RETURN BIDS TO:

By Email:

nc-solicitations-gd@hrsdc-rhdcc.gc.ca

(Size limit – 13MB)

Attention:
Estelle Benoit

REQUEST FOR PROPOSAL

Proposal To: Employment and Social Development 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 or attached hereto, the goods, services, and construction listed herein and on any attached sheets at the price(s) set out therefor.

Instructions : See Herein

Vendor/Firm Name and address

Title: Organizational Chart Software as a Service (SaaS) Solution and related services **Amendment 3**	
Solicitation No.: 100021358	**Date:** September 6th, 2022
File No. – N° de dossier:	
Solicitation Closes **At 02 :00 PM / 14 h** **On September 12th, 2022**	**Time Zone** Eastern Daylight SavingTime
Address Inquiries to : Estelle Benoit at nc-solicitations-gd@hrsdc-rhdcc.gc.ca	
Destination: See Herein	

Vendor/firm Name and address : **Facsimile No. :** **Telephone No. :**
Name and title of person authorized to sign on behalf of Vendor/firm (type or print): **Name:** **Title:** **Signature:** **Date:**

THE AMENDMENT 1 IS RAISED TO:

1. Change wording throughout the document to conform with the Software as a Service and Cloud language;
2. Change the wording in the Milestones 4 and 5 throughout the document;
3. Change the technical rated criteria R10;
4. Add accessibility information under the clause 4.1.1.2.1;
5. Remove the clause 7.2.2 Supplemental General Conditions and remove its mention from the clause 7.11 Priority of Documents;
6. In the Annex A, ESDC – General Conditions (2022-04-07), remove the clause 20 Copyright and adjust numbering accordingly;
7. In the Annex B, Statement of Work, change the clause 10.1 ESDC Security & Accessibility Requirements in its entirety; and,
8. In the Annex D, Security Requirement Check List (Phase 2), change the SRCL used from a common form to a standard form, *without changing any security clause*.

All changes/additions have been highlighted in Yellow.

THE AMENDMENT 2 IS RAISED TO:

1. Extend the solicitation period, *in order to give us more time to prepare the revised Q&As document, and to make the necessary changes to the RFP*:

On the first page of this RFP, DELETE:

Solicitation Closes
At 02 :00 PM / 14 h
On August 30, 2022

INSERT:

Solicitation Closes
At 02 :00 PM / 14 h
On September 6th, 2022

ALL OTHER TERMS AND CONDITIONS REMAIN THE SAME

THE AMENDMENT 3 IS RAISED TO:

1. Extend the solicitation period:

On the first page of this RFP, DELETE:

Solicitation Closes
At 02 :00 PM / 14 h
On September 6th, 2022

INSERT:

Solicitation Closes
At 02 :00 PM / 14 h
On September 12th, 2022

2. Change wording throughout the document to conform with the Software as a Service and Cloud language (SaaS Solution);
3. Change wording throughout the document to replace the role of Software Expert for Subject Matter Expert;
4. Under the Attachement 1 to Part 3 – Pricing Schedule, add clarifications to the Firm Annual Unit Price table, to answer to Q10.
5. Remove the clause 7.1.1.2 Minimum Work Guarantee - All the Work - Task Authorizations;
6. Change the clause 7.3 Security Requirements – Phase 2 of Contract;
7. Change the clause 7.4.1 Period of the Contract and adjust the pricing tables accordingly;
8. Change the clause 7.7.3 Basis of Payment – Firm Unit Price for the Software as a Service (SaaS) Solution Annual Subscriptions to remove the mention of Task Authorizations;
9. Change the clauses 2.5 and 7.10 Applicable Laws for Ontario instead of Quebec;
10. Change the Statement of Work, in the Annex B, in it's entirety;
11. Change the Electronic Payment Instruments clause, in the Annex E, in it's entirety; and,
12. Add the Annex G Service Level Agreements (SLA) and add its mention in the clause 7.11 Priority of Documents.

All changes/additions have been highlighted in Green.

TABLE OF CONTENTS

PART 1 - GENERAL INFORMATION

1.1 Introduction

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

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

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

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

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

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

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

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

The Annexes include the General Conditions, Statement of Work, the Basis of Payment, the Security Requirements Checklist, the Electronic Payment Instruments, the Task Authorization Form, and the Service Level Agreements.

1.2 Summary

1.2.1 HRSB is requesting an Organization Chart Software as a Service (SaaS) Solution that is automated, with a user-friendly approach for creating, developing and maintaining organization charts. The SaaS Solution must integrate with ESDC's PeopleSoft 9.2 production environment and its processes, and must be able to support, at a minimum, approximately 60,000 positions within ESDC and approximately 10,400 users (Classification Officers and ESDC managers and Administrative Assistants). The SaaS Solution should enable a significant reduction in time and resources to the department and increase department-wide organizational understanding and analysis ability. The SaaS Solution should provide a single source of truth and will allow everyone to access the same organizational picture. The project will unfold in two phases. PHASE 1 - The first phase will be the Minimal Viable Product (MVP) and will only reference Unclassified Data. PHASE 2 - The second phase will contain Classified Data (Protected B). The vendor will need to demonstrate to IT security that they indeed meet the mandatory requirements, including the need for the Bidder to be certified for IT security. The Phase 1 MVP requirement will be to go live with a SaaS Solution for unclassified data by January 2023. Phase 1 is considered as a high priority. Phase 2 requirements is to generate organizational charts for up to Protected B data which will come at a later date, once ESDC is ready to move forward with this phase and the vendor has obtained all necessary security clearances. Under the resulting contract, the vendor will need to provide professional services from a Subject Matter Expert, a Training Expert, and training services. The initial period of the contract is for one (1) year, with six (6) additional option periods of one (1) year.

1.2.2 There are security requirements associated with this requirement for Phase 2 of resulting Contract. For additional information, consult Part 6 - Security, Financial and Other Requirements, Part 7 - Resulting Contract Clauses, and Appendix A to Annex B. For more information on personnel and organization security screening or security clauses, 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.

1.3 Debriefings

Bidders may request a debriefing on the results of the bid solicitation process. Bidders should make the request to the Contracting Authority within 15 working days from receipt of the results of the bid solicitation process. The debriefing may be in writing, by telephone or in person.

PART 2 - BIDDER INSTRUCTIONS

2.1 Standard Instructions, Clauses and Conditions

2.1.1 Integrity provisions—bid

1. The *Ineligibility and Suspension Policy* (the "Policy") in effect on the date the bid solicitation is issued, and all related Directives in effect on that date, are incorporated by reference into, and form a binding part of the bid solicitation. The Bidder must comply with the Policy and Directives, which can be found at *Ineligibility and Suspension Policy*.

2. Under the Policy, charges and convictions of certain offences against a Supplier, its affiliates or first tier subcontractors, and other circumstances, will or may result in a determination by Public Works and Government Services Canada (PWGSC) that the Supplier is ineligible to enter, or is suspended from entering into a contract with Canada. The list of ineligible and suspended Suppliers is contained in PWGSC's Integrity Database. The Policy describes how enquiries can be made regarding the ineligibility or suspension of Suppliers.

3. In addition to all other information required in the bid solicitation, the Bidder must provide the following:
    a. by the time stated in the Policy, all information required by the Policy described under the heading "Information to be Provided when Bidding, Contracting or Entering into a Real Property Agreement"; and
    b. with its bid, a complete list of all foreign criminal charges and convictions pertaining to itself, its affiliates and its proposed first tier subcontractors that, to the best of its knowledge and belief, may be similar to one of the listed offences in the Policy. The list of foreign criminal charges and convictions must be submitted using an Integrity Declaration Form, which can be found at Declaration form for procurement.

4. Subject to subsection 5, by submitting a bid in response to this bid solicitation, the Bidder certifies that:
    a. it has read and understands the *Ineligibility and Suspension Policy*;
    b. it understands that certain domestic and foreign criminal charges and convictions, and other circumstances, as described in the Policy, will or may result in a determination of ineligibility or suspension under the Policy;
    c. it is aware that Canada may request additional information, certifications, and validations from the Bidder or a third party for purposes of making a determination of ineligibility or suspension;
    d. it has provided with its bid a complete list of all foreign criminal charges and convictions pertaining to itself, its affiliates and its proposed first tier subcontractors that, to the best of its knowledge and belief, may be similar to one of the listed offences in the Policy;
    e. none of the domestic criminal offences, and other circumstances, described in the Policy that will or may result in a determination of ineligibility or suspension, apply to it, its affiliates and its proposed first tier subcontractors; and
    f. it is not aware of a determination of ineligibility or suspension issued by PWGSC that applies to it.

5. Where a Bidder is unable to provide any of the certifications required by subsection 4, it must submit with its bid a completed Integrity Declaration Form, which can be found at Declaration form for procurement.

6. Canada will declare non-responsive any bid in respect of which the information requested is incomplete or inaccurate, or in respect of which the information contained in a certification or declaration is found by Canada to be false or misleading in any respect. If Canada establishes after award of the Contract that the Bidder provided a false or misleading certification or declaration, Canada may terminate the Contract for default. Pursuant to the Policy, Canada may also determine the Bidder to be ineligible for award of a contract for providing a false or misleading certification or declaration.

2.1.2 Standard instructions, clauses and conditions

Pursuant to the *Department of Public Works and Government Services Act* (S.C. 1996, c.16), the instructions, clauses and conditions identified in the bid solicitation and resulting contract by number, date, and title are incorporated by reference into and form part of the bid solicitation and resulting contract as though expressly set out in the bid solicitation and resulting contract.

2.1.3 Definition of Bidder

"Bidder" means the person or entity (or, in the case of a joint venture, the persons or entities) submitting a bid to perform a contract for goods, services or both. It does not include the parent, subsidiaries or other affiliates of the Bidder, or its subcontractors.

2.1.4 Submission of bids

1. Canada requires that each bid, at solicitation closing date and time or upon request from the Contracting Authority, be signed by the Bidder or by an authorized representative of the Bidder. If a bid is submitted by a joint venture, it must be in accordance with section 2.1.15.
2. It is the Bidder's responsibility to:
    a. obtain clarification of the requirements contained in the bid solicitation, if necessary, before submitting a bid;
    b. prepare its bid in accordance with the instructions contained in the bid solicitation;
    c. submit by solicitation closing date and time a complete bid;
    d. send its bid only to the e-mail address specified on Page 1;
    e. ensure that the Bidder's name, return address, bid solicitation number, and solicitation closing date and time are clearly visible on the bid; and,
    f. provide a comprehensible and sufficiently detailed bid, including all requested pricing details, that will permit a complete evaluation in accordance with the criteria set out in the bid solicitation.
3. Canada will make available Notices of Proposed Procurement (NPP), bid solicitations and related documents for download through the Government Electronic Tendering Service (GETS). Canada is not responsible and will not assume any liabilities whatsoever for the information found on websites of third parties. In the event an NPP, bid solicitation or related documentation would be amended, Canada will not be sending notifications. Canada will post all amendments, including significant enquiries received and their replies, using GETS. It is the sole responsibility of the Bidder to regularly consult GETS for the most up-to-date information. Canada will not be liable for any oversight on the Bidder's part nor for notification services offered by a third party.
4. Bids will remain open for acceptance for a period of not less than 90 days from the closing date of the bid solicitation, unless specified otherwise in the bid solicitation. Canada reserves the right to seek an extension of the bid validity period from all responsive bidders in writing, within a minimum of 3 days before the end of the bid validity period. If the extension is accepted by all responsive bidders, Canada will continue with the evaluation of the bids. If the extension is not accepted by all responsive bidders, Canada will, at its sole discretion, either continue with the evaluation of the bids of those who have accepted the extension or cancel the solicitation.
5. Bid documents and supporting information may be submitted in either English or French.
6. Bids received on or before the stipulated bid solicitation closing date and time will become the property of Canada and will not be returned. All bids will be treated as confidential, subject to the provisions of the Access to Information Act (R.S. 1985, c. A-1) and the Privacy Act (R.S., 1985, c. P-21).
7. Unless specified otherwise in the bid solicitation, Canada will evaluate only the documentation provided with a bidder's bid. Canada will not evaluate information such as references to Web site addresses where additional information can be found, or technical manuals or brochures not submitted with the bid.
8. A bid cannot be assigned or transferred in whole or in part.

2.1.5 Late bids

Canada will return or delete bids delivered after the stipulated solicitation closing date and time, unless they qualify as a delayed bid as described in section 2.1.6.

Late physical bids will be returned, and for bids submitted electronically, the late bids will be deleted.

2.1.6 Customs clearance

It is the responsibility of the Bidder to allow sufficient time to obtain Customs clearance, where required, before the bid closing date and time. Delays related to the obtaining of Customs clearance cannot be construed as "undue delay in the mail" and will not be accepted as a delayed bid under section 2.1.6.

2.1.7 Legal capacity

The Bidder must have the legal capacity to contract. If the Bidder is a sole proprietorship, a partnership or a corporate body, the Bidder must provide, if requested by the Contracting Authority, a statement and any requested supporting documentation indicating the laws under which it is registered or incorporated together with the registered or corporate name and place of business. This also applies to bidders submitting a bid as a joint venture.

2.1.8 Rights of Canada

Canada reserves the right to:

a. reject any or all bids received in response to the bid solicitation;
b. enter into negotiations with bidders on any or all aspects of their bids;
c. accept any bid in whole or in part without negotiations;
d. cancel the bid solicitation at any time;
e. reissue the bid solicitation;
f. if no responsive bids are received and the requirement is not substantially modified, reissue the bid solicitation by inviting only the bidders who bid to resubmit bids within a period designated by Canada; and,
g. negotiate with the sole responsive Bidder to ensure best value to Canada.

2.1.9 Rejection of bid

1. Canada may reject a bid where any of the following circumstances is present:

    a. the Bidder is subject to a Vendor Performance Corrective Measure, under the Vendor Performance Corrective Measure Policy, which renders the Bidder ineligible to bid on the requirement;

    b. an employee, or subcontractor included as part of the bid, is subject to a Vendor Performance Corrective Measure, under the Vendor Performance Corrective Measure Policy, which would render that employee or subcontractor ineligible to bid on the requirement, or the portion of the requirement the employee or subcontractor is to perform;

    c. the Bidder is bankrupt or where, for whatever reason, its activities are rendered inoperable for an extended period;

    d. evidence, satisfactory to Canada, of fraud, bribery, fraudulent misrepresentation or failure to comply with any law protecting individuals against any manner of discrimination, has been received with respect to the Bidder, any of its employees or any subcontractor included as part of the bid;

    e. evidence satisfactory to Canada that based on past conduct or behavior, the Bidder, a subcontractor or a person who is to perform the Work is unsuitable or has conducted himself/herself improperly;

    f. with respect to current or prior transactions with the Government of Canada:

        i. Canada has exercised its contractual remedies of suspension or termination for default with respect to a contract with the Bidder, any of its employees or any subcontractor included as part of the bid;

        ii. Canada determines that the Bidder's performance on other contracts, including the efficiency and workmanship as well as the extent to which the Bidder performed the Work

in accordance with contractual clauses and conditions, is sufficiently poor to jeopardize the successful completion of the requirement being bid on.

2. Where Canada intends to reject a bid pursuant to a provision of subsection 1. (f), the Contracting Authority will so inform the Bidder and provide the Bidder 10 days within which to make representations, before making a final decision on the bid rejection.

3. Canada reserves the right to apply additional scrutiny, in particular, when multiple bids are received in response to a bid solicitation from a single bidder or a joint venture. Canada reserves the right to:

    a. reject any or all of the bids submitted by a single bidder or joint venture if their inclusion in the evaluation has the effect of prejudicing the integrity and fairness of the process, or;

    b. reject any or all of the bids submitted by a single bidder or joint venture if their inclusion in the procurement process would distort the solicitation evaluation, and would cause a result that would not reasonably have been expected under prevailing market conditions and/or would not provide good value to Canada.

2.1.10 Communications—solicitation period

To ensure the integrity of the competitive bid process, enquiries and other communications regarding the bid solicitation must be directed only to the Contracting Authority identified in the bid solicitation. Failure to comply with this requirement may result in the bid being declared non-responsive.

