.

19. Complaints

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

20. Exception

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

Schedule D – Security Obligations

1. General

(a) Purpose

The purpose of this Schedule is to set forth the obligations of the Contractor/Subcontractor relating to the proper configuration and management of Assets and Information Assets, in order to protect such Assets and Information Assets from unauthorized modification, access or exfiltration, all in accordance with the contract, this Schedule, the Supplier's Specific Security Measures, and Canada's Security Policies (collectively, the "Security Obligations").

(b) Flow-Down of Security Obligations

The obligations of the Supplier contained in these Security Obligations must be flowed down by the Supplier to Supplier Sub-processors, to the extent applicable to each Supplier Sub-processor, given the nature of the services provided by it to the Supplier.

(c) Change Management

The Supplier must, throughout the Contract, take all steps required, through the Change Management Procedures, to update and maintain the Security Requirements as needed to comply with the security practices of industry standards, provided that if these Changes can reasonably be accommodated with no additional resources, the Supplier must perform such Changes at no additional cost to Canada (i.e. via a zero cost Change Order).

The Supplier must advise Canada of all improvements that affect the Services in this Contract, including technological, administrative or other types of improvements. The Supplier agrees to offer all improvements it is offering to its customers at large as part of its standard service offering at no additional cost to Canada.

2. Acknowledgments

The parties acknowledge that:

(a) All Assets and Information Assets are subject to these Security Obligations.

(b) Notwithstanding any other provision of this Schedule, the parties have shared responsibility for developing and maintaining policies, procedures and security controls relating to Assets and Information Assets.

(c) The Supplier must not have or attempt to gain custody of any Information Asset, nor permit any Services Personnel to access any Information Asset prior to the implementation of the Security Requirements as required under this Schedule on or before Contract Award.

(d) Security Obligations apply to both Tier 1 (up to Protected A / Low injury) and for Tier 2 (up to Protected B / Medium injury), unless specified.

3. Securing Information Assets

(a) The Supplier must design its Services to protect Assets and Information Assets from unauthorized access, modification, or exfiltration. This includes implementing and maintaining appropriate information security policies, procedures, and security controls to preserve the confidentiality, integrity, and availability of Assets and Information Assets (hereinafter referred to as the "**Specific Security Measures**").

4. Roles and Responsibilities for Security

(a) The Supplier must clearly delineate the roles and responsibilities for the security controls and features of the Services between the Supplier (any Supplier Sub-processors, as applicable) and Canada. This includes, at a minimum, the parties' 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.

(b) The Supplier must provide to Canada an up-to-date document that delineates the roles and responsibilities between the Supplier, Supplier Sub-processors, and Canada for security controls and features: (i) on an annual basis; (ii) when there are significant changes to such roles and responsibilities as a result of a Change to the Services; or (iii) upon request of Canada.

5. Third-Party Assurance: Certifications and Reports

(a) The Supplier must ensure that all Assets, Supplier Infrastructure (including any IaaS, PaaS or SaaS Service provided to Canada) and Service Locations are secured in accordance with industry certifications and audit reporting.

(b) For **Tier 1**, the Supplier must demonstrate compliance to the following certifications and audit reports by providing independent third party assessment reports or certifications for ALL portions of the Service:

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

(ii) 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

(iii) Self-assessment of its services against the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) version 3.01 or subsequent version.

(c) The Supplier must demonstrate compliance to the following certifications and audit reports by providing independent third party assessment reports or certifications for ALL portions of the Service:

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

(ii) ISO/IEC 27017:2015 Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services achieved by an accredited certification body; **AND**

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

(d) The Supplier must demonstrate compliance to these certifications and audit reports by providing independent third party assessment reports or certifications for all portions of the Service.

(e) Each certification or audit report provided must: (i) identify the legal business name of the Supplier or applicable Supplier Sub-processor; (ii) identify the Supplier's or Supplier Sub-processor's certification date and the status of that certification; (iii) identify the list of Assets, Supplier Infrastructure, and Service Locations 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.