To ensure consistency and quality of information provided to bidders, significant enquiries received and their replies will be posted on the Government Electronic Tendering Service (GETS). For further information, consult subsection 3 of section 2.1.4.

2.1.11 Price justification

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

a. a current published price list indicating the percentage discount available to Canada; or

b. a copy of paid invoices for the like quality and quantity of the goods, services or both sold to other customers; or

c. a price breakdown showing the cost of direct labour, direct materials, purchased items, engineering and plant overheads, general and administrative overhead, transportation, etc., and profit; or

d. price or rate certifications; or

e. any other supporting documentation as requested by Canada.

2.1.12 Bid costs

No payment will be made for costs incurred in the preparation and submission of a bid in response to the bid solicitation. Costs associated with preparing and submitting a bid, as well as any costs incurred by the Bidder associated with the evaluation of the bid, are the sole responsibility of the Bidder.

2.1.13 Conduct of evaluation

1. In conducting its evaluation of the bids, Canada may, but will have no obligation to, do the following:

    a. seek clarification or verification from bidders regarding any or all information provided by them with respect to the bid solicitation;

    b. contact any or all references supplied by bidders to verify and validate any information submitted by them;

    c. request, before award of any contract, specific information with respect to bidders' legal status;

d. conduct a survey of bidders' facilities and/or examine their technical, managerial, and financial capabilities to determine if they are adequate to meet the requirements of the bid solicitation;

e. correct any error in the extended pricing of bids by using unit pricing and any error in quantities in bids to reflect the quantities stated in the bid solicitation; in the case of error in the extension of prices, the unit price will govern.

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

g. interview, at the sole costs of bidders, any bidder and/or any or all of the resources proposed by bidders to fulfill the requirement of the bid solicitation.

2. Bidders will have the number of days specified in the request by the Contracting Authority to comply with any request related to any of the above items. Failure to comply with the request may result in the bid being declared non-responsive.

2.1.14 Joint venture

1. 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 bid together on a requirement. Bidders who bid as a joint venture must indicate clearly that it is a joint venture and provide the following information:

   a. the name of each member of the joint venture;

   b. the Procurement Business Number of each member of the joint venture;

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

   d. the name of the joint venture, if applicable.

2. If the information is not clearly provided in the bid, the Bidder must provide the information on request from the Contracting Authority.

3. The bid and any resulting contract must be signed by all the members of the joint venture unless one member has been appointed to act on behalf of all members of the joint venture. The Contracting Authority may, at any time, require each member of the joint venture to confirm that the representative has been appointed with full authority to act as its representative for the purposes of the bid solicitation and any resulting contract. If a contract is awarded to a joint venture, all members of the joint venture will be jointly and severally or solidarily liable for the performance of any resulting contract.

2.1.15 Conflict of interest—unfair advantage

1. In order to protect the integrity of the procurement process, bidders are advised that Canada may reject a bid in the following circumstances:

   a. if the Bidder, any of its subcontractors, any of their respective employees or former employees was involved in any manner in the preparation of the bid solicitation or in any situation of conflict of interest or appearance of conflict of interest;

   b. if the Bidder, any of its subcontractors, any of their respective employees or former employees had access to information related to the bid solicitation that was not available to other bidders and that would, in Canada's opinion, give or appear to give the Bidder an unfair advantage.

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

3. Where Canada intends to reject a bid under this section, the Contracting Authority will inform the Bidder and provide the Bidder an opportunity to make representations before making a final decision. Bidders who are in doubt about a particular situation should contact the Contracting Authority before bid closing. By submitting a bid, the Bidder represents that it does not consider itself to be in conflict of interest nor to have an unfair advantage. The Bidder acknowledges that it is within Canada's sole discretion to determine whether a conflict of interest, unfair advantage or an appearance of conflict of interest or unfair advantage exists.

2.1.16 Entire requirement

The bid solicitation documents contain all the requirements relating to the bid solicitation. Any other information or documentation provided to or obtained by a bidder from any source are not relevant. Bidders should not assume that practices used under previous contracts will continue, unless they are described in the bid solicitation. Bidders should also not assume that their existing capabilities meet the requirements of the bid solicitation simply because they have met previous requirements.

2.1.17 Further information

For further information, bidders may contact the Contracting Authority identified in the bid solicitation.

2.1.18 Code of Conduct for Procurement—bid

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

2.2 Submission of Bids

Bids must be submitted only to Employment and Social Development Canada (ESDC) by the date, time and place or email address indicated on page 1 of the bid solicitation.

It is the Bidders responsibility to ensure their proposal and all associated documents are received in full and on time. It is advised that Bidders send the proposal in advance of the closing time to ensure confirmation of receipt.

Bidders must ensure e-mails do not exceed 13MB to avoid problems with transmission. For security reasons, any information submitted on a USB key will not be evaluated.

Due to the nature of the bid solicitation, bids transmitted by facsimile to ESDC will not be accepted.

2.3 Former Public Servant

Contracts awarded to former public servants (FPS) in receipt of a pension or of a lump sum payment must bear the closest public scrutiny, and reflect fairness in the spending of public funds. In order to comply with Treasury Board policies and directives on contracts awarded to FPS, bidders must provide the information required below before contract award. If the answer to the questions and, as applicable the information required have not been received by the time the evaluation of bids is completed, Canada will inform the Bidder of a time frame within which to provide the information. Failure to comply with Canada’s request and meet the requirement within the prescribed time frame will render the bid non-responsive.

Definitions

For the purposes of this clause:
"former public servant" is any former member of a department as defined in the *Financial Administration Act*, R.S., 1985, c. F-11, a former member of the Canadian Armed Forces or a former member of the Royal Canadian Mounted Police.
A former public servant may be:

a. an individual;
b. an individual who has incorporated;
c. a partnership made of former public servants; or

d. a sole proprietorship or entity where the affected individual has a controlling or major interest in the entity.

"lump sum payment period" means the period measured in weeks of salary, for which payment has been made to facilitate the transition to retirement or to other employment as a result of the implementation of various programs to reduce the size of the Public Service. The lump sum payment period does not include the period of severance pay, which is measured in a like manner.

"pension" means a pension or annual allowance paid under the *Public Service Superannuation Act* (PSSA), R.S., 1985, c. P-36, and any increases paid pursuant to the *Supplementary Retirement Benefits Act*, R.S., 1985, c. S-24 as it affects the PSSA. It does not include pensions payable pursuant to the *Canadian Forces Superannuation Act*, R.S., 1985, c. C-17, the *Defence Services Pension Continuation Act*, 1970, c. D-3, the *Royal Canadian Mounted Police Pension Continuation Act* , 1970, c. R-10, and the *Royal Canadian Mounted Police Superannuation Act*, R.S., 1985, c. R-11, the *Members of Parliament Retiring Allowances Act*, R.S. 1985, c. M-5, and that portion of pension payable to the *Canada Pension Plan Act*, R.S., 1985, c. C-8.

Former Public Servant in Receipt of a Pension

As per the above definitions, is the Bidder a FPS in receipt of a pension? **Yes** ( ) **No** ( )

If so, the Bidder must provide the following information, for all FPSs in receipt of a pension, as applicable:
a. name of former public servant;
b. date of termination of employment or retirement from the Public Service.

By providing this information, Bidders agree that the successful Bidder's status, with respect to being a former public servant in receipt of a pension, will be reported on departmental websites as part of the published proactive disclosure reports in accordance with Contracting Policy Notice: 2019-01 and the Guidelines on the Proactive Disclosure of Contracts.

Work Force Adjustment Directive

Is the Bidder a FPS who received a lump sum payment pursuant to the terms of the Work Force Adjustment Directive? **Yes** ( ) **No** ( )

If so, the Bidder must provide the following information:
a. name of former public servant;
b. conditions of the lump sum payment incentive;
c. date of termination of employment;
d. amount of lump sum payment;
e. rate of pay on which lump sum payment is based;
f. period of lump sum payment including start date, end date and number of weeks;
g. number and amount (professional fees) of other contracts subject to the restrictions of a work force adjustment program.

2.4 Enquiries - Bid Solicitation

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

Bidders should reference as accurately as possible the numbered item of the bid solicitation to which the enquiry relates. Care should be taken by Bidders to explain each question in sufficient detail in order to enable Canada to provide an accurate answer. Technical enquiries that are of a proprietary nature must be clearly marked "proprietary" at each relevant item. Items identified as "proprietary" will be treated as such except where Canada determines that the enquiry is not of a proprietary nature. Canada may edit the question(s) or may request that the Bidder do so, so that the proprietary nature of the question(s) is eliminated and the enquiry can be answered to all Bidders. Enquiries not submitted in a form that can be distributed to all Bidders may not be answered by Canada.

2.5 Applicable Laws

Any resulting contract must be interpreted and governed, and the relations between the parties determined, by the laws in force in Ontario.

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

2.6 Improvement of Requirement during Solicitation Period

Should bidders consider that the specifications or Statement of Work contained in the bid solicitation could be improved technically or technologically, bidders are invited to make suggestions, in writing, to the Contracting Authority named in the bid solicitation. Bidders must clearly outline the suggested improvement as well as the reason for the suggestion. Suggestions that do not restrict the level of competition nor favour a particular bidder will be given consideration provided they are submitted to the Contracting Authority at least five (5) days before the bid closing date. Canada will have the right to accept or reject any or all suggestions.

2.7 Bid Challenge and Recourse Mechanisms

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

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

- Office of the Procurement Ombudsman (OPO)
- Canadian International Trade Tribunal (CITT)

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

PART 3 - BID PREPARATION INSTRUCTIONS

3.1 Bid Preparation Instructions

Canada requests that Bidders provide their full company name and address, e-mail address, as well as contact name, and telephone number.

Canada requests that bidders provide their bid in separate files, as follows:

Section I: Technical Bid, 1 soft copy via e-mail;
Section II: Financial Bid, 1 soft copy via e-mail;
Section III: Certifications, 1 soft copy via e-mail; and,
Section IV: Additional Information, 1 soft copy via e-mail.

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

Canada requests that Bidders use a numbering system that corresponds to the bid solicitation when preparing their bid.

Section I: Technical Bid

In their technical bid, Bidders should demonstrate their understanding of the requirements contained in the bid solicitation and explain how they will meet these requirements. Bidders should demonstrate their capability and describe their approach in a thorough, concise and clear manner for carrying out the work.

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

Section II: Financial Bid

Bidders must submit their financial bid in accordance with the Pricing Schedule in Attachment 1 to part 3.

3.1.1 Electronic Payment of Invoices – Bid

If you are willing to accept payment of invoices by Electronic Payment Instruments, complete Annex E Electronic Payment Instruments, to identify which ones are accepted.

If Annex E Electronic Payment Instruments is not completed, it will be considered as if Electronic Payment Instruments are not being accepted for payment of invoices.

Acceptance of Electronic Payment Instruments will not be considered as an evaluation criterion.

3.1.2 Exchange Rate Fluctuation

The requirement does not offer exchange rate fluctuation risk mitigation. Requests for exchange rate fluctuation risk mitigation will not be considered. All bids including such provision will render the bid non-responsive.

Section III: Certifications

Bidders must submit the certifications and additional information required under Part 5.

Section IV: Additional Information – For Phase 2

3.1.3 Bidder's Proposed Sites or Premises Requiring Safeguarding Measures

3.1.3.1 As indicated in Part 6 under Security Requirements, the Bidder must provide the full addresses of the Bidder's and proposed individuals' sites or premises for which safeguarding measures are required for Work Performance:

Street Number / Street Name, Unit / Suite / Apartment Number
City, Province, Territory / State
Postal Code / Zip Code
Country

3.1.3.2 The Company Security Officer must ensure through the Contract Security Program that the Bidder and proposed individuals hold a valid security clearance at the required level, as indicated in Part 6 – Security, Financial and Other Requirements.

3.1.3.3 See APPENDIX A to Annex B: Security Obligations for Tier 2 (up to Protected B), for additional information regarding Phase 2 of resulting Contract.

ATTACHEMENT 1 TO PART 3 – PRICING SCHEDULE

Bidders must submit their financial bid in accordance with the following Pricing Schedule.

The financial bid total price will be calculated as per the following equation:

Financial Bid Total= (0.1 x A) + (0.1 x B) + (0.5 x C) + (0.15 x D) + (0.15 x E)

Professional Services

Customs duties are included and Applicable Taxes are extra.

Period	Estimated Level of Effort	Resource Category	Firm Hourly Rate
Initial Period	''As and When Requested'' Basis	Subject Matter Expert	A1 $ _____
		Training Expert	A2 $ _____
Option Period - 1	''As and When Requested'' Basis	Subject Matter Expert	A3 $ _____
		Training Expert	A4 $ _____
Option Period - 2	''As and When Requested'' Basis	Subject Matter Expert	A5 $ _____
		Training Expert	A6 $ _____
Option Period – 3	''As and When Requested'' Basis	Subject Matter Expert	A7 $ _____
		Training Expert	A8 $ _____
Option Period – 4	''As and When Requested'' Basis	Subject Matter Expert	A9 $ _____
		Training Expert	A10 $ _____
Option Period – 5	''As and When Requested'' Basis	Subject Matter Expert	A11 $ _____
		Training Expert	A12 $ _____
Option Period – 6	''As and When Requested'' Basis	Subject Matter Expert	A13 $ _____
		Training Expert	A14 $ _____
(A) Total Professional Services (Sum of A1 to A14):			**(A) $ _____**

*Training Expert as per Part 10 of the Statement of Work.

Training Services (As per Part 9 of the Statement of Work)

Customs duties are included and Applicable Taxes are extra.

Period	Group Type	Estimated Quantity	Firm Unit Price	Subtotal
Initial Period	Group 1 (From 10 to 30 participants)	7	B1.1 $ _____	B1.2 $ _____
	Group 2 (From 5 to 15 participants)	12	B2.1 $ _____	B2.2 $ _____
Option Period - 1	Group 1 (From 10 to 30 participants)	5	B3.1 $ _____	B3.2 $ _____
	Group 2 (From 5 to 15 participants)	5	B4.1 $ _____	B4.2 $ _____
Option Period - 2	Group 1 (From 10 to 30 participants)	1	B5.1 $ _____	B5.2 $ _____
	Group 2 (From 5 to 15 participants)	1	B6.1 $ _____	B6.2 $ _____
(B) Total Training Services (Sum of B1.2 to B6.2):				**(B) $ _____**

Software as a Service Solution – Annual Subscription

Customs duties are included and Applicable Taxes are extra.

***This basis of payment will begin the day following the Project Authority's acceptance of the release.** As per the Statement of work, after the expiration of the 60-days Error Free Stabilization period, if the release conforms to the Acceptance Criteria, ESDC will accept the release.*

Period	Firm Annual Unit Price *Annual Subscription fees per user				
	From 0 up to 150 users	More than 150 up to 1,000 users	More than 1,000 up to 6,500 users	More than 6,500 up to 10,500 users	Subtotal
Initial Period	C1.1 $ ____	C1.2 $ ____	C1.3 $ ____	C1.4 $ ____	**C1 $ _____ (C1 = C1.1 + C1.2 + C1.3 + C1.4)**
Option Period – 1	C2.1 $ ____	C2.2 $ ____	C2.3 $ ____	C2.4 $ ____	**C2 $ _____ (C2 = C2.1 + C2.2 + C2.3 + C2.4)**
Option Period – 2	C3.1 $ ____	C3.2 $ ____	C3.3 $ ____	C3.4 $ ____	**C3 $ _____ (C3 = C3.1 + C3.2 + C3.3 + C3.4)**
Option Period – 3	C4.1 $ ____	C4.2 $ ___	C4.3 $ ____	C4.4 $ ____	**C4 $ _____ (C4 = C4.1 + C4.2 + C4.3 + C4.4)**
Option Period – 4	C5.1 $ ____	C5.2 $ ____	C5.3 $ ____	C5.4 $ ____	**C5 $ _____ (C5 = C5.1 + C5.2 + C5.3 + C5.4)**
Option Period – 5	C6.1 $ ____	C6.2 $ ___	C6.3 $ ____	C6.4 $ ____	**C6 $ _____ (C6 = C6.1 + C6.2 + C6.3 + C6.4)**
Option Period – 6	C7.1 $ ____	C7.2 $ ____	C7.3 $ ____	C7.4 $ ____	**C7 $ _____ (C7 = C7.1 + C7.2 + C7.3 + C7.4)**
(C) Total Software as a Service Annual Subscription (Sum of C1 to C7):					**(C) $ _____**

**We are estimating the quantity of users to start at 80 users for the first month(s), but to go up to 10,400 users during the period of the contract including the option periods.*

SaaS Solution Configuration and Go-live – Phase 1 Unclassified Data

Canada will make milestone payments in accordance with the Schedule of Milestones detailed in the Contract and the payment provisions of the Contract. Customs duties are included and Applicable Taxes are extra.

******See basis of payment and Statement of Work for more details***

Milestone No.	Description or "Deliverable"	Firm Amount
1	**Kick-off** ***(Project Start-up)***	N/A
2	**Project Planning** ***(Project Management Planning complete)***	D1 $ _____
3	**Architecture and Design**	D2 $ _____
4	**Core Solution Configuration and Integration Testing**	D3 $ _____
5	**Operations** **Includes the Annual Subscription Fee during the 60-days stabilization step*	D4 $ _____
	(D) Total SaaS Solution Configuration and Go-live for Phase 1 (Sum of D1 to D4):	**(D) $ _____**

SaaS Solution Configuration and Go-live – Phase 2 Protected Data

***Phase 2 is conditional to the vendor obtaining all necessary Security Clearances under this Contract, as per the clauses in 7.3 of the contract and the APPENDIX A to Annex B: Security Obligations for Tier 2 (up to Protected B) AND will occur if/when ESDC decides to move forward with this phase.**

Canada will make milestone payments in accordance with the Schedule of Milestones detailed in the Contract and the payment provisions of the Contract. Customs duties are included and Applicable Taxes are extra.

******See basis of payment and Statement of Work for more details***

Milestone No.	Description or "Deliverable"	Firm Amount
1	**Kick-off** ***(Project Start-up)***	N/A
2	**Project Planning** ***(Project Management Planning complete)***	E1 $ _____
3	**Architecture and Design**	E2 $ _____
4	**Core Solution Configuration and Integration Testing**	E3 $ _____
5	**Operations** **Includes the Annual Subscription Fee during the 60-days stabilization step*	E4 $ _____
	(E) Total SaaS Solution Configuration and Go-live for Phase 2 (Sum of E1 to E4):	**(E) $ _____**

PART 4 - EVALUATION PROCEDURES AND BASIS OF SELECTION

4.1 Evaluation Procedures

(a) Bids will be assessed in accordance with the entire requirement of the bid solicitation including the technical and financial evaluation criteria.

(b) An evaluation team composed of representatives of Canada will evaluate the bids.

4.1.1 Technical Evaluation

4.1.1.1 Mandatory Technical Criteria

Full compliance with mandatory criteria is required in order for proposals to be further evaluated.

	MANDATORY CRITERIA REQUIREMENTS	Met	Not Met	Reference/Comments Cross reference to proposal page number
M1	The bidder **must** demonstrate that the proposed solution is a cloud-based software-as-a-service (SaaS), which **must** have data centers located in Canada and in a wholly Canadian region to support data up to and including Protected B status.			
M2	The bidder **must** demonstrate that the proposed solution is available to ESDC designated users throughout Canada.			
M3	The bidder **must** demonstrate that the solution and all metadata are equally and fully functional/available in both English and French.			
M4	The bidder **must** demonstrate that the proposed solution is able to integrate with and use data from ESDC's **HCM system myEMS (Peoplesoft HCM 9.2)** to generate the organization chart.			
M5	The bidder **must** demonstrate that the proposed solution automatically generates the organization chart with the ability to add or update through text editing and/or drag and drop.			
M6	The bidder **must** demonstrate that the proposed solution is able to support a minimum of 60,000 positions in the organization chart.			

4.1.1.2 Point Rated Technical Criteria

Bidders should respond to the questions below clearly and concisely. If the bidder is attaching documents as part of their response to a specific question, the bidder should reference the attachments in their response.

Indicate, using the table below, the features that are currently available and any details about the feature that you wish to share. To guide your response to these questions please consider the following: "Feature Available" means that the features are readily available in the platform and would require only

minimal input or configuration to set up. Any features that are not currently developed or would require in-depth customization would not qualify.

For R2 to R13: The bidder must include additional notes describing how the requirement is met (up to a maximum of 500 words or one (1) page per feature).

	TECHNICAL RATED CRITERIA	Scoring	Reference/Comments Cross reference to proposal, page number
R1	The bidder **must** provide an overview of their Organization Chart solution with the key features/services that have been used throughout five (5) past or current projects with different clients, for at least six (6) months per project, in a similar capacity to ESDC's requirements*. *Please illustrate how your solution's features/services support your client's business objectives.* Response must be limited to five (5) pages. Example: - Client/Organization Name; - Approximate number of users; - Data Protection level (ie. Protected A, B, etc) or examples of securing sensitive data (personal or sensitive information, on any type of secured system); - Number of positions in the Organization Chart; - Start date (MM-YYYY) and end date (MM-YYY) of project; - Additional notes or details. ***ESDC's requirement is approximately 60,000 positions.***	**Maximum Points: 20** **Minimum Points*: 10** ***Minimum scored points required for the bid to be compliant and to move to the evaluation of the next rated criteria.*** **Up to 4 points per project/client:** **Up to 1 point for number of users:** - 1 point if more than 5,000 users; - 0.75 point if more than 4,000 users, but less than 5,000 users; - 0.50 point if more than 2,000 users, but less than 4,000 users; - 0.25 point if more than 1,000 users, but less than 2,000 users; - 0 point if less than 1,000 users. **Up to 1 point for number of positions in the Organization Chart:** - 1 point if more than 50,000 positions; - 0.75 point if more than 40,000 positions, but less than 50,000 positions; - 0.50 point if more than 30,000 positions, but less than 40,000 positions; - 0.25 point if more than 20,000 positions, but less than 30,000 positions; - 0 point if less than 20,000 positions. **Up to 1 point for examples of data protection or security:** - 0.5 point if Protected A or more (or personal information in the private sector); - 0.5 point if the bidder has provided an example of securing sensitive data. **Up to 1 point for the period of the project:** - 1 point for more than 24 months; - 0.75 point for more than 18 months but less than 24 months; - 0.50 point for more than 12 months but less than 18 months; - 0.25 point for more than 6 months but less than 12 months; - 0 point for less than 6 months.	
R2	**General Functionality** The bidder should demonstrate how the Solution	**Maximum Points: 2**	

	is able to print the organization chart that is formatted and aggregated in PDF (with a minimum of 20 boxes on a page).	- 1 point if the Solution is able to print the organization chart that is formatted and aggregated in a PDF format; - 1 additional point if the Solution is able to print a minimum of 20 boxes on a single page.	
R3	**General Functionality** The bidder should demonstrate how the Solution allows the user to search for a position within the organization chart by entering the data fields below: - Position Number; - Reports to Position Number; - Last Name; - First Name; and, - Department ID.	**Maximum Points: 2** - 0.5 point for ''Position Number''; - 0.5 point for ''Reports to Position Number''; - 0.25 point for ''Last Name''; - 0.25 point for ''First Name''; and, - 0.5 point for ''Department ID''.	
R4	**General Functionality** The bidder should demonstrate how the organization chart identifies: - the Branch and Division names; - the name of the sub-delegated manager; and, - the date the chart has been generated.	**Maximum Point: 1** - 1 point if all three elements are identified; - 0 point if not all three elements are identified.	
R5	**General Functionality** The bidder should demonstrate how the Solution extracts the HR data fields from myEMS (PeopleSoft HCM 9.2) for each position within an organization chart, whether vacant or occupied, at a minimum of two supervisory/reporting levels, from Level 3 through level 7.	**Maximum Points: 3** - 3 points if the bidder demonstrates all required elements in this criterion; - 0 point if any element is missing from the bid.	
R6	**General Functionality** The bidder should demonstrate how the Solution provides the capability of developing and storing what-if scenarios to accommodate future organizational changes.	**Maximum Points: 3** - 3 points if the bidder demonstrates all required elements in this criterion; - 0 point if any element is missing from the bid.	
R7	**Workflow** The bidder should demonstrate how the Solution provides workflow capability to allow HR Delegated Managers and the HR Classification staff to collaborate and share organizational changes prior to submission; and approve submitted changes after review.	**Maximum Points: 2** - 2 points if the bidder demonstrates all required elements in this criterion; - 0 point if any element is missing from the bid.	
R8	**Integration** The bidder should demonstrate how the Solution is able to provide Single Sign On capability using ESDC's LDAP username/password.	**Maximum Points: 3** - 3 points if the bidder demonstrates all required elements in this criterion; - 0 point if any element is missing from the bid.	

R9	**Integration**
	The bidder should demonstrate how the Solution supports **at least two** of the most recent stable releases of the following browsers:
	- Microsoft Edge:
	  ○ Version 102.0.1245.30 (Official build) (64-bit) or greater,
	- Mozilla FireFox:
	  ○ Version 101.0 (64-bit) or greater.
		Maximum Point: 1
		- 0.5 point if the Solution supports at least two of the most recent stable releases of Microsoft Edge;
		- 0.5 point if the Solution supports at least two of the most recent stable releases of Mozilla FireFox.	

R10	**Accessibility** The bidder should demonstrate that the Solution conforms to accessibility guidelines as defined under the ETSI EN 301 549 - V3.2.1 - Accessibility requirements for ICT products and services specifically clauses 9.1 – 9.4 – Web (includes WCAG 2.1 Level AA), 10.0 General – Non Web documents (ie. PDF) and 12.1 – Product documentation (training) The bidder should provide an Accessibility Conformance Report (ACR) based on a VPAT 2.4 Rev EU® (Voluntary Product Accessibility Template) that outlines how their Solution meets or doesn't meet the ICT requirements. The ACR should be prepared by a third-party unless the Bidder has a qualified accessibility office themselves. To be deemed valid, the ACR must have been completed within 24 months from bid closing date.	**Maximum Points: 5** - 1 point will be awarded for conformance to each clause from 9.1 to 9.4 – Web (includes WCAG 2.1 Level AA) - 0.5 point will be awarded for conformance to clause 10.0 General – Non Web documents - 0.5 point will be awarded for conformance to clause 12.1 – Product documentation **Points will only be awarded if the bidder has provided a current ACR, completed within 24 months from the bid closing date.*	
R11	**Access** The bidder should demonstrate how the Solution provides an admin account management system where specific Groups (ie. HR Delegated Manager, HR Classification) or Users (Employee) access permissions can be managed to control access to the Organization Chart and displayed information.	**Maximum Points: 2** - 1 point if the Solution provides an admin account management system; - 0.5 additional point if there are specific Groups access permissions that can be managed; - 0.5 additional point if there are specific Users access permissions that can be managed.	
R12	**Training** The bidder should demonstrate that the Solution provides a training guide that is user-friendly and available in both official languages (English and French).	**Maximum Point: 1** - 0.5 point if available training in French; - 0.5 point if available training is in English.	
R13	**Certification** The bidder should demonstrate that they are certified by one of the following data security management certification, and that they will be renewed annually at no additional charge: - AICPA Service Organization Control (SOC) 2 Type II Audit Report, - ISO/IEC 27001:2013 Information technology, and/or - ISO/IEC 27017:2015 Information technology. ****Will be necessary to move forward with Phase 2 of the contract. If the winning bidder is not certified, ESDC expects the vendor to work on obtaining the necessary certifications in a timely manner for Phase 2.***	**Maximum Points: 5** - 5 points: Bidder demonstrates they are certified by **all these three** data security management certifications; - 4 points: Bidder demonstrates they are certified by **at least two of these three** data security management certifications; - 3 points: Bidder demonstrates they are certified by **at least one of these three** data security management certifications; - 0 point: Bidder is not certified by any of these three data security management certifications.	
	Minimum Points Required	**30 points**	
	Maximum Points	**50 points**	
	Total		

4.1.1.2.1 Accessibility

By submitting a bid to this request for proposals (RFP) #100021358, the vendor commits to conform with the accessibility requirements in a timely manner, if they do not already comply fully with the criterion R10. If required by the project authority, the vendor must provide an accessibility roadmap before the end of the period of the resulting contract.

4.2 Basis of Selection

4.2.1 Basis of Selection – Highest Combined Rating of Technical Merit and Price 70/30

1. To be declared responsive, a bid must:
   a. comply with all the requirements of the bid solicitation;
   b. meet all mandatory criteria;
   c. obtain the required minimum points specified for criterion number R1 for the technical evaluation; and,
   d. obtain the required minimum of **30** points overall for the technical evaluation criteria which are subject to point rating.
   The rating is performed on a scale of **50** points.

2. Bids not meeting (a) or (b) or (c) and (d) will be declared non-responsive.

3. The selection will be based on the highest responsive combined rating of technical merit and price. The ratio will be 70 % for the technical merit and 30 % for the price.

4. To establish the technical merit score, the overall technical score for each responsive bid will be determined as follows: total number of points obtained / maximum number of points available multiplied by the ratio of 70 %.

5. To establish the pricing score, each responsive bid will be prorated against the lowest evaluated price and the ratio of 30 %.

6. For each responsive bid, the technical merit score and the pricing score will be added to determine its combined rating.

7. Neither the responsive bid obtaining the highest technical score nor the one with the lowest evaluated price will necessarily be accepted. The responsive bid with the highest combined rating of technical merit and price will be recommended for award of a contract.

8. If two of more responsive bids achieve an identical score (total number of points) and this score is determined to be the Highest Combined Rating of Technical Merit and Price, the bidder who achieved the highest technical merit score will be recommended for contract award.

The table below illustrates an example where all three bids are responsive and the selection of the contractor is determined by a 70/30 ratio of technical merit and price, respectively. The total available points equals 135 and the lowest evaluated price is $45,000 (45).

Basis of Selection - Highest Combined Rating Technical Merit (70%) and Price (30%)

		Bidder 1	Bidder 2	Bidder 3
Overall Technical Score		115/135	89/135	92/135
Bid Evaluated Price		$55,000.00	$50,000.00	$45,000.00
Calculations	**Technical Merit Score**	115/135 x 70 = 59.63	89/135 x 70 = 46.15	92/135 x 70 = 47.70
	Pricing Score	45/55 x 30 = 24.55	45/50 x 30 = 27.00	45/45 x 30 = 30.00
Combined Rating		84.18	73.15	77.7
Overall Rating		1st	3rd	2nd

PART 5 – CERTIFICATIONS AND ADDITIONAL INFORMATION

Bidders must provide the required certifications and additional information to be awarded a contract.

The certifications provided by Bidders to Canada are subject to verification by Canada at all times. Unless specified otherwise, Canada will declare a bid non-responsive, or will declare a contractor in default if any certification made by the Bidder is found to be untrue, whether made knowingly or unknowingly, during the bid evaluation period or during the contract period.

The Contracting Authority will have the right to ask for additional information to verify the Bidder's certifications. Failure to comply and to cooperate with any request or requirement imposed by the Contracting Authority will render the bid non-responsive or constitute a default under the Contract.

5.1 Certifications Required with the Bid

Bidders must submit the following duly completed certifications as part of their bid.

5.1.1 Integrity Provisions - Declaration of Convicted Offences

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.

5.2 Certifications Precedent to Contract Award and Additional Information

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

5.2.1 Integrity Provisions – Required Documentation

In accordance with the section titled Information to be provided when bidding, contracting or entering into a real procurement agreement of the Ineligibility and Suspension Policy (http://www.tpsgc-pwgsc.gc.ca/ci-if/politique-policy-eng.html), the Bidder must provide the required documentation, as applicable, to be given further consideration in the procurement process.