(f) Each ISO certification provided must be valid throughout the contract, within the 12 months prior to the start of the contract. Certifications must be accompanied by supporting evidence such as the ISO assessment report developed to validate compliance to the ISO certification.

(g) Each SOC audit report must have been performed within the 12 months prior to the start of the contract.

(h) The Supplier must maintain the currency of its certification to the standards described in Subsection 5(1) throughout the contract. The Supplier must provide, at least annually, and promptly upon the request of the Canada, all reports or records that may be reasonably required to demonstrate that the Supplier's certifications remain current, and is valid for the duration of the contract.

6. Auditing Compliance

(a) The Supplier must conduct the privacy and security audits of the security of the computers, computing environment and physical data centers that it uses in processing and protecting Assets and Information Assets as follows:

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

(ii) 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

(iii) Each audit will be performed by qualified, independent, third party auditor 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 Supplier's selection and expense.

(b) Each audit will result in the generation of an audit report that must be shared with Canada. The audit report must clearly disclose any material findings by the third party auditor. The Supplier must promptly remediate issues raised in any audit report to the satisfaction of the auditor, and must (i) provide Canada with the plan to correct any negative findings arising from such reports and (ii) provide implementation progress reports to Canada upon request within ten (10) Federal Government Working Days.

7. IT Security Assessment Program

(a) In addition to the industry certifications described in Section 5 (Third-Party Assurance: Certifications and Reports), the Supplier must demonstrate compliance with the security requirements selected in the GC Security Control Profile for Cloud-Based GC IT Services available (https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/cloud-computing/government-canada-security-control-profile-cloud-based-it-services.html) or subsequent version ,for the scope of the Services provided by the Supplier. Compliance must be demonstrated through the mapping of security controls to the applicable industry certifications identified below, and validated through independent third party assessments.

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

Any Supplier that has participated in the process must provide documentation to confirm that they have completed the on-boarding process with (i) a copy of the most recent completed assessment report provided by CCCS; and (ii) a copy of the most recent summary report provided by CCCS.

To initiate the on-boarding process, the Supplier should contact the CCCS Client Services to receive a copy of the onboarding submission form and any additional information related to the CSP IT Assessment Program.

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

8. Data Protection

(a) The Supplier must:

(i) Implement encryption of data at rest for all Information Assets.

(ii) Take reasonable measures to ensure that encryption of data at rest remains in effect, uninterrupted, and active at all times, even in the case of equipment or technology failure.

(iii) Transmit Information Assets in a secure manner. This includes implementing encryption for data in transit for all transmissions of Assets and Information Assets.

(iv) Implement security controls that restricts administrative access to Information Assets and Systems by the Supplier and provides the ability to require the approval of Canada before the Supplier can access Information Assets to perform support, maintenance or operational activities using Information Assets that consist of Canada data.

(v) Take reasonable measures to ensure that Services Personnel do not have standing or ongoing access rights to Information Assets, and access is restricted to those who must access Assets and Information Assets to provide technical or customer support based on approval from Canada.

(b) The Supplier must not make any copies of databases or any part of those databases containing Information Assets, and must not move or transmit approved copies to any location, except when approval is obtained from Canada.

9. Data Isolation

The Supplier must implement controls to ensure appropriate isolation of resources such that Information Assets are not co-mingled with other tenant data, while in use, storage or transit, and throughout all aspects of the Supplier's Service's and Supplier Infrastructure's functionality and system administration. This includes implementing access controls and enforcing appropriate logical or physical segregation to support:

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

(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.

10. Data Location

(a) The Supplier must have the ability for Canada to store and protect its Information Assets, 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:

(i) A data centre that meets all security requirements and certifications identified in Section 32 for Physical (Data Centre / Facilities) Security

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

(b) Employs encryption to ensure that no data is written to disk in an unencrypted form.

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

(d) The Supplier must have the ability for Canada to isolate Assets and Information Assets in data centers that are geographically located in Canada.

(e) Upon request, the Supplier must:

(i) Provide the GC with an up-to-date list of the physical locations, including city, which may contain Assets and Information Assets for each data centre that will be used to provide Services; and

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

(f) It is the continuous obligation of the Supplier of the proposed Services to notify Canada when there are updates to the list of physical locations which may contain Assets and Information Assets.