5.2.2 Security Requirements – Required Documentation – Phase 2 of Contract

In accordance with the requirements of the Contract Security Program of Public Works and Government Services Canada (http://www.tpsgc-pwgsc.gc.ca/esc-src/introduction-eng.html), the Bidder must provide a completed Contract Security Program Application for Registration (AFR) form to be given further consideration in the procurement process.

Bidders are reminded to obtain the required security clearance and, as applicable, security capabilities promptly. As indicated above, bidders who do not provide all the required information at bid closing will be given the opportunity to complete any missing information from the AFR form within a period set by the Contracting Authority. If that information is not provided within the timeframe established by the Contracting Authority (including any extension granted by the Contracting Authority in its discretion), or if Canada requires further information from the Bidder in connection with assessing the request for security clearance (i.e., information not required by the AFR form), the Bidder will be required to submit that information within the time period established by the Contracting Authority, which will not be less than 48 hours. If, at any time, the Bidder fails to provide the required information within the timeframe established by the Contracting Authority, its bid will be declared non-compliant.

PART 6 - SECURITY, FINANCIAL AND OTHER REQUIREMENTS

6.1 Security Requirements – Phase 1

There are no security requirements associated with the Phase 1 of this solicitation.

6.2 Security Requirements – Phase 2

1. Before award of Phase 2 of contract, the following conditions must be met:

   (a) the Bidder must hold a valid organization security clearance as indicated in Part 7 - Resulting Contract Clauses.

   (b) the Bidder must provide the addresses of proposed sites or premises of work performance and document safeguarding as indicated in Part 3 - Section IV Additional Information.

2. Before access to sensitive information is provided to the Bidder, the following conditions must be met:

   (a) the Bidder's proposed individuals requiring access to sensitive information, assets or sensitive work sites must meet the security requirements as indicated in Part 7 - Resulting Contract Clauses.

   (b) the Bidder’s security capabilities must be met as indicated in Part 7 - Resulting Contract Clauses.

3. 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.

PART 7 - RESULTING CONTRACT CLAUSES

The following clauses and conditions apply to and form part of any contract resulting from the bid solicitation.

7.1 Statement of Work

The Contractor must perform the Work in accordance with the Statement of Work at Annex B.

7.1.1 Task Authorization

The Work or a portion of the Work to be performed under the Contract will be on an "as and when requested basis" using a Task Authorization (TA). The Work described in the TA must be in accordance with the scope of the Contract.

7.1.1.1 Task Authorization Process

1. The Project Authority will provide the Contractor with a description of the task using the "Task Authorization" form specified in Annex F.

2. The Task Authorization (TA) will contain the details of the activities to be performed, a description of the deliverables, and a schedule indicating completion dates for the major activities or submission dates for the deliverables. The TA will also include the applicable basis(bases) and methods of payment as specified in the Contract.

3. The Contractor must provide the Project Authority, within five (5) calendar days of its receipt, the proposed total estimated cost for performing the task and a breakdown of that cost, established in accordance with the Basis of Payment specified in the Contract.

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

7.1.1.2 Periodic Usage Reports - Contracts with Task Authorizations

The Contractor must compile and maintain records on its provision of services to the federal government under authorized Task Authorizations issued under the Contract.

The Contractor must provide this data in accordance with the reporting requirements detailed below. If some data is not available, the reason must be indicated. If services are not provided during a given period, the Contractor must still provide a "nil" report.

The data must be submitted on a monthly basis to the Contracting Authority.

The monthly periods are defined as the period between the first day and the last day of each month inclusively.

The data must be submitted to the Contracting Authority no later than seven (7) calendar days after the end of the reporting period.

Reporting Requirement- Details
A detailed and current record of all authorized tasks must be kept for each contract with a task authorization process. This record must contain:

For each authorized task:

1. the authorized task number or task revision number(s);

2. a title or a brief description of each authorized task;
3. the total estimated cost specified in the authorized Task Authorization (TA) of each task, exclusive of Applicable Taxes;
4. the total amount, exclusive of Applicable Taxes, expended to date against each authorized task;
5. the start and completion date for each authorized task; and
6. the active status of each authorized task, as applicable.

For all authorized tasks:

i. the amount (exclusive of Applicable Taxes) specified in the contract (as last amended, as applicable) as Canada's total liability to the contractor for all authorized TAs; and
ii. the total amount, exclusive of Applicable Taxes, expended to date against all authorized TAs.

7.2 Standard Clauses and Conditions

All clauses and conditions identified in the Contract 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.

7.2.1 General Conditions

The General Conditions – ESDC (2022-04-07) at Annex "A", apply to and form part of the Contract.

7.3 Security Requirements – Phase 2 of Contract

7.3.1 The following security requirements (SRCL and related clauses provided by the Contract Security Program) apply and form part of the Phase 2 of the Contract:

1. The contractor/offeror must, at all times during the performance of the contract/standing offer, hold a valid designated organization screening (DOS) with approved document safeguarding at the level of **protected B**, issued by the Contract Security Program (CSP), Public Works and Government Services Canada (PWGSC);
2. The contractor/offeror personnel requiring access to **protected** information, assets or work site(s) must **each** hold a valid **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 ESDC has issued written approval. After approval has been granted or approved, these tasks may be performed up to the level of **protected B,** including an IT Link up to 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; and,
5. The contractor/offeror must comply with the provisions of the:
    a. Security Requirements Check List and security guide, attached at Annex D,
    b. Contract Security Manual (latest edition),
    c. Security Requirements at Appendix A to Annex B.

7.3.2 Contractor's Sites or Premises Requiring Safeguarding Measures

7.3.2.1 Where safeguarding measures are required in the performance of the Work, the Contractor must diligently maintain up-to-date the information related to the Contractor's and proposed individuals' sites or premises for the following addresses:

Street Number / Street Name, Unit / Suite / Apartment Number
City, Province, Territory / State
Postal Code / Zip Code
Country

7.3.2.2 The Company Security Officer must ensure through the Contract Security Program that the Contractor and individuals hold a valid security clearance at the required level.

7.4 Term of Contract

7.4.1 Period of the Contract

The period of the Contract is for exactly one year, starting at date of contract award.

7.4.2 Option to Extend the Contract

The Contractor grants to Canada the irrevocable option to extend the term of the Contract by up to six (6) additional one (1) year periods under the same conditions. The Contractor agrees that, during the extended period of the Contract, it will be paid in accordance with the applicable provisions as set out in the Basis of Payment.

Canada may exercise this option at any time by sending a written notice to the Contractor at least fifteen calendar days before the expiry date of the Contract. The option may only be exercised by the Contracting Authority, and will be evidenced for administrative purposes only, through a contract amendment.

7.5 Authorities

7.5.1 Contracting Authority

The Contracting Authority for the Contract is: *(To be determined at contract award)*

Name: _____
Title: _____
Employment and Social Development Canada
Directorate: _____
Address: _____
Telephone: ___-___-_____
E-mail address: _____
The Contracting Authority is responsible for the management of the Contract and any changes to the Contract must be authorized in writing by the Contracting Authority. The Contractor must not perform work in excess of or outside the scope of the Contract based on verbal or written requests or instructions from anybody other than the Contracting Authority.

7.5.2 Project Authority

The Project Authority for the Contract is: *(To be determined at contract award)*

Name: _____
Title: _____
Employment and Social Development Canada
Address: _____
Telephone: ___-___-_____
E-mail address: _____

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

7.5.3 Contractor's Representative *(To be determined at contract award)*

Name: _____
Title: _____
Company: _____
Address: _____
Telephone: ___-___-_____
E-mail address: _____

7.6 Proactive Disclosure of Contracts with Former Public Servants

By providing information on its status, with respect to being a former public servant in receipt of a *Public Service Superannuation Act* (PSSA) pension, the Contractor has agreed that this information will be reported on departmental websites as part of the published proactive disclosure reports, in accordance with Contracting Policy Notice: 2019-01 of the Treasury Board Secretariat of Canada.

7.7 Payment

7.7.1 Basis of Payment – Professional Services

The Contractor will be paid for the Work specified in the authorized task authorization, in accordance with the Basis of payment at annex C.

Canada's liability to the Contractor under the authorized task authorization must not exceed the limitation of expenditure specified in the authorized task authorization. Custom duties are included and Applicable Taxes are extra.

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

7.7.2 Basis of Payment – Training Services

In consideration of the Contractor satisfactorily completing all of its obligations under the authorized Task Authorization (TA), the Contractor will be paid the firm unit price in accordance with the basis of payment, in Annex C, as specified in the authorized TA. Customs duties are included and Applicable Taxes are extra.

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

7.7.3 Basis of Payment – Firm Unit Price for the Software as a Service (SaaS) Solution Annual Subscriptions

In consideration of the Contractor satisfactorily completing all of its obligations under the contract, the Contractor will be paid the firm unit price in accordance with the basis of payment, in Annex C. Customs duties are included and Applicable Taxes are extra.

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

7.7.4 Limitation of Expenditure - Cumulative Total of all Task Authorizations

1. Canada's total liability to the Contractor under the Contract for all authorized Task Authorizations (TAs), inclusive of any revisions, must not exceed the sum of $ _____ *(To be determined at contract award)*. Customs duties are included and Applicable Taxes are extra.

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

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

    a. when it is 75 percent committed, or
    b. four (4) months before the contract expiry date, or
    c. as soon as the Contractor considers that the sum is inadequate for the completion of the Work required in all authorized TAs, inclusive of any revisions,
    whichever comes first.

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

7.7.5 Method of Payment – Milestone Payments

Canada will make milestone payments in accordance with the Schedule of Milestones detailed in the basis of payment in Annex C and the payment provisions of the Contract if:

a. an accurate and complete claim for payment and any other document required by the Contract have been submitted in accordance with the invoicing instructions provided in the Contract;
b. all work associated with the milestone and as applicable any deliverable required has been completed and accepted by Canada.

7.7.6 Electronic Payment of Invoices – Contract

The Government of Canada is switching from cheques to direct deposit as primary payment method, an electronic transfer of funds deposited directly into your bank account. Direct deposit is faster, more convenient and more secure. Enroll for direct deposit or update the banking information you already have on file by sending your completed Direct Deposit Enrollment Form at the following email address: nc-cfob-dgapf-fournis-vendors-gd@hrsdc-rhdcc.gc.ca.

7.8 Invoicing Instructions

The Contractor must submit invoices in accordance with the section entitled "Invoice Submission" of the general conditions. Invoices cannot be submitted until all work identified in the invoice is completed.

7.9 Certifications and Additional Information

7.9.1 Compliance

Unless specified otherwise, the continuous compliance with the certifications provided by the Contractor in its bid or precedent to contract award, and the ongoing cooperation in providing additional information are conditions of the Contract and failure to comply will constitute the Contractor in default. Certifications are subject to verification by Canada during the entire period of the Contract.

7.10 Applicable Laws

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

7.11 Priority of Documents

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

(a) the Articles of Agreement;
(b) Annex A, ESDC - General Conditions (2022-04-07);
(c) Annex B, Statement of Work;
(d) Annex C, Basis of Payment;
(e) Annex D, Security Requirements Check List;
(f) Annex E, Electronic Payment Instruments;
(g) Annex F, Task Authorizations Form (including all of its annexes, if any);
(h) Annexe G, Service Level Agreements (SLA); and,
(i) the Contractor's bid dated _____, (*insert date of bid*) (*If the bid was clarified or amended, insert at the time of contract award:*", as clarified on _____" ***or*** ",as amended on _____" *and insert date(s) of clarification(s) or amendment(s)).*

7.12 Foreign Nationals (Canadian Contractor *OR* Foreign Contractor) *(To be determined at contract award)*

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

OR

The Contractor must comply with Canadian immigration legislation applicable to foreign nationals entering Canada to work temporarily in fulfillment of the Contract. If the Contractor wishes to hire a foreign national to work in Canada to fulfill the Contract, the Contractor should immediately contact the nearest Canadian Embassy, Consulate or High Commission in the Contractor's country to obtain instructions, information on Citizenship and Immigration Canada's requirements and any required documents. The Contractor is responsible to ensure that foreign nationals have the required information, documents and authorizations before performing any work under the Contract in Canada. The Contractor is responsible for all costs incurred as a result of non-compliance with immigration requirements.

7.13 Insurance

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

7.14 Environmental Considerations

As part of the Greening Government Strategy (GGS), the Government of Canada is committed to aid the transition to a net-zero, circular economy through green procurement that includes life-cycle assessment principles and the adoption of clean technologies and green products and services. To align with departmental efforts to reduce

Canada's carbon footprint, when applicable, the Contractor should undertake the following measures to improve environmental performance and support the transition to a low-carbon economy:

a. Provide and transmit draft reports, final reports, other documents and bids in electronic format. Should printed material be required, double-sided printing in black and white format is the default.
b. Provide printed material on a minimum recycled content of 30% and/or certified as originating from a sustainably managed forest.
c. Recycle unneeded printed documents (in accordance with Security Requirements).
d. Use video and/or teleconferencing where possible to cut down unnecessary travel.
e. Use of public/green transit where feasible.
f. Use of Properties with Environmental Ratings, including accommodations while travelling.
g. Take actions to reduce the amount of fuel consumed by its vehicles. This can include such provisions as promoting good driving behaviour (eg - anti-idling, speed, car-sharing initiatives, green driving habits, etc) and purchasing fuel efficient and hybrid vehicles.
h. Select and operate IT and office equipment in a manner that reduces energy consumption and material usage.
i. Use and/or provide consumables that minimize environmental impacts through reduce, recycle, reuse and elimination of packaging.

7.15 Dispute Resolution

a. The parties agree to maintain open and honest communication about the Work throughout and after the performance of the contract.
b. The parties agree to consult and co-operate with each other in the furtherance of the contract and promptly notify the other party or parties and attempt to resolve problems or differences that may arise.
c. If the parties cannot resolve a dispute through consultation and cooperation, the parties agree to consult a neutral third party offering alternative dispute resolution services to attempt to address the dispute.
d. Options of alternative dispute resolution services can be found on Canada's Buy and Sell website under the heading "Dispute Resolution".

ANNEX A

ESDC - GENERAL CONDITIONS (2022-04-07)

Table of Content

01 Interpretation

In the Contract, unless the context otherwise requires:

"Applicable Taxes" means the Goods and Services Tax (GST), the Harmonized Sales Tax (HST), and any provincial tax, by law, payable by Canada such as, the Quebec Sales Tax (QST) as of April 1, 2013;

"Articles of Agreement" means the clauses and conditions incorporated in full text or incorporated by reference from the *Standard Acquisition Clauses and Conditions Manual* to form the body of the Contract; it does not include these general conditions, any supplemental general conditions, annexes, the Contractor's bid or any other document;

"Canada", "Crown", "Her Majesty" or "the Government" means Her Majesty the Queen in right of Canada as represented by the Minister of Employment and Social Development Canada (ESDC) and any other person duly authorized to act on behalf of that minister;

"Contract" means the Articles of Agreement, these general conditions, any supplemental general conditions, annexes and any other document specified or referred to as forming part of the Contract, all as amended by agreement of the Parties from time to time;

"Contracting Authority" means the person designated by that title in the Contract, or by notice to the Contractor, to act as Canada's representative to manage the Contract;

"Contractor" means the person, entity or entities named in the Contract to supply goods, services or both to Canada;

"Contract Price" means the amount stated in the Contract to be payable to the Contractor for the Work, exclusive of Applicable Taxes;

"Cost" means cost determined according to Contract Cost Principles 1031-2 as revised to the date of the bid solicitation or, if there was no bid solicitation, the date of the Contract;

"Government Property" means anything supplied to the Contractor by or on behalf of Canada for the purposes of performing the Contract and anything acquired by the Contractor in any manner in connection with the Work, the cost of which is paid by Canada under the Contract;

"Party" means Canada, the Contractor, or any other signatory to the Contract and "Parties" means all of them;

"Specifications" means the description of the essential, functional or technical requirements of the Work in the Contract, including the procedures for determining whether the requirements have been met;

"Total Estimated Cost", "Revised Estimated Cost", "Increase (Decrease)" on page 1 of the Contract or Contract Amendment means an amount used for internal administrative purposes only that comprises the Contract Price, or the revised Contract Price, or the amount that would increase or decrease the Contract Price and the Applicable Taxes as evaluated by the Contracting Authority, and does not constitute tax advice on the part of Canada;

"Work" means all the activities, services, goods, equipment, matters and things required to be done, delivered or performed by the Contractor under the Contract.

02 Standard clauses and conditions

Pursuant to the *Department of Public Works and Government Services Act*, S.C. 1996, c. 16, the clauses and conditions identified by number, date and title in the Contract are incorporated by reference and form part of the Contract as though expressly set out in the Contract.

03 Powers of Canada

All rights, remedies, powers and discretions granted or acquired by Canada under the Contract or by law are cumulative, not exclusive.

04 Status of the Contractor

The Contractor is an independent contractor engaged by Canada to perform the Work. Nothing in the Contract is intended to create a partnership, a joint venture or an agency between Canada and the other Party or Parties. The Contractor must not represent itself as an agent or representative of Canada to anyone. Neither the Contractor nor any of its personnel is engaged as an employee or agent of Canada. The Contractor is responsible for all deductions and remittances required by law in relation to its employees.

05 Conduct of the Work

1. The Contractor represents and warrants that:
    a. it is competent to perform the Work;
    b. it has everything necessary to perform the Work, including the resources, facilities, labour, technology, equipment, and materials; and
    c. it has the necessary qualifications, including knowledge, skill, know-how and experience, and the ability to use them effectively to perform the Work.

2. The Contractor must:
    a. perform the Work diligently and efficiently;
    b. except for Government Property, supply everything necessary to perform the Work;
    c. use, as a minimum, quality assurance procedures, inspections and controls generally used and recognized by the industry to ensure the degree of quality required by the Contract;
    d. select and employ a sufficient number of qualified people;
    e. perform the Work in accordance with standards of quality acceptable to Canada and in full conformity with the Specifications and all the requirements of the Contract;
    f. provide effective and efficient supervision to ensure that the quality of workmanship meets the requirements of the Contract.

3. The Work must not be performed by any person who, in the opinion of Canada, is incompetent, unsuitable or has conducted himself/herself improperly.

4. All services rendered under the Contract must, at the time of acceptance, be free from defects in workmanship and conform to the requirements of the Contract. If the Contractor is required to correct or replace the Work or any part of the Work, it will be at no cost to Canada.

5. Canada's facilities, equipment and personnel are not available to the Contractor to perform the Work unless the Contract specifically provides for it. The Contractor is responsible for advising the Contracting Authority in advance if it requires access to Canada's facilities, equipment or personnel to perform the Work. The Contractor must comply and ensure that its employees and subcontractors comply with all security measures, standing orders, policies or other rules in force at the site where the Work is performed.

6. Unless the Contracting Authority orders the Contractor to suspend the Work or part of the Work pursuant to section 28, the Contractor must not stop or suspend the Work or part of the Work pending the settlement of any dispute between the Parties about the Contract.

7. The Contractor must provide all reports that are required by the Contract and any other information that Canada may reasonably require from time to time.

8. The Contractor is fully responsible for performing the Work. Canada will not be responsible for any negative consequences or extra costs if the Contractor follows any advice given by Canada unless the

Contracting Authority provides the advice to the Contractor in writing and includes a statement specifically relieving the Contractor of any responsibility for negative consequences or extra costs that might result from following the advice.

06 Subcontracts

1. Except as provided in subsection 2, the Contractor must obtain the Contracting Authority's written consent before subcontracting or permitting the subcontracting of any part of the Work. A subcontract includes a contract entered into by any subcontractor at any tier to perform any part of the Work.

2. The Contractor is not required to obtain consent for subcontracts specifically authorized in the Contract. The Contractor may also without the consent of the Contracting Authority:
    a. purchase "off-the-shelf" items and any standard articles and materials that are ordinarily produced by manufacturers in the normal course of business;
    b. subcontract any portion of the Work as is customary in the carrying out of similar contracts; and;
    c. permit its subcontractors at any tier to make purchases or subcontract as permitted in paragraphs (a) and (b).

3. In any subcontract other than a subcontract referred to in paragraph 2.(a), the Contractor must, unless the Contracting Authority agrees in writing, ensure that the subcontractor is bound by conditions compatible with and, in the opinion of the Contracting Authority, not less favourable to Canada than the conditions of the Contract, with the exception of requirements under the Federal Contractors Program for employment equity which only apply to the Contractor.

4. Even if Canada consents to a subcontract, the Contractor is responsible for performing the Contract and Canada is not responsible to any subcontractor. The Contractor is responsible for any matters or things done or provided by any subcontractor under the Contract and for paying any subcontractors for any part of the Work they perform.

07 Specifications

1. All Specifications provided by Canada or on behalf of Canada to the Contractor in connection with the Contract belong to Canada and must be used by the Contractor only for the purpose of performing the Work.

2. If the Contract provides that Specifications furnished by the Contractor must be approved by Canada, that approval will not relieve the Contractor of its responsibility to meet all requirements of the Contract.

08 Replacement of specific individuals

1. If specific individuals are identified in the Contract to perform the Work, the Contractor must provide the services of those individuals unless the Contractor is unable to do so for reasons beyond its control.

2. If the Contractor is unable to provide the services of any specific individual identified in the Contract, it must provide a replacement with similar qualifications and experience. The replacement must meet the criteria used in the selection of the Contractor and be acceptable to Canada. The Contractor must, as soon as possible, give notice to the Contracting Authority of the reason for replacing the individual and provide:
    a. the name, qualifications and experience of the proposed replacement; and
    b. proof that the proposed replacement has the required security clearance granted by Canada, if applicable.

3. The Contractor must not, in any event, allow performance of the Work by unauthorized replacement persons. The Contracting Authority may order that a replacement stop performing the Work. In such a case, the Contractor must immediately comply with the order and secure a further replacement in accordance with subsection 2. The fact that the Contracting Authority does not order that a replacement

stop performing the Work does not relieve the Contractor from its responsibility to meet the requirements of the Contract.

09 Time of the essence

It is essential that the Work be performed within or at the time stated in the Contract.

10 Excusable delay

1. A delay in the performance by the Contractor of any obligation under the Contract that is caused by an event that

    a. is beyond the reasonable control of the Contractor,
    b. could not reasonably have been foreseen,
    c. could not reasonably have been prevented by means reasonably available to the Contractor, and
    d. occurred without the fault or neglect of the Contractor,

    will be considered an "Excusable Delay" if the Contractor advises the Contracting Authority of the occurrence of the delay or of the likelihood of the delay as soon as the Contractor becomes aware of it. The Contractor must also advise the Contracting Authority, within 15 working days, of all the circumstances relating to the delay and provide to the Contracting Authority for approval a clear work around plan explaining in detail the steps that the Contractor proposes to take in order to minimize the impact of the event causing the delay.

2. Any delivery date or other date that is directly affected by an Excusable Delay will be postponed for a reasonable time that will not exceed the duration of the Excusable Delay.

3. However, if an Excusable Delay has continued for 30 days or more, the Contracting Authority may, by giving notice in writing to the Contractor, terminate the Contract. In such a case, the Parties agree that neither will make any claim against the other for damages, costs, expected profits or any other loss arising out of the termination or the event that contributed to the Excusable Delay. The Contractor agrees to repay immediately to Canada the portion of any advance payment that is unliquidated at the date of the termination.

4. Unless Canada has caused the delay by failing to meet an obligation under the Contract, Canada will not be responsible for any costs incurred by the Contractor or any of its subcontractors or agents as a result of an Excusable Delay.

5. If the Contract is terminated under this section, the Contracting Authority may require the Contractor to deliver to Canada, in the manner and to the extent directed by the Contracting Authority, any completed parts of the Work not delivered and accepted before the termination and anything that the Contractor has acquired or produced specifically to perform the Contract. Canada will pay the Contractor:

    a. the value, of all completed parts of the Work delivered to and accepted by Canada, based on the Contract Price, including the proportionate part of the Contractor's profit or fee included in the Contract Price; and
    b. the Cost to the Contractor that Canada considers reasonable in respect of anything else delivered to and accepted by Canada.

    The total amount paid by Canada under the Contract to the date of termination and any amounts payable under this subsection must not exceed the Contract Price.

11 Inspection and acceptance of the Work

1. All the Work is subject to inspection and acceptance by Canada. Inspection and acceptance of the Work by Canada do not relieve the Contractor of its responsibility for defects or other failures to meet the requirements of the Contract. Canada will have the right to reject any Work that is not in accordance with the requirements of the Contract and require its correction or replacement at the Contractor's expense.

2. The Contractor must provide representatives of Canada access to all locations where any part of the Work is being performed at any time during working hours. Representatives of Canada may make examinations and such tests of the Work as they may think fit. The Contractor must provide all assistance and facilities, test pieces, samples and documentation that the representatives of Canada may reasonably require for the carrying out of the inspection. The Contractor must forward such test pieces and samples to such person or location as Canada specifies.

3. The Contractor must inspect and approve any part of the Work before submitting it for acceptance or delivering it to Canada. The Contractor must keep accurate and complete inspection records that must be made available to Canada on request. Representatives of Canada may make copies and take extracts of the records during the performance of the Contract and for up to three years after the end of the Contract.

12 Invoice submission

1. Invoices must be submitted, in the Contractor's name, to the Project or Technical Authority identified in the contract. The Contractor must submit invoices for each delivery or shipment; invoices must only apply to the Contract. Each invoice must indicate whether it covers partial or final delivery.

2. Invoices must show:

    a. the date, the name and address of the client, item or reference numbers, deliverable/description of the Work, contract number and financial code(s);
    b. details of expenditures (such as item, quantity, unit of issue, unit price, fixed time labour rates and level of effort, subcontracts, as applicable) in accordance with the Basis of Payment, exclusive of Applicable Taxes;
    c. deduction for holdback, if applicable;
    d. the extension of the totals, if applicable; and
    e. if applicable, the method of shipment together with date, case numbers and part or reference numbers, shipment charges and any other additional charges.

3. Applicable Taxes must be specified on all invoices as a separate item along with corresponding registration numbers from the tax authorities. All items that are zero-rated, exempt or to which Applicable Taxes do not apply, must be identified as such on all invoices.

4. By submitting an invoice, the Contractor certifies that the invoice is consistent with the Work delivered and is in accordance with the Contract.

13 Taxes

1. Federal government departments and agencies are required to pay Applicable Taxes.

2. Applicable Taxes will be paid by Canada as provided in the Invoice Submission section. It is the sole responsibility of the Contractor to charge Applicable Taxes at the correct rate in accordance with applicable legislation. The Contractor agrees to remit to appropriate tax authorities any amounts of Applicable Taxes paid or due.

3. The Contractor is not entitled to use Canada’s exemptions from any tax, such as provincial sales taxes, unless otherwise specified by law. The Contractor must pay applicable provincial sales tax, ancillary taxes, and any commodity tax, on taxable goods or services used or consumed in the performance of the Contract (in accordance with applicable legislation), including for material incorporated into real property.

4. In those cases where Applicable Taxes, customs duties, and excise taxes are included in the Contract Price, the Contract Price will be adjusted to reflect any increase, or decrease, of Applicable Taxes, customs duties, and excise taxes that will have occurred between bid submission and contract award. However, there will be no adjustment for any change to increase the Contract Price if public notice of the

change was given before bid submission date in sufficient detail to have permitted the Contractor to calculate the effect of the change.

5. Tax Withholding of 15 Percent – Canada Revenue Agency

   Pursuant to the *Income Tax Act*, 1985, c. 1 (5th Supp.) and the *Income Tax Regulations*, Canada must withhold 15 percent of the amount to be paid to the Contractor in respect of services provided in Canada if the Contractor is not a resident of Canada, unless the Contractor obtains a valid waiver from the *Canada Revenue Agency*. The amount withheld will be held on account for the Contractor in respect to any tax liability which may be owed to Canada.

14 Transportation costs

If transportation costs are payable by Canada under the Contract and the Contractor makes the transportation arrangements, shipments must be made by the most direct and economical means consistent with normal shipping practice. The costs must be shown as a separate item on the invoice.

15 Transportation carriers' liability

The federal government's policy of underwriting its own risks precludes payment of insurance or valuation charges for transportation beyond the point at which ownership of goods passes to the federal government (determined by the FOB point or Incoterms). Where increased carrier liability is available without charge, the Contractor must obtain the increased liability for shipment.

16 Payment period

1. Canada's standard payment period is 30 days. The payment period is measured from the date an invoice in acceptable form and content is received in accordance with the Contract or the date the Work is delivered in acceptable condition as required in the Contract, whichever is later. A payment is considered overdue on the 31st day following that date and interest will be paid automatically in accordance with the section 17.

2. If the content of the invoice and its substantiating documentation are not in accordance with the Contract or the Work is not in acceptable condition, Canada will notify the Contractor within 15 days of receipt. The 30-day payment period begins upon receipt of the revised invoice or the replacement or corrected Work. Failure by Canada to notify the Contractor within 15 days will only result in the date specified in subsection 1 to apply for the sole purpose of calculating interest on overdue accounts.

17 Interest on overdue accounts

1. For the purpose of this section:

   "Average Rate" means the simple arithmetic mean of the Bank Rates in effect at 4:00 p.m. Eastern Time each day during the calendar month immediately before the calendar month in which payment is made;

   "Bank Rate" means the rate of interest established from time to time by the Bank of Canada as the minimum rate at which the Bank of Canada makes short term advances to members of the Canadian Payments Association;

   "date of payment" means the date of the negotiable instrument drawn by the Receiver General for Canada to pay any amount under the Contract;

   an amount becomes **"overdue"** when it is unpaid on the first day following the day on which it is due and payable according to the Contract.

2. Canada will pay to the Contractor simple interest at the Average Rate plus 3 percent per year on any amount that is overdue, from the date that amount becomes overdue until the day before the date of payment, inclusive. The Contractor is not required to provide notice to Canada for interest to be payable.

3. Canada will pay interest in accordance with this section only if Canada is responsible for the delay in paying the Contractor. Canada will not pay interest on overdue advance payments.

18 Compliance with applicable laws

1. The Contractor must comply with all laws applicable to the performance of the Contract. The Contractor must provide evidence of compliance with such laws to Canada at such times as Canada may reasonably request.

2. The Contractor must obtain and maintain at its own cost all permits, licenses, regulatory approvals and certificates required to perform the Work. If requested by the Contracting Authority, the Contractor must provide a copy of any required permit, license, regulatory approvals or certificate to Canada.

19 Ownership

1. Unless provided otherwise in the Contract, the Work or any part of the Work belongs to Canada after delivery and acceptance by or on behalf of Canada.

2. However if any payment is made to the Contractor for or on account of any Work, either by way of progress or milestone payments, that work paid for by Canada belongs to Canada upon such payment being made. This transfer of ownership does not constitute acceptance by Canada of the Work or any part of the Work and does not relieve the Contractor of its obligation to perform the Work in accordance with the Contract.

3. Despite any transfer of ownership, the Contractor is responsible for any loss or damage to the Work or any part of the Work until it is delivered to Canada in accordance with the Contract. Even after delivery, the Contractor remains responsible for any loss or damage to any part of the Work caused by the Contractor or any subcontractor.

4. Upon transfer of ownership to the Work or any part of the Work to Canada, the Contractor must, if requested by Canada, establish to Canada's satisfaction that the title is free and clear of all claims, liens, attachments, charges or encumbrances. The Contractor must execute any conveyances and other instruments necessary to perfect the title that Canada may require.

20 Translation of documentation

The Contractor agrees that Canada may translate in the other official language any documentation delivered to Canada by the Contractor that does not belong to Canada. The Contractor acknowledges that Canada owns the translation and that it is under no obligation to provide any translation to the Contractor. Canada agrees that any translation must include any copyright notice and any proprietary right notice that was part of the original. Canada acknowledges that the Contractor is not responsible for any technical errors or other problems that may arise as a result of the translation.