11. Data Transfer and Retrieval

The Supplier must, upon request by Canada:

(a) Extract all online, nearline, and offline 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 user can use these instructions to migrate from one environment to another environment; and

(b) Securely transfer all Information Assets, including metadata, in a machine-readable and usable format acceptable to Canada, in accordance with the Library and Archives Canada Guidelines on File Formats for Transferring Information Resources of Enduring Value (https://www.bac-lac.gc.ca/eng/services/government-information-resources/guidelines/Pages/guidelines-file-formats-transferring-information-resources-enduring-value.aspx).

12. Data Disposition and Returning Records to Canada

(a) The Supplier must upon request, securely dispose or reuse resources (e.g. equipment, data storage, files, and memory) that contain Information Assets and ensure that previously stored data cannot be addressed by others customers after it is released. This includes all copies of Information Assets that are made through replication for high availability and disaster recovery. The Supplier's disposal or reuse of resources must be aligned with one of the following: (i) National Industrial Security Program Operating Manual (DoD 5220.22-M6); (ii) Guidelines for Media Sanitization (NIST SP 800-88); or (iii) Clearing and Declassifying Electronic Data Storage Devices (CSE ITSG-06).

(b) The Supplier must provide evidence 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 removed from the Canada instance.

13. Cryptographic Protection

The Supplier 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 key sizes and crypto periods;

(b) Use cryptographic algorithms and cryptographic key sizes and crypto periods that have been validated by the Cryptographic Algorithm Validation Program (http://csrc.nist.gov/groups/STM/cavp/), and are specified in ITSP.40.111 Cryptographic Algorithms for Unclassified, Protected A, and Protected B Information, or subsequent versions (https://cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-and-protected-b-information-itsp40111);

(c) Ensure that FIPS 140 validated cryptography is employed when encryption is required, and is implemented, configured, and operated in a Cryptographic Module, validated by the Cryptographic Module Validation Program (https://www.cse-cst.gc.ca/en/group-groupe/crypto-module-validation-program), in an either approved or an allowed mode to provide a high degree of certainty that the FIPS 140-2 validated cryptographic module is providing the expected security services in the expected manner; and

(d) Ensure that any FIPS 140-2 modules in use have an active, current, and valid certification. FIPS 140 compliant/validated products will have certificate numbers.

14. Key Management

The Supplier must provide Canada with a key management service that enables:

(a) Creation/generation and deletion of encryption keys by the GC;

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

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

(d) Audits all events related to key management services, including Supplier access for Canada's review.

15. Access Control

The Supplier must have the ability for Canada to support secure access to Services including ability to configure:

(a) multi-factor authentication in accordance with CSE's ITSP.30.031 V2 (or subsequent versions) (https://www.cse-cst.gc.ca/en/node/1842/html/26717) 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.

16. Privileged Access Management

The Supplier must provide documentation that demonstrate how to Software as a service is able to meet the following security requirements:

(a) 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;

(b) Restrict and minimize access to the Services and Canada's Information Assets to only authorized devices and End Users with an explicit need to have access;

(c) Enforce and audit authorizations for access to the Services and Information Assets;

(d) Constrain all access to service interfaces that host Assets and Information Assets to uniquely identified, authenticated and authorized End Users, devices, and processes (or services);

(e) Implement password policies to protect credentials from compromise by either on-line 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 CSE's ITSP.30.031 V2 (or subsequent versions) (https://www.cse-cst.gc.ca/en/node/1842/html/26717);

(f) Implement multi-factor authentication mechanisms to authenticate End Users with privileged access, in accordance with CSE's ITSP.30.031 V2 (or subsequent versions) (https://www.cse-cst.gc.ca/en/node/1842/html/26717);

(g) Implement role-based access control mechanisms to assign privileges which form the basis to enforce access to Assets and Information Assets;

(h) 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;

(i) Adhere to the principles of least privilege and need-to-know when granting access to the Services and Assets and Information Assets;

(j) 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 Services and Supplier Infrastructure;

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

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

17. Master / Root Account Management

The Supplier must ensure the adequate protection of the account management and billing management process used to establish the Security measures include but is not limited to:

(a) Limiting access to only authorized users who are permitted to execute transactions and functions such as Master account creation and issuance, and billing and invoicing;

(b) Ensuring the separation of duties of individuals;

(c) Employing the principle of least privilege, including for specific security functions and privileged accounts;

(d) Ensuring that authorized users are provided with security awareness and training as part of employment onboarding and when their roles change and are made aware of the security requirements associated with the contract.