21 Confidentiality

1. The Contractor must keep confidential all information provided to the Contractor by or on behalf of Canada in connection with the Work, including any information that is confidential or proprietary to third parties, and all information conceived, developed or produced by the Contractor as part of the Work when copyright or any other intellectual property rights in such information belongs to Canada under the Contract. The Contractor must not disclose any such information without the written permission of Canada. The Contractor may disclose to a subcontractor any information necessary to perform the subcontract as long as the subcontractor agrees to keep the information confidential and that it will be used only to perform the subcontract.

2. The Contractor agrees to use any information provided to the Contractor by or on behalf of Canada only for the purpose of the Contract. The Contractor acknowledges that all this information remains the property of Canada or the third party, as the case may be. Unless provided otherwise in the Contract, the Contractor must deliver to Canada all such information, together with every copy, draft, working paper and

note that contains such information, upon completion or termination of the Contract or at such earlier time as Canada may require.

3. Subject to the *Access to Information Act* , R.S., 1985, c. A-1, and to any right of Canada under the Contract to release or disclose, Canada must not release or disclose outside the Government of Canada any information delivered to Canada under the Contract that is proprietary to the Contractor or a subcontractor.

4. The obligations of the Parties set out in this section do not apply to any information if the information:
   a. is publicly available from a source other than the other Party; or
   b. is or becomes known to a Party from a source other than the other Party, except any source that is known to be under an obligation to the other Party not to disclose the information; or
   c. is developed by a Party without use of the information of the other Party.

5. Wherever possible, the Contractor must mark or identify any proprietary information delivered to Canada under the Contract as "Property of (Contractor's name), permitted Government uses defined under Employment and Social Development Canada (ESDC) Contract No. (fill in Contract Number)". Canada will not be liable for any unauthorized use or disclosure of information that could have been so marked or identified and was not.

6. If the Contract, the Work, or any information referred to in subsection 1 is identified as TOP SECRET, SECRET, CONFIDENTIAL, PROTECTED, COSMIC TOP SECRET, NATO SECRET, NATO CONFIDENTIAL, or NATO RESTRICTED by Canada, the Contractor must at all times take all measures reasonably necessary for the safeguarding of the material so identified, including those set out in the *PWGSC Contract Security Manual* and its supplements and any other instructions issued by Canada.

7. If the Contract, the Work, or any information referred to in subsection 1 is identified as TOP SECRET, SECRET, CONFIDENTIAL, PROTECTED, COSMIC TOP SECRET, NATO SECRET, NATO CONFIDENTIAL, or NATO RESTRICTED by Canada, representatives of Canada are entitled to inspect the Contractor's premises and the premises of a subcontractor at any tier for security purposes at any time during the term of the Contract. The Contractor must comply with, and ensure that any subcontractor complies with, all written instructions issued by Canada dealing with the material so identified, including any requirement that employees of the Contractor or of any subcontractor execute and deliver declarations relating to reliability screenings, security clearances and other procedures.

22 Government Property

1. All Government Property must be used by the Contractor solely for the purpose of the Contract and remains the property of Canada. The Contractor must maintain adequate accounting records of all Government Property and, whenever feasible, mark it as being the property of Canada.

2. The Contractor must take reasonable and proper care of all Government Property while it is in its possession or subject to its control. The Contractor is responsible for any loss or damage resulting from its failure to do so other than loss or damage caused by ordinary wear and tear.

3. All Government Property, unless it is installed or incorporated in the Work, must be returned to Canada on demand. All scrap and all waste materials, articles or things that are Government Property must, unless provided otherwise in the Contract, remain the property of Canada and must be disposed of only as directed by Canada.

4. At the time of completion of the Contract, and if requested by the Contracting Authority, the Contractor must provide to Canada an inventory of all Government Property relating to the Contract.

23 Liability

The Contractor is liable for any damage caused by the Contractor, its employees, subcontractors, or agents to Canada or any third party. Canada is liable for any damage caused by Canada, its employees or agents to the

Contractor or any third party. The Parties agree that no limitation of liability or indemnity provision applies to the Contract unless it is specifically incorporated in full text in the Articles of Agreement. Damage includes any injury to persons (including injury resulting in death) or loss of or damage to property (including real property) caused as a result of or during the performance of the Contract.

24 Intellectual property infringement and royalties

1. The Contractor represents and warrants that, to the best of its knowledge, neither it nor Canada will infringe any third party's intellectual property rights in performing or using the Work, and that Canada will have no obligation to pay royalties of any kind to anyone in connection with the Work.

2. If anyone makes a claim against Canada or the Contractor concerning intellectual property infringement or royalties related to the Work, that Party agrees to notify the other Party in writing immediately. If anyone brings a claim against Canada, according to *Department of Justice Act*, R.S., 1985, c. J-2, the Attorney General of Canada must have the regulation and conduct of all litigation for or against Canada, but the Attorney General may request that the Contractor defend Canada against the claim. In either case, the Contractor agrees to participate fully in the defence and any settlement negotiations and to pay all costs, damages and legal costs incurred or payable as a result of the claim, including the amount of any settlement. Both Parties agree not to settle any claim unless the other Party first approves the settlement in writing.

3. The Contractor has no obligation regarding claims that were only made because:
    a. Canada modified the Work or part of the Work without the Contractor's consent or used the Work or part of the Work without following a requirement of the Contract; or
    b. Canada used the Work or part of the Work with a product that the Contractor did not supply under the Contract (unless that use is described in the Contract or the manufacturer's specifications or other documentation); or
    c. the Contractor used equipment, drawings, specifications or other information supplied to the Contractor by Canada (or by someone authorized by Canada); or
    d. the Contractor used a specific item of equipment or software that it obtained because of specific instructions from the Contracting Authority; however, this exception only applies if the Contractor has included the following language in its own contract with the supplier of that equipment or software: "[Supplier name] acknowledges that the purchased items will be used by the Government of Canada. If a third party claims that equipment or software supplied under this contract infringes any intellectual property right, [supplier name], if requested to do so by either [Contractor name] or Canada, will defend both [Contractor name] and Canada against that claim at its own expense and will pay all costs, damages and legal fees payable as a result of that infringement." Obtaining this protection from the supplier is the Contractor's responsibility and, if the Contractor does not do so, it will be responsible to Canada for the claim.

4. If anyone claims that, as a result of the Work, the Contractor or Canada is infringing its intellectual property rights, the Contractor must immediately do one of the following:
    a. take whatever steps are necessary to allow Canada to continue to use the allegedly infringing part of the Work; or
    b. modify or replace the Work to avoid intellectual property infringement, while ensuring that the Work continues to meet all the requirements of the Contract; or
    c. take back the Work and refund any part of the Contract Price that Canada has already paid.

    If the Contractor determines that none of these alternatives can reasonably be achieved, or if the Contractor fails to take any of these steps within a reasonable amount of time, Canada may choose either to require the Contractor to do (c), or to take whatever steps are necessary to acquire the rights to use the allegedly infringing part(s) of the Work itself, in which case the Contractor must reimburse Canada for all the costs it incurs to do so.

25 Amendment and waivers

1. To be effective, any amendment to the Contract must be done in writing by the Contracting Authority and the authorized representative of the Contractor.

2. While the Contractor may discuss any proposed modifications to the Work with other representatives of Canada, Canada will not be responsible for the cost of any modification unless it has been incorporated into the Contract in accordance with subsection 1.

3. A waiver will only be valid, binding or affect the rights of the Parties if it is made in writing by, in the case of a waiver by Canada, the Contracting Authority and, in the case of a waiver by the Contractor, the authorized representative of the Contractor.

4. The waiver by a Party of a breach of any condition of the Contract will not be treated or interpreted as a waiver of any subsequent breach and therefore will not prevent that Party from enforcing of that term or condition in the case of a subsequent breach.

26 Assignment

1. The Contractor must not assign the Contract without first obtaining the written consent of the Contracting Authority. Any assignment made without that consent is void and will have no effect. The assignment will be effective upon execution of an assignment agreement signed by the Parties and the assignee.

2. Assignment of the Contract does not relieve the Contractor from any obligation under the Contract and it does not impose any liability upon Canada.

27 Suspension of the Work

1. The Contracting Authority may at any time, by written notice, order the Contractor to suspend or stop the Work or part of the Work under the Contract for a period of up to 180 days. The Contractor must immediately comply with any such order in a way that minimizes the cost of doing so. While such an order is in effect, the Contractor must not remove any part of the Work from any premises without first obtaining the written consent of the Contracting Authority. Within these 180 days, the Contracting Authority must either cancel the order or terminate the Contract, in whole or in part, under section 29 or section 30.

2. When an order is made under subsection 1, unless the Contracting Authority terminates the Contract by reason of default by the Contractor or the Contractor abandons the Contract, the Contractor will be entitled to be paid its additional costs incurred as a result of the suspension plus a fair and reasonable profit.

3. When an order made under subsection 1 is cancelled, the Contractor must resume work in accordance with the Contract as soon as practicable. If the suspension has affected the Contractor's ability to meet any delivery date under the Contract, the date for performing the part of the Work affected by the suspension will be extended for a period equal to the period of suspension plus a period, if any, that in the opinion of the Contracting Authority, following consultation with the Contractor, is necessary for the Contractor to resume the Work. Any equitable adjustments will be made as necessary to any affected conditions of the Contract.

28 Default by the Contractor

1. If the Contractor is in default in carrying out any of its obligations under the Contract, the Contracting Authority may, by giving written notice to the Contractor, terminate for default the Contract or part of the Contract. The termination will take effect immediately or at the expiration of a cure period specified in the notice, if the Contractor has not cured the default to the satisfaction of the Contracting Authority within that cure period.

2. If the Contractor becomes bankrupt or insolvent, makes an assignment for the benefit of creditors, or takes the benefit of any statute relating to bankrupt or insolvent debtors, or if a receiver is appointed under a debt instrument or a receiving order is made against the Contractor, or an order is made or a resolution

passed for the winding-up of the Contractor, the Contracting Authority may, to the extent permitted by the laws of Canada, by giving written notice to the Contractor, immediately terminate for default the Contract or part of the Contract.

3. If Canada gives notice under subsection 1 or 2, the Contractor will have no claim for further payment except as provided in this section. The Contractor will be liable to Canada for all losses and damages suffered by Canada because of the default or occurrence upon which the notice was based, including any increase in the cost incurred by Canada in procuring the Work from another source. The Contractor agrees to repay immediately to Canada the portion of any advance payment that is unliquidated at the date of the termination.

4. Upon termination of the Contract under this section, the Contracting Authority may require the Contractor to deliver to Canada, in the manner and to the extent directed by the Contracting Authority, any completed parts of the Work, not delivered and accepted before the termination and anything the Contractor has acquired or produced specifically to perform the Contract. In such a case, subject to the deduction of any claim that Canada may have against the Contractor arising under the Contract or out of the termination, Canada will pay or credit to the Contractor:

    a. the value, of all completed parts of the Work delivered to and accepted by Canada, based on the Contract Price, including the proportionate part of the Contractor's profit or fee included in the Contract Price; and
    b. the cost to the Contractor that Canada considers reasonable in respect of anything else delivered to and accepted by Canada.

    The total amount paid by Canada under the Contract to the date of the termination and any amount payable under this subsection must not exceed the Contract Price.

5. Title to everything for which payment is made to the Contractor will, once payment is made, pass to Canada unless it already belongs to Canada under any other provision of the Contract.

6. If the Contract is terminated for default under subsection 1, but it is later determined that grounds did not exist for a termination for default, the notice will be considered a notice of termination for convenience issued under subsection 1 of section 30.

29 Termination for convenience

1. At any time before the completion of the Work, the Contracting Authority may, by giving notice in writing to the Contractor, terminate for convenience the Contract or part of the Contract. Once such a notice of termination for convenience is given, the Contractor must comply with the requirements of the termination notice. If the Contract is terminated in part only, the Contractor must proceed to complete any part of the Work that is not affected by the termination notice. The termination will take effect immediately or, as the case may be, at the time specified in the termination notice.

2. If a termination notice is given pursuant to subsection 1, the Contractor will be entitled to be paid, for costs that have been reasonably and properly incurred to perform the Contract to the extent that the Contractor has not already been paid or reimbursed by Canada. The Contractor agrees that it will only be paid the following amounts:

    a. on the basis of the Contract Price, for any part of the Work completed that is inspected and accepted in accordance with the Contract, whether completed before, or after the termination in accordance with the instructions contained in the termination notice;
    b. the Cost incurred by the Contractor plus a fair and reasonable profit thereon as determined by Canada in accordance with the profit provisions found in PWGSC Supply Manual section 10.65 Calculation of profit on negotiated contracts, for any part of the Work commenced, but not completed, prior to the date of the termination notice. The Contractor agrees that it is not entitled to any anticipated profit on any part of the Contract terminated; and

c. all costs incidental to the termination of the Work incurred by the Contractor but not including the cost of severance payments or damages to employees whose services are no longer required, except wages that the Contractor is obligated by statute to pay.

3. Canada may reduce the payment in respect of any part of the Work, if upon inspection, it does not meet the requirements of the Contract.

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

30 Accounts and audit

1. The Contractor must keep proper accounts and records of the cost of performing the Work and of all expenditures or commitments made by the Contractor in connection with the Work, including all invoices, receipts and vouchers. The Contractor must retain records, including bills of lading and other evidence of transportation or delivery, for all deliveries made under the Contract.

2. If the Contract includes payment for time spent by the Contractor, its employees, representatives, agents or subcontractors performing the Work, the Contractor must keep a record of the actual time spent each day by each individual performing any part of the Work.

3. Unless Canada has consented in writing to its disposal, the Contractor must retain all the information described in this section for six years after it receives the final payment under the Contract, or until the settlement of all outstanding claims and disputes, whichever is later. During this time, the Contractor must make this information available for audit, inspection and examination by the representatives of Canada, who may make copies and take extracts. The Contractor must provide all reasonably required facilities for any audit and inspection and must furnish all the information as the representatives of Canada may from time to time require to perform a complete audit of the Contract.

4. The amount claimed under the contract, calculated in accordance with the Basis of Payment provision in the Articles of Agreement, is subject to government audit both before and after payment is made. If an audit is performed after payment, the Contractor agrees to repay any overpayment immediately on demand by Canada. Canada may hold back, deduct and set off any credits owing and unpaid under this section from any money that Canada owes to the Contractor at any time (including under other contracts). If Canada does not choose to exercise this right at any given time, Canada does not lose this right.

31 Right of set-off

Without restricting any right of set-off given by law, Canada may set-off against any amount payable to the Contractor under the Contract, any amount payable to Canada by the Contractor under the Contract or under any other current contract. Canada may, when making a payment pursuant to the Contract, deduct from the amount payable to the Contractor any such amount payable to Canada by the Contractor which, by virtue of the right of set-off, may be retained by Canada.

32 Notice

Any notice under the Contract must be in writing and may be delivered by hand, courier, mail, facsimile or other electronic method that provides a paper record of the text of the notice. It must be sent to the Party for whom it is intended at the address stated in the Contract. Any notice will be effective on the day it is received at that address. Any notice to Canada must be delivered to the Contracting Authority.

33 Conflict of interest and Values and Ethics Codes for the Public Service

The Contractor acknowledges that individuals who are subject to the provisions of the *Conflict of interest Act*, 2006, c. 9, s. 2, the *Conflict of interest Code for Members of the House of Commons*, the *Values and Ethics*

Code for the Public Service or all other codes of values and ethics applicable within specific organizations cannot derive any direct benefit resulting from the Contract.

34 No bribe or conflict

1. The Contractor declares that no bribe, gift, benefit, or other inducement has been or will be paid, given, promised or offered directly or indirectly to any official or employee of Canada or to a member of the family of such a person, with a view to influencing the entry into the Contract or the administration of the Contract.

2. The Contractor must not influence, seek to influence or otherwise take part in a decision of Canada knowing that the decision might further its private interest. The Contractor must have no financial interest in the business of a third party that causes or would appear to cause a conflict of interest in connection with the performance of its obligations under the Contract. If such a financial interest is acquired during the period of the Contract, the Contractor must immediately declare it to the Contracting Authority.