(e) Creating, protecting, and retaining audit records related to the activities that support account management of Services provisioned to Canada;

(f) Providing Canada with reports on audited events for actions related to the issuance and management of Master accounts used by personnel to manage GC accounts;

(g) Implementing security measures that grant and maintain the required level of security screening for personnel supporting the management of Master accounts linked to Canada, in accordance with the SRCL; and

(h) Ensuring that Assets and Information Assets are protected during and after personnel actions such as terminations and transfers.

18. Federation

The Supplier must have the ability for Canada to support federated identity integration including:

(a) Support for Security Assertion Markup Language (SAML) 2.0 and OpenID Connect 1.0 where the End User credentials and authentication to cloud services are under the sole control of Canada; and

(b) 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. Endpoint Protection

(a) The Supplier must implement, manage, and monitor security-hardened endpoints to prevent against 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.

20. Secure Development

(a) The Supplier 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 (i) NIST, (ii) ISO, (iii) ITSG-33, (iv) SAFECode, or (v) Open Web Application Security Project (OWASP) standards such as Application Security Verification Standard (ASVS) or an equivalent standard approved by Canada in writing.

21. Application Programming Interface (API)

The Supplier must:

(a) Provide Services that uses open, published, supported, and documented Application Programming Interfaces (API) to support interoperability between components and to facilitate migrating applications.

(b) Take reasonable measures to protect both internal and external APIs through secure authentication methods. This includes ensuring that all externally exposed API queries require successful authentication before they can be called.

(c) For SaaS, the Supplier must provide APIs that provide the ability to:

(i) Interrogate data at rest in the applications; and

(ii) Assess events and incidents stored in SaaS application logs.

22. Network and Communications Security

The Supplier must:

(a) Provide the ability for Canada to establish secure connections to the Services, including providing data-in-transit protection between Canada and the Service using TLS 1.2, or subsequent versions, and using supported cryptographic algorithms and certificates, as outlined in CSE'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-and-protected-b-information-itsp40111);

(b) Provides data-in-transit protection between microservices and applications used within the Services;

(c) Use correctly configured certificates within the TLS connections in accordance with CSE guidance.

(d) Disable known-weak protocols such as all versions of Secure Sockets Layer (SSL) (e.g. SSLv2 and SSLv3) and older versions of TLS (e.g. TLS 1.0 and TLS 1.1), as per CSE ITSP.40.062, and known-weak ciphers (e.g. RC4 and 3DES); and

(e) Provide the ability for Canada to implement network access controls and security rules that allow or deny network traffic to Canada resources.

23. Dedicated Connections

The Supplier must provide the ability for the GC to establish private redundant connectivity to the Services. This includes:

(a) Establishing connectivity either directly into the GC Wide Area Network (WAN) or via GC Cloud Exchange Provider located at 151 Front in Toronto and/or 625 Rene Levesque in Montreal;

(b) Enabling full backup and disaster recovery services through redundant connections within and across Contractor data centers;

(c) Physical connectivity links that are optical, and that provide a minimum of 10Gbps with the option to bundle additional 10G links up to 40G, with optional 100G connectivity;

(d) Support for virtualization and multi-tenancy for all network components;

(e) Support for dynamic routing protocols (BGP) for all connections;

(f) Support for GC-approved protocols as outlined in:

i. ITSP.40.062 Guidance on Securely Configuring Network Protocols, Section 3.1 for AES cipher suites
ii. ITSP.40.111 Cryptographic Algorithms for Unclassified, Protected A, and Protected B Information

(g) Provide a description of all the data centre geographical locations in Canada where the capability is available.