3. The Contractor warrants that, to the best of its knowledge after making diligent inquiry, no conflict exists or is likely to arise in the performance of the Contract. In the event the Contractor becomes aware of any matter that causes or is likely to cause a conflict in relation to the Contractor's performance under the Contract, the Contractor must immediately disclose such matter to the Contracting Authority in writing.

4. If the Contracting Authority is of the opinion that a conflict exists as a result of the Contractor's disclosure or as a result of any other information brought to the Contracting Authority's attention, the Contracting Authority may require the Contractor to take steps to resolve or otherwise deal with the conflict or, at its entire discretion, terminate the Contract for default. Conflict means any matter, circumstance, interest, or activity affecting the Contractor, its personnel or subcontractors, which may or may appear to impair the ability of the Contractor to perform the Work diligently and independently.

35 Survival

All the Parties' obligations of confidentiality, representations and warranties set out in the Contract as well as the provisions, which by the nature of the rights or obligations might reasonably be expected to survive, will survive the expiry or termination of the Contract.

36 Severability

If any provision of the Contract is declared by a court of competent jurisdiction to be invalid, illegal or unenforceable, that provision will be removed from the Contract without affecting any other provision of the Contract.

37 Successors and assigns

The Contract is to the benefit of and binds the successors and permitted assignees of Canada and of the Contractor.

38 Contingency fees

The Contractor certifies that it has not directly or indirectly, paid or agreed to pay and agrees that it will not, directly or indirectly, pay a contingency fee for the solicitation, negotiation or obtaining of the Contract to any person, other than an employee of the Contractor acting in the normal course of the employee's duties. In this section, "contingency fee" means any payment or other compensation that depends or is calculated based on a degree of success in soliciting, negotiating or obtaining the Contract and "person" includes any individual who is required to file a return with the registrar pursuant to section 5 of the *Lobbying Act*, 1985, c. 44 (4th Supplement).

39 International sanctions

1. Persons in Canada, and Canadians outside of Canada, are bound by economic sanctions imposed by Canada. As a result, the Government of Canada cannot accept delivery of goods or services that originate, either directly or indirectly, from the countries or persons subject to economic sanctions.

2. The Contractor must not supply to the Government of Canada any goods or services which are subject to economic sanctions.

3. The Contractor must comply with changes to the regulations imposed during the period of the Contract. The Contractor must immediately advise Canada if it is unable to perform the Work as a result of the imposition of economic sanctions against a country or person or the addition of a good or service to the list of sanctioned goods or services. If the Parties cannot agree on a work around plan, the Contract will be terminated for the convenience of Canada in accordance with section 30.

40 Integrity provisions—contract

The *Ineligibility and Suspension Policy* (the "Policy") and all related Directives incorporated by reference into the bid solicitation on its closing date are incorporated into, and form a binding part of the Contract. The Contractor must comply with the provisions of the Policy and Directives, which can be found on Public Works and Government Services Canada's website at *Ineligibility and Suspension Policy*.

41 Harassment in the workplace

1. The Contractor acknowledges the responsibility of Canada to ensure, for its employees, a healthy work environment, free of harassment. A copy of the *Policy on Harassment Prevention and Resolution*, which is also applicable to the Contractor, is available on the Treasury Board Web site.

2. The Contractor must not, either as an individual, or as a corporate or unincorporated entity, through its employees or subcontractors, harass, abuse, threaten, discriminate against or intimidate any employee, contractor or other individual employed by, or under contract with Canada. The Contractor will be advised in writing of any complaint and will have the right to respond in writing. Upon receipt of the Contractor's response, the Contracting Authority will, at its entire discretion, determine if the complaint is founded and decide on any action to be taken.

42 Entire agreement

The Contract constitutes the entire and only agreement between the Parties and supersedes all previous negotiations, communications and other agreements, whether written or oral, unless they are incorporated by reference in the Contract. There are no terms, covenants, representations, statements or conditions binding on the Parties other than those contained in the Contract.

43 Access to information

Records created by the Contractor, and under the control of Canada, are subject to the *Access to Information Act*. The Contractor acknowledges the responsibilities of Canada under the *Access to Information Act* and must, to the extent possible, assist Canada in discharging these responsibilities. Furthermore, the Contractor acknowledges that section 67.1 of the *Access to Information Act* provides that any person, who destroys, alters, falsifies or conceals a record, or directs anyone to do so, with the intent of obstructing the right of access that is provided by the *Access to Information Act* is guilty of an offence and is liable to imprisonment or a fine, or both.

44 Code of Conduct for Procurement—Contract

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

ANNEX B

STATEMENT OF WORK

1. Background

1.1 The Organizational Chart is an integral component of Organizational Design and Classification and Human Resources (HR) for Managers and Senior Management. It gives an accurate and timely view of an organization, the number and type of positions within that organization, and the relationship between positions in an organization. It also allows managers to organize their teams with clear responsibilities, titles and lines of authority and provides Human Resources with additional information on the type of job, mandate, program and work performed.

1.2 Ensuring accurate and efficient capture of an organization's current status, change and/or development and evolution is a complex, labour-intensive, and often unreliable, undertaking for both the Human Resources Services Branch (HRSB) and its clients. Currently, there is no enterprise solution no standardized method or approach within Employment and Social Development Canada (ESDC) on creating, developing, and maintaining the organization chart by the clients. Generally, a chart may be produced using a variety of software options, each requiring varying levels of effort, understanding, efficiency, appearance, and access to or availability within ESDC such as: Visio, Power Point, Excel, Org Plus, Adobe PDF and Word. At this time, only the Center of Expertise in organisational design and classification has the tools, capacity and the know-how to produce the organization charts, however, given the size of the department, it takes a little over 2 months to have them completed department-wide which is why they are only produced twice a year.

1.3 Urgency for ESDC Organization Chart Software SaaS Solution has been increased due to the government-wide Classification Program Renewal Initiative, established to **modernize all aspects of classification** (the infrastructure). The Classification Program, managed by the Workforce, Organization and Classification (WOC) Directorate within the Office of the Chief Human Resources Officer (OCHRO) at the Treasury Board of Canada Secretariat (TBS) mandates all departments to comply with its renewed direction.

1.4 HRSB is requesting an Organization Chart Software SaaS Solution; an automated and user-friendly approach for creating, developing and maintaining organization charts that should support PeopleSoft processes and could be used by both HRSB and the clients. Automating the organization chart function will enable a significant reduction in time and money to the department and increase department-wide organizational understanding and analysis ability. It will provide a single source of truth and will allow everyone to access the same organizational picture, which currently does not exist.

2. Scope of Work Overview

2.1 Objectives

2.1.1 The Contractor must meet the stated objectives as part of the requirements identified in this Statement of Work. ESDC will support the Contractor with Subject Matter Experts where necessary to achieve the following stated goals and objectives:

a) Enable nimble and informed decision making,
b) Enable recruitment and retention of employees with the right competencies,
c) Enable effective management and use of available organizational information and data; and,
d) Provide Managers and HR Classification with a shared organization chart that accurately represents the hierarchical and functional relationships of a specific team/organization, division, directorate, branch, and/or portfolio, the vacancies and official language capacity to deliver the services.

2.2 Overview

2.2.1 Requirements

2.2.1.1 Software as a Service. The Contractor will provide the Solution through a Software as a Service ("SaaS") delivery model, allowing Canada to access and use the Solution which is hosted by the Contractor. The SaaS solution must be delivered in accordance with the milestones and respective dates as documented in the *Table 1: Master Project Schedule Summary (7.1.3)* or an equivalent schedule proposed by the Contractor and approved by ESDC.

2.2.1.2 Commercially-Available Solution. ESDC acknowledges that the SaaS Solution is a commercially-available solution provided to other customers. As part of the subscription to use the Solution, the Contractor agrees to make available to ESDC all the features and functionalities included in the commercially available version of the Solution, and be responsible for the incidental and required information technology infrastructure services required to deliver the Solution, all of which is included in the subscription price.

2.2.1.3 Improvements to and Evolution of the Solution: Features or Functionalities.
ESDC acknowledges that the SaaS solution, underlying software application or associated infrastructure may evolve during the course of the Contract Period. The Contractor agrees to continue to provide the Services as the commercially available Solution, with functionality or features with terms that are materially no less favorable than as at the time of Contract award.

The parties acknowledge that technology and business models evolve quickly and that any SaaS solution provided at the beginning of the Contract Period inevitably will be different from the Solution provided at the end of the Contract Period and the method(s) by which the SaaS solution and any potential peripheral systems are provided to ESDC are likely to change or evolve, and that, at the time of entering into this Contract, the parties cannot possibly contemplate all the goods or services that may be delivered under this Contract, other than they will be connected to delivering to Users. With that in mind, the parties agree that:

a) The Contractor must maintain and continuously improve the SaaS solution and infrastructure throughout the Contract Period on a commercially reasonable basis, and must provide those improvements and enhancements to ESDC as part of ESDC's subscription, with no price adjustment if those improvements and enhancements are also offered to other customers at no additional cost.
b) If the Contractor removes any functions from the commercial offering to the SaaS solution and offers those functions in any new or other services or products, the Contractor must continue to provide those functions to ESDC as part of ESDC's subscription to the Services, under the existing terms and conditions of the Contract regardless of whether those other services or products also contain new or additional functions. The Contractor has no obligation to comply with this paragraph if the SaaS solution acquired by ESDC is still offered by Contractor in parallel with the new services offered to other customers.

2.2.1.4 Core Functionality

a) The proposed SaaS solution must be able to:

- Automates the production of the organization chart in real-time with functionality to easily enable manual manipulation, updates and amendments to support organizational development, design and capacity planning requirements while complying with the statutory obligations under the *Privacy Act* and *Access to Information Act*;
- Provide capability of developing and storing "what-if scenarios" in the SaaS Solution to support organizational change management including but not limited to compliance with TBS' Classification Program Renewal Initiative (ex. IT, PA Conversion);

- Provide access to the current and "what-if scenarios" organization chart in both English and French as required to both HR Delegated Managers and HR Classification staff using security controls to restrict access where required; ie. defining specific roles (HR Delegated Manager, Classification Specialist, Classification Supervisor etc.);
- Provide capability to support 2,000 concurrent users;
- Provide workflow capability and Mobile Device Management capabilities for platforms such as smartphones, tablets, Android, etc. to allow HR Delegated Managers and the HR Classification staff to collaborate and share organizational changes prior to submission for approval;
- The proposed SaaS Solution must conform to accessibility guidelines as set out in the latest standards on accessibility as defined under the ETSI EN 301 549 - V3.2.1 - Accessibility requirements for ICT products and services specifically clauses 9.1 – 9.4 – Web (includes WCAG 2.1 Level AA), 10.0 General – Non Web documents (ie. PDF) and 12.1 – Product documentation (training);
- Have data centers located in Canada and in a wholly Canadian region;
- Provide a SaaS Solution that meets all requirements as identified in this Statement of Work. These include the configuration, setup, deployment, integration testing and training, as well as necessary maintenance and support of the Organization Chart SaaS solution for the agreed time periods;
- Support minimal configuration changes such as text or label changes where feasible.

b) Integration Testing between the SaaS solution and ESDC HR ERP System

- The SaaS Solution must provide a well established capability to integrate with ESDC's existing PeopleSoft 9.2 HCM system to transfer data in and out and as and when required;
- The SaaS Solution must be capable of leveraging an ESDC active directory to provide Single Sign-On capabilities to provide a seamless end-user experience;
- The Contractor must configure and deploy the SaaS Solution as per the Acceptance Criteria defined in Section 5 - Testing and Implementation Services for the SaaS Solution (or its components thereof), and for document deliverables of the Statement of Work.

c) Service Levels

- Bidders must submit published service level agreements (SLA) that outline the service level agreements as per Annex G – Service Level Agreements (SLA).

d) Notifications

- Timely notification of any interruption that is expected to impact service availability and performance (as agreed to by the parties and included in the Statement of Work (SOW) and/or Service Level Agreement (SLA));
- Regular updates on the status of returning the SaaS solution to an operating state according to the agreed upon SLAs and system availability requirements, both as advance alerts and post-go-live alerts; and
- Information system security alerts, advisories, and directives via email for vulnerabilities that pose a threat to the SaaS solution.

e) Training

The Contractor must provide training to ESDC resources to assist users in comprehension of business processes and navigation and use of the new SaaS Solution. The training must be delivered through online or in-person training sessions, including training manuals and instructional videos.

f) Security Requirements

- A phased approach will require the SaaS Solution to initially support Unclassified data.
- The subsequent phase (phase 2) would require the SaaS Solution to support data up to and including Protected B status. This second phase would see the SaaS Solution store Protected B data elements in the organization chart in addition to what was deployed in the initial phase. The Contractor must be able to meet the mandatory security obligations, for Tier 2 data (up to Protected B) to protect and secure ESDC data from unauthorized access, modification, or exfiltration as specified in Appendix A to Annex B: Security Obligations for Tier 2 (up to Protected B).

3. Project Management and Governance Services

3.1 Project Governance

3.1.1 The Contractor must work collaboratively with ESDC to develop a Contract Management Plan, which must comprise the project governance and Contract management structure that meets ESDC's requirements.

3.2 Project Planning

3.2.1 The formal start of the Project will commence with a Kick-off meeting that will be led by the Project Authority. This Kick-off meeting will take place after contract award between ESDC and the Contractor. The timing of the Kick-off meeting and all subsequent Project Deliverables will be in accordance with the high-level timelines indicated in Table 1: Master Project Schedule Summary identified in Section 7.1.3;

3.2.2 The Contractor must submit a preliminary Project Plan within 20 business days of the Kick-Off Meeting for approval by ESDC that identifies a schedule to complete the plans and the scope of work specified in this Statement of Work;

3.2.3 The Contractor must develop a detailed Project Plan against the timeline outlined in Table 1 - Master Project Schedule Summary against the Milestones and Deliverables for the work they will be completing, based on the Preliminary Project Plan as approved by ESDC;

3.3 Project Management Methodology and Plan

3.3.1 Following approval of the preliminary Project Plan for review and approval by the Project Authority; the Contractor must provide to the Project Authority a draft Project Management Plan, which includes the Implementation Plan that was proposed as part of the Contractor's bid submission; which should then be applied to the detailed Project Plan. This should meet the details outlined in Section Master Project Schedule Summary;

3.3.2 Once the detailed project plan has been reviewed and approved by the Project Authority, the project management plan must address and integrate all the key project management knowledge areas as defined in frameworks such as PMBOK edition 5 or PRINCE2 and must include sections covering, but not limited to, the following:

a) Baselines for scope, schedule, and cost;

b) Management plans for scope, schedule, cost, quality, how the contractor will be working alongside ESDC resources, communications, risk, and procurement. These planning documents outline the management approach for dealing with such items as scope change, managing delivery to the approved baseline schedule, controlling project costs, defining and achieving project quality objectives, engaging and retaining the right resources and skills to the appropriate project tasks and activities, the type and frequency of project communications to stakeholders, managing project risks, and any changes to the project scope.

3.4 Minimal Configuration

3.4.1 The Contractor must support minimal configuration changes to the SaaS Solution such as field labels when feasible.

4. Pre-Implementation Services

4.1 Confirmation that the SaaS Solution meets the requirements

4.1.1 The Contractor must demonstrate that the SaaS Solution meets established requirements before its implementation (deployment).

4.2 Intellectual Propriety

4.2.1 It is understood that any refinements and design changes to the contractor's SaaS Solution will become an integral part of that SaaS Solution and will remain the intellectual property of the contractor. ESDC will have access to these changes under the terms of the contract for life of the contract.

4.2.2 As part of these Services, the Contractor must provide the services associated with requirements refinement identified in the following table:

No.	Roles and Responsibilities	Contractor	ESDC
1.	Provide subject matter guidance, decision making support and be an available point of contact to ESDC	X	X
2.	Leverage Contractor's Service Level Agreements to apply to stakeholder groups as required for any setup, configuration or provisioning of subscriptions		X
3.	Review and approve refinements and prioritization of requirements		X
4.	Identify and recommend what minimal configuration changes (e.g. labels) are possible to better meet requirements	X	
5.	Review and approve the minimal configuration changes (e.g. labels)		X

4.3 Basic Configuration Services

4.3.1 The Contractor must provide basic configuration services to support minimal configuration changes to the SaaS Solution such as labels.

a) Providing expertise in confirming that the Organization Chart SaaS Solution is compliant with the selected Core Technology's functional, non-functional, and technical requirements, including with commercially published design recommendations.