24. Logging and Auditing

(a) The Supplier must implement log generation and management practices and controls for all Service components that store or process Assets and Information Assets, and that conform with the practices of Leading Service Providers, such as those found in NIST 800-92 (Guide to Computer Security Log Management), or an equivalent standard approved by Canada in writing.

(b) The Supplier must enable Canada to centrally review and analyze audit records from multiple components within the Services provided by the Supplier. This includes the ability for Canada to:

(i) 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;

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

(iii) 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 Service provided to it by the Supplier or a Supplier Sub-processor; and

(iv) forward Canada tenant events and logs to a GC-managed centralized audit log system 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.).

25. Continuous Monitoring

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

(i) Actively and continuously monitor threats and vulnerabilities to its Assets, Supplier Infrastructure, Service Locations, or Information Assets;

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

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

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

(v) 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 Services or libraries that the Services make use of, and provide advance notices of patches in accordance with agreed-upon service level commitments;

(vi) Respond, contain, and recover from threats and attacks against the Supplier Services; and

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

(b) The Contractor's 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).

(c) The Contractor's Services must allow Canada to deploy and operate security software to perform advanced monitoring and mitigations of cyber threats for Canada's Services at the Canada managed host and network layer, for Canada managed components only.

26. Notifications

The Supplier must provide:

(a) Timely notification of any interruption that is expected to impact service availability and performance (as agreed to by the parties and included in the SOW and/or SLA);

(b) Regular updates on the status of returning the services to an operating state according to the agreed upon SLAs and system availability requirements, both as advance alerts and post-implementation alerts; and

(c) Information system security alerts, advisories, and directives via email for vulnerabilities that pose a threat to the Services.

27. Security Incident Management

(a) The Supplier's Security Incident response process for the Services must encompass the IT security incident management lifecycle and supporting practices for preparation, detection, analysis, containment, and recovery activities, 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/treasury-board-secretariat/services/access-information-privacy/security-identity-management/government-canada-cyber-security-event-management-plan.html); or (iv) other best practices of Leading Service Providers if Canada determines, in its discretion, that they meet Canada's security requirements.

(b) The Supplier's Security Incident response process must include the following:

(i) A documented process and procedures of how the Supplier will identify, respond, remediate, report, and escalate Security Incidents to Canada, including: (i) the scope of the Security Incidents that the Supplier must report to Canada; (ii) the level of disclosure and the measures used by the Supplier for detection of Security Incidents, and the Supplier's associated responses for specific types of Security Incident; (iii) the target timeframe in which notification and escalation of Security Incidents will occur; (iv) the procedure for the notification and escalation of Security Incidents; (v) contact information for the handling of issues relating to Security Incidents; and (vi) any remedies that apply if certain Security Incidents occur.

(ii) Procedures for responding to requests for potential digital evidence or other information from within the Supplier's service environment or Supplier Infrastructure, including forensic procedures and safeguards for the maintenance of a chain of custody over Information Assets stored or processed by the Supplier or a Supplier Sub-processor. Forensic and digital evidence practices and controls must conform with the practices of Leading Service Providers, such as those found in NIST 800-62 (Guide to Integrating Forensic Techniques into Incident Response), ISO 27037 (Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence), or an equivalent standard approved by Canada in writing.

28. Security Incident Response

(a) The Supplier must alert and promptly notify Canada (via phone and email) of any compromise, breach or of any evidence such as (i) a security incident, (ii) a security multifunction 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 Supplier, that leads the Supplier 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 24 hours.

(b) If the Supplier becomes aware of a 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 Supplier (each a "Security Incident"), the Supplier 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 reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

(c) The Supplier must collaborate with Canada on the containment, eradication, and recovery of Security Incidents in accordance with the Supplier's Security Incident response process and in alignment with the GC Cyber Security Event Management Plan (GC CSEMP) (https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/government-canada-cyber-security-event-management-plan.html). This includes:

(i) Allowing only designated representatives of Canada to have the ability to:

i. request and receive information associated with the Security Incident and any compromised Information Assets (including 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. track the status of a reported information security event or Security Incident.

(ii) Supporting Canada's investigative efforts in the case of any compromise of the users or data in the service that is identified.

(d) The Supplier must:

(i) 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, and the procedure for recovering data or the service; and

(ii) Track, or enable Canada to track, disclosures of Assets and Information Assets, including what data has been disclosed, to whom, and at what time.

29. E-discovery and Legal Holds

(a) The Supplier must (and must, to the extent applicable given the nature of the subcontracted services provided by each Supplier Sub-processor, require Supplier Sub-processors to) take reasonable measures to ensure the Services provides e-discovery and legal hold features for the Security Event Logs in order to enable Canada to conduct timely and effective security investigations and meet legal court requests for legal holds.

30. Penetration Testing

(a) The Supplier must have a process that allows Canada to conduct a non-disruptive and non-destructive Vulnerability Scan or Penetration Test of Canada's portion of the Service components within the Supplier environment.

31. Security Screening

(a) The Supplier must (and must, to the extent applicable given the nature of the subcontracted services provided by each Supplier Sub-processor, require Supplier Sub-processors to):

(i) Undertake employee due-diligence screening for all Services Personnel prior to their receiving authorization to access Supplier Systems or Information Assets; and

(ii) Implement security measures that grant and maintain the required level of security screening for Services Personnel pursuant to their access privileges to Systems on which Information Assets are stored and processed.

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

(i) A description of the employee and Sub-processor positions that require access to Information Assets or have the ability to affect the confidentiality, integrity or availability of an Information Asset;

(ii) A process for security screening, including notification procedures that need to be followed if screening has not been completed or if the results give cause for doubt or concern;

(iii) A process for ensuring that employees and Sub-processors understand, are aware of, and fulfil, their responsibilities for information security, and are suitable for the roles for which they are considered;

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

(v) A process for security awareness and training as part of employment onboarding and when employee and sub-processor roles change; and

(vi) An approach to detecting potential malicious insiders and controls implemented to mitigate the risk of access to GC data and/or affect on the reliability of cloud services hosting GC assets and data.

32. Physical (Data Centre / Facilities) Security

The Supplier must implement physical security measures that ensure the protection of IT facilities and information system assets on which Assets and Information Assets are stored and processed against all forms of tampering, loss, damage, and seizure. Physical protection of all facilities that host GC data and information assets, 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 Royal Canadian Mounted Police (RCMP) guidance and standards on physical security. The security measures required under this include, at a minimum:

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

(b) Proper handling of IT Media;

(c) Controlled maintenance of all assets and 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 GC data and Information Assets;

(e) Controlling and managing physical access devices;

(f) Limiting physical access to Assets and Service Locations to authorized Services Personnel based on position or role and the need-to-access principle, and validated by two forms of identification;

(g) Escorting visitors and monitoring visitor activity;

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

(i) Recording and monitoring all physical access to Service Locations and all logical access to Systems hosting data and information systems, using a combination of access logs and surveillance and intrusion detection mechanisms.

33. Supply Chain Risk Management

(b) The Supplier of the Services 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 Services. This includes, but is not limited to 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.

(c) The Supplier must provide Canada with a "**Supply Chain Risk Management (SCRM) Plan**" that describes the Supplier's approach to supply chain risk management (SCRM) and demonstrates how the Supplier's approach to SCRM will reduce and mitigate supply chain risks. The SCRM Plan must be aligned with one of the following best practices and be assessed and validated by an independent third party certified under AICPA or CPA Canada, and/or ISO certification regime: (i) ISO/IEC 27036 Information technology -- Security techniques -- Information security for supplier relationships (Parts 1 to 4); (ii) NIST Special Publication 800-161 -- Supply Chain Risk Management Practices for Federal Information Systems and Organizations; or (iii) ITSG-33 security control for SA-12 where the organization defined security safeguards are documented in an SRCM plan.

(d) Notwithstanding the foregoing, the Supplier's SCRM Plan must include, at a minimum:

(i) A process to specify and design Supplier Infrastructure and Systems following security engineering processes so that they are protected against external threats and against Hardware and Software vulnerabilities;

(ii) A process to determine critical functions and the protection techniques (countermeasures and sub-countermeasures) used to achieve System protection for all critical Hardware and Software components in use along the Supplier's entire supply

(iii) The physical and logical delivery mechanisms that will be used by the Supplier and Supplier Sub-processors to protect against Security Incidents;

(iv) The operational processes (during maintenance, upgrade, patching, element replacement, or other sustainment activities) and disposal processes that limit opportunities for Security Incidents;

(v) The relationship between the Supplier and any manufacturer of an Asset as one of the following: (1) OEM; (2) authorized reseller; (3) authorized partner/distributor; or (4) unknown/unidentified source; and

(vi) The Supplier's SCRM training and awareness program.

(e) The Supplier must provide an up-to-date SRCM Plan to Canada on an annual basis, or promptly following any material Change to the SRCM Plan.

(e) The Supplier must provide a list of perimeter protection devices (PPDs) present in the Services environment. The types of IT products that are defined as PPDs are IT devices that can enforce (block/deny or allow) IP traffic based on IP address, IP port or type of IP based protocol deployed at the boundary of the Cloud Service Provider's cloud network. Internal (behind the boundary) perimeter protection devices are excluded from the supply chain PPD review. When requested, the Supplier must provide the GC with a list of perimeter protection devices (PPDs) present in the Services environment within 10 business days of receipt of any request, in a standard format approved by the Technical Authority.

34. Sub-processors

(a) The Supplier 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.

(b) The Supplier 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-processors with access to Customer Data or Personal Data. The Supplier must assist Canada with verification of sub-processors within 10 working days.

Schedule E – Supply Chain Integrity for SaaS Requirements

1. On-going Supply Chain Integrity Process

(a) The Contractor acknowledges that security is a critical consideration for Canada with respect to this Contract and that on-going assessment of Cloud Services will be required with respect to this Contract.

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

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

2. Sub-processors

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

(b) The Contractor must provide a list of Sub-processors prior to Contract award, in accordance with the attached forms. The Contractor must provide Canada notice (by updating the website and providing Customer with a mechanism to obtain notice of that update) of any new Sub-processor at least 14-days in advance of providing that Sub-processors with access to Customer Data or Personal Data.

3. Change of Control

(a) 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 calendar days of receiving the notice from the Contractor regarding the change of control. Canada will not be required to provide its reasons for terminating the 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.

(b) If Canada determines in its sole discretion that a change of control affecting a subcontractor (either in the subcontractor itself or any of its parents, up to the ultimate owner) may be injurious to national security, Canada will notify the Contractor in writing of its determination. Canada will not be required to provide the reasons for its determination, if Canada determines in its discretion that the disclosure of those reasons could itself be injurious to national security. The Contractor must, within 30 calendar days of receiving Canada's determination, arrange for another subcontractor, acceptable to Canada, to deliver the portion of the Cloud Services being delivered by the existing subcontractor (or the Contractor must deliver this portion of the Cloud Services itself). If the Contractor fails to do so within this time period, Canada will be entitled to terminate the Contract on a "no-fault" basis by providing notice to the Contractor within 120 calendar days of receiving the original notice from the Contractor regarding the change of control.

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

(d) 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.

FORM 1

MASTER ITQ SUBMISSION FORM

Respondent Profile

Respondent's Registered Legal Business Name ("Respondent"):	
Street Address:	
City/Province:	
Postal Code:	
Phone Number:	
Parent Organization (if any):	
Names of Board of Directors or Owner(s):	
Procurement Business Number (PBN):	
ITQ Primary Contact Person	Name: Title: Email Address: Telephone Number:
Respondent is an Aboriginal Business as defined in Annex A (Yes / No)	

Respondent Representative

Name and Title of Respondent Representative(s)	
Address	
Telephone Number(s)	
E-Mail Address	
Preferred Language (English or French)	

Respondent Team member

Name and Title of Respondent Team Members	
Company (Registered or Corporate Name)	
Address	
Telephone Number(s)	
E-Mail Address	
Preferred Language (English or French)	

Respondent Team member

Name and Title of Respondent Team Members	
Company (Registered or Corporate Name)	
Address	
Telephone Number(s)	
E-Mail Address	
Preferred Language (English or French)	

Respondent Team member

Name and Title of Respondent Team Members	
Company (Registered or Corporate Name)	
Address	
Telephone Number(s)	
E-Mail Address	
Preferred Language (English or French)	

Respondent Team member

Name and Title of Respondent Team Members	
Company (Registered or Corporate Name)	
Address	
Telephone Number(s)	
E-Mail Address	
Preferred Language (English or French)	

Respondent Team member

Name and Title of Respondent Team Members	
Company (Registered or Corporate Name)	
Address	
Telephone Number(s)	
E-Mail Address	
Preferred Language (English or French)	

Copy the above table if you are proposing more than five (5) team members.

The above named Respondent Representative hereby declares on its own behalf and, for clarity, on behalf of all Respondent Team Members that:

a. it has the power and authority to bind the Respondent for the purpose of the ITQ;

b. the Respondent is a:
   - ☐ a sole proprietor;
   - ☐ a limited liability or general partnership;
   - ☐ a corporation; or
   - ☐ an unincorporated consortium carrying on business under the above mentioned Respondent name

c. if invited to participate in the RFP, the Respondent would prefer to receive correspondence and associated procurement documentation in the following language during the RFP process. Please select just one (1) language as the Respondent's preferred language:
   - ☐ English
   - ☐ French

d. this Master ITQ Submission Form has not been modified in any manner, except to include the Respondent's required information and the Amendment information required by this Form; and

e. the Respondent and its affiliates are in compliance with the Integrity Provisions set in Section 5.1 – Integrity Provisions, of the ITQ. In witness whereof, the Respondent Representative has signed this - Master ITQ Submission Form as of the date indicated below.

Respondent Representative:

Name: _____

Title: _____

Date: _____

_____
Signature

I/We have authority to bind the Respondent Representative and to bind the Respondent and each Respondent Team Member.

Solicitation No. HT300-193651/A

Buyer ID: 052eem

FORM 2

SOFTWARE PUBLISHER CERTIFICATION FORM

(to be used where the Respondent itself is the Software Publisher)

The Respondent certifies that is the software publisher of all the following software products and components and that it has all the rights necessary to license them (and any non-proprietary sub-components incorporated into the software) on a royalty-free basis to Canada:

_____

_____

_____

_____

_____

[*respondent should add or remove lines as needed*]

ITQ Number: _____

Name of the Respondent: _____

Signature of authorized signatory of the Respondent: _____

Print Name of authorized signatory of the Respondent: _____

Title of the authorized signatory of the Respondent: _____

Telephone Number: _____

Solicitation No. Buyer ID:

HT300-193651/A 052eem

Form 3

Software Publisher Authorization Form

(to be used where the Respondent is not the Software Publisher)

This confirms that the software publisher identified below has authorized the Respondent named below to license its proprietary software products under the contract resulting from the bid solicitation identified below. The software publisher acknowledges that no shrink-wrap or click-wrap or other terms and conditions will apply, and that the contract resulting from the bid solicitation (as amended from time to time by its parties) will represent the entire agreement, including with respect to the license of the software products of the software publisher listed below. The software publisher further acknowledges that, if the method of delivery (such as download) requires a user to "click through" or otherwise acknowledge the application of terms and conditions not included in the bid solicitation, those terms and conditions do not apply to Canada's use of the software products of the software publisher listed below, despite the user clicking "I accept" or signalling in any other way agreement with the additional terms and conditions.

This authorization applies to the following software products:

_____

_____

[Respondent should add or remove lines as needed]

Name of Software Publisher (SP) _____

Signature of authorized signatory of SP _____

Print Name of authorized signatory of SP _____

Print Title of authorized signatory of SP _____

Address for authorized signatory of SP _____

Telephone no. for authorized signatory of SP _____

Fax no. for authorized signatory of SP _____

Date signed _____

Solicitation Number _____

Name of Respondent _____