4.3.2 The Contractor must provide base-line data on Data Architecture including:

a) How the system data is designed to be backed-up;

b) How much data will the system be able to hold; and,

c) The period over which system data can be stored based on ESDC HRSB Retention and Disposition rules.

4.3.3 Any upgrades or improvements that outlines how system modules and/or components will be added.

4.3.4 The Contractor must provide the following in the event a rebuild is required post implementation or critical technical issues arise:

a) Assistance with the re-configuration and re-integration of the Organization Chart SaaS Solution with the existing ESDC Peoplesoft HCM 9.2 production instance; and,

b) Security Incident management procedures.

4.3.5 As part of these Services, the Contractor must provide the services associated with design, configuration and development identified in the following table:

No.	Roles and Responsibilities	Contractor	ESDC
1.	Recommend solutions, identify any gaps and provide mitigations or process changes.	X	
2.	Approve recommended solutions for all identified gaps.		X
3.	Review and adhere to ESDC's technical standards and conventions.	X	

5. Testing and Implementation Services

5.1 Test and Optimization

5.1.1 ESDC reserves the right to carry out independent Quality Assurance by itself or by a third party;

5.1.2 The Contractor must provide Test and Optimization services that is not necessarily limited to the following activities:

a) Develop and provide to the Project Authority a Testing and Integration Plan for testing the SaaS Solution .This document will include, but not be limited to, test plans, test phases, test environments, automation opportunities, test tools, test data, roles and responsibilities, and other components that align with ESDC's testing tools, including but not limited to: Microsoft Test Manager, a Test Automation Framework based on IBM Rational Functional Tester and Selenium, MicroFocus Loadrunner or Performance Centre, Parasoft Load with SOATest, and Apache Jmeter;

b) Execute a series of tests using historical or mock data to validate the SaaS Solution and its implementation through testing of:

i) Adherence to business requirements and successful completion of use cases for compliance to the defined SaaS Solution business rules and policies as independent units;

ii) Performance;

iii) System integration;

iv) User Acceptance;

c) Utilize the following, but not limited to, testing techniques:

i) Regression testing

ii) Acceptance testing

iii) Functional testing

iv) Non-functional testing

v) Software performance testing

vi) Accessibility testing

vii) Security and Vulnerability testing

d) Remediate defects found in the SaaS Solution or technical environment;

e) Provide a test coordinator to coordinate testing efforts with all activities required and parties involved;

f) Provide expertise on the acceptance of the software, business processes, and technology;

g) Validate the SaaS Solution implementation checklist and completeness of the required ESDC requirements, and ensure the system is ready for implementation;

h) Optimize and address any required modifications in terms of the overall SaaS Solution; Business processes, databases, and network components are further tested and fine-tuned for performance; new critical software and architectural components are improved for reliability, adaptability, and for other technical considerations where possible;

i) User Acceptance Testing is designed and performed by ESDC Subject Matter Experts, business analysts, and other users deemed necessary by ESDC for testing the core process life cycle in a non-production environment; and

j) Final ESDC acceptance for implementation of the SaaS Solution into the production environment is obtained.

5.1.3 As part of these Services, the Contractor must provide the services associated with requirements definition identified in the following table.

No.	Roles and Responsibilities	Contractor	ESDC
1.	Facilitate and support User Acceptance testing (establish adequate test environment based on User Acceptance Criteria, prepare data to support test scenarios within modified system as well as manage the relationship with all interfaced systems necessary to conduct test, troubleshoot, support Users to progress through scenarios, simulate interfaces or work with integrated systems to conduct end-to-end tests, exercise functionality, and report results) as prescribed by ESDC.	X	
2.	Conduct User Acceptance testing as required.	X	X
3.	Review testing results for compliance with policies, procedures, plans, and test criteria and metrics (e.g., defect rates, progress against schedule, etc.).		X
4.	Correct Defects found as a result of testing efforts throughout the implementation as defined in the testing approach defined by the Contractor.	X	
5.	Conduct User Acceptance re-testing of corrected Defects found throughout the implementation.	X	X
6.	Provide testing approach appropriate for ESDC approval and execute Security/Vulnerability Test Plan as applicable.	X	

5.2 Integration Testing

5.2.1 The Contractor must conduct the following Integration Testing activities:

a) Provide proposed integration test strategy and plan to verify functional, performance, and system reliability requirements for the ESDC systems; and,

b) Recommend integration testing requirements.

5.3 User Acceptance Testing (UAT)

5.3.1 Prior to releasing functional components into production, the Contractor must submit each release for UAT by ESDC. Prior to submitting the release for testing, the Contractor must have completed all of the required system testing with respect to the release. The Contractor must:

a) Facilitate and document User Acceptance Testing results per each requirement;

b) Implement corrective action based on the UAT results; and,

c) Assess and communicate the overall impact and potential risk to system components prior to implementing Changes.

5.3.2 Upon receiving each release, ESDC will perform UAT in accordance with the applicable Acceptance Criteria and will inform the Contractor of the outcome of such testing. ESDC reserves the right to determine the final Acceptance Criteria for each release.

5.3.3 ESDC reserves the right to reject releases that do not meet the Acceptance Criteria. At the end of the testing, ESDC will, in writing, either: (1) accept the Deliverable; (2) reject the Deliverable, identifying reasons for rejection; or (3) continue the acceptance period in accordance with a mutually agreed time for continued review.

5.3.4 In the event that ESDC rejects a release, the Contractor must promptly resolve any outstanding issues that are required in order for the release to meet all applicable Acceptance Criteria. ESDC will cooperate in the Contractor's efforts to resolve any problems, including indicating the reasons for rejection, and will not withhold acceptance unreasonably.

5.3.5 When submitting a previously rejected Deliverable to the Project Authority, the Contractor must produce written evidence of how the Deliverable was modified from its previously submitted state, and how this modification will address the concern documented by ESDC in the rejection document. Emphasis is to be on establishing conformance with the previously unmet requirements noted in the Deliverable rejection document. This is to both provide assurance that ESDC's needs have been met, and to accelerate the Acceptance Period by enabling ESDC to focus on reviewing the modifications made by the Contractor.

5.4 Implementation of the SaaS Solution

5.4.1 The Contractor must perform implementation activities as required to implement all the components of the SaaS Solution. The implementation comprises of all the activities commencing after the completion of all testing activities, up to and including successful Go-live.

5.4.2 The Contractor must execute the **Implementation Plan**.

5.4.3 As part of these activities, the Contractor must provide the services associated with the roles and responsibilities identified in the following table:

No.	Roles and Responsibilities	Contractor	ESDC
1.	Assist with data extract/transform/load activities to the SaaS Solution, as required by ESDC for successful implementation.	X	
2.	Support Go-live activities with ESDC and other user(s) that may be affected by the implementation of the SaaS Solution.	X	
3.	Provide post implementation validation approval.		X
4.	Create detailed "technical Go-live" plan as per Implementation plan.		X
5.	Create final decision "go/no-go" checklist and conduct the "go/no-go" meetings to determine decision to go live based on test results.		X

6.	Approve production implementation “go/no-go” decisions.		X
7.	Stage systems before implementation as per Implementation plan.	X	
8.	Deploy system as per Implementation process.	X	
9.	Perform contingency planning to provide service directives when an implementation does not proceed.		X
10.	Implement contingency plans when an implementation does not proceed.	X	X
Go-live			
11.	Go-live criteria and delivery requirements.		X
12.	Comply with Go-live criteria and delivery requirements.	X	
13.	Provide training to ESDC SaaS Solution and Administrative (IT Operations) users as agreed through tutorial sessions (online or in-person), training manuals, instructional videos, etc.	X	
14.	Approve production implementation “Go/No-go” decisions.		X

6. Acceptance of Deliverables

6.1 Overview

6.1.1 ESDC will:

a) Review and determine the acceptance of the SaaS Solution (or its components thereof) against the Acceptance Criteria for the Functional and Non-functional, Security, Accessibility and other requirements as described in the appropriate test plans, including User Acceptance Testing. These activities are described in Section 5.1– Test and Optimization. All documentation that is included in or as a result of the testing above must be reviewed as per Acceptance of Document Deliverables Framework below;

b) Review and determine the acceptance of the documentation as per Acceptance of Document Deliverables Framework identified in Sections 6.2.

6.2 Acceptance of Document Deliverables Framework

6.2.1 Unless otherwise stipulated differently, document Deliverables will be reviewed and accepted or rejected as described below.

a) After the submission of any deliverables, ESDC will utilize a review period of up to **10 business days** to review the deliverable against the Acceptance Criteria.

b) If the Deliverable does not meet Acceptance Criteria, ESDC reserves the right to reject such Deliverable. At completion of the review or at the end of the review period (whichever comes first), the Project Authority will provide in writing, either: (1) acceptance of the Deliverable; (2) rejection of the Deliverable, identifying reasons for rejection; or (3) mutually agree with the Contractor to extend the review period in order to complete the review of the Deliverable.

c) In the event that ESDC rejects a Deliverable, the Contractor must promptly resolve any outstanding issues that are required in order for the Deliverable to meet all applicable Acceptance Criteria. The Contractor and ESDC may agree to a joint review of the feedback prior to any action by the Contractor. The Contractor must submit the revised Deliverable to the Project Authority within **10 business days** of the receipt of ESDC’s feedback, or the joint review of the feedback, whichever is later. The Contractor and ESDC may mutually agree to different timelines or an alternate process for given Deliverable(s) than as prescribed above. ESDC will cooperate in the Contractor’s efforts to resolve any problems, and will not withhold acceptance unreasonably.

d) A Deliverable will be deemed to be accepted by ESDC only upon written notice of acceptance.

e) ESDC, with the assistance of the Contractor if required, may develop specific User Acceptance Criteria the SaaS Solution. In addition to the specific SaaS Solution User Acceptance Criteria, all documentation Deliverables, including those arising as a result of TAs, will comply with and will be evaluated for the following attributes:

No.	Criterion	Description
1.	Document Format and Clarity	1. Consistent format is used; 2. Correct and continuous section numbering is used; 3. Material is presented logically; 4. Non-standard terms, phrases, acronyms, and abbreviations are defined; 5. Proper titles and labels on figures are used; 6. No ambiguous statements or content are used; 7. Use of passive voice is minimal and appropriate; 8. No typographical errors, spelling errors, missing words, or incorrect page and section numbers; 9. Generally accepted rules of grammar, capitalization, punctuation, symbols, and notation are used; 10. Cross-references are identified appropriately and accurately; and, 11. Documents are provided in an editable format (if requested by ESDC).
2.	Alignment and Consistency	12. Terms have the same meaning throughout the document; 13. The material does not contradict predecessor document (*i.e.* if the Deliverable contains requirements, they align with ESDC business needs as defined in Part 4, under the clause 4.1 Evaluation Procedures); and, 14. All material in subsequent documents has a basis in the predecessor document, for example: a) If the Deliverable contains designs, the design addresses the defined requirements or specifications.
3.	Completeness	15. If the Deliverable contains a plan or a process, it is clear who is responsible for which task, when the plan or process is planned to be completed, and how the plan or process will be evaluated and determined to be successful. This will be developed by the Contractor and approved by ESDC; 16. If the Deliverable contains business or technical designs or specifications, all elements of the design are complete and clear so that readers understand the related functionality that will be developed; 17. If the Deliverable contains requirements, specifications, or success criteria, they include specific metrics against which achievement can be measured. They are clear enough to be used in the development of future Deliverables (for example, the requirements are written clearly enough to aid in the writing of use cases and success criteria). This will be defined by the Contractor and approved by ESDC; and, 18. If the Deliverable contains findings and recommendations, the Deliverable clearly states how these were developed.

6.3 Acceptance of Document Deliverables Framework

6.3.1 When re-submitting a previously rejected Deliverable to ESDC, the Contractor must produce a written document that provides a high-level description of how the Deliverable was modified from its previously submitted state, and how this modification will address the concern documented by ESDC in the rejection document. Emphasis is to be on establishing conformance with the previously unmet requirements noted in

the deliverable rejection document. The Contractor must identify any changes or issues that were not addressed, and provide rationale as to why these changes were not included.

6.4 Deliverable Submission Process

6.4.1 In order to avoid acceptance delays, inconsistencies and contradictions in related Deliverables, the Contractor should take measures to avoid submitting Deliverables at the same time, unless stipulated in the Contract (or Task Authorization). If the Contractor submits multiple Deliverables at the same time, outside the stipulated Deliverable dates in the Contract (or Task Authorization), ESDC reserves the right for additional review time and will adjust the review process accordingly.

7. Master Project Schedule Summary

7.1 Overview

7.1.1 The Deliverables, (i.e. documentation or the SaaS Solution - or its various components thereof), must be delivered in accordance with the timelines specified in each milestone in the Master Project Schedule Summary in the tables below. The milestone target dates represent the estimated timelines the Contractor is expected to meet. ESDC recognizes that these timelines may change following the consultation and planning phases with the Contractor after Contract Award. As well, the dates may be subject to change in response to any unforeseen difficulties and potential delays. As such, at the sole discretion of ESDC and in consultation with the Contractor, the timelines may be adjusted following the Contract Award. The same milestones apply to the on boarding of any subsequent ESDC's legacy applications.

7.1.2 The Master Project Schedule Summary provides the basis for the implementation plan that the Contractor will be required to produce.

7.1.3 For Phase 1, the Master Project Schedule Summary assumes that the Project Start-up will commence with an official Project Kick-off meeting that will happen no later than one (1) week after contract signing with the Contractor.

Table 1: Master Project Schedule Summary – Phase 1 – Unclassified Data

Milestone No.	Description or "Deliverable"	Firm Amount	Due Date or "Delivery Date"
1	**Kick-off** ***(Project Start-up)*** Project Authority, with the support of the Contractor will Kick-off the start of the project, and then ESDC and the Contractor will proceed with planning and design activities, as described in **Section 3 of the Statement of Work - Project Management and Governance Services**.	N/A	One (1) week after Contract/TA signing **Mid-September**
2	**Project Planning** ***(Project Management Planning complete)*** ESDC and the Contractor has delivered the project management planning Deliverables as described **in Section 3 of the Statement of Work - Project Management and**	$(TBD)	(TBD) **Mid-October**

	Governance Services, and these have been accepted by ESDC.		
3	**Architecture and Design** ESDC and the Contractor has delivered the Architecture and Design planning Deliverables as describe in **Section 4.3 of the Statement of Work – Design and Configuration Services**	$(TBD)	(TBD) ***Must be before December 16, 2022**
4	**Core SaaS Solution Configuration and Integration Testing** Contractor has implemented and tested the SaaS Solution as described in **Section 5 of the Statement of Work – Testing and Implementation Services (Go-Live);** AND All Deliverables must be accepted by ESDC.	$(TBD)	(TBD) ***Must be before January 16, 2023**
5	**Operations** Contractor will commence performing operations, and related service activities, as described in **Section 8.2 of the Statement of Work - Operations**; Contractor has delivered, for the work required for this milestone, all the relevant elements of the plans described in **Section 3 of the Statement of Work - Project Management and Governance Services;** AND All Deliverables must be accepted by ESDC.	$(TBD) *Includes the Annual Subscription Fee during the 60-days stabilization step	One (1) day after the Milestone #4 *(Ongoing - Starts for each ESDC on-boarded application the day following its Go-live date)*

7.1.4 For Phase 2, the Master Project Schedule Summary assumes that the Project Start-up will commence with an official Project Kick-off meeting that will happen no later than one (1) week after the signature of the related task authorization, conditional to the contractor obtaining all necessary security clearance, once ESDC has decided to move forward with Phase 2.

Table 2: Master Project Schedule Summary – Phase 2 – Protected B Data

Milestone No.	Description or "Deliverable"	Firm Amount	Due Date or "Delivery Date"
1	**Kick-off** ***(Project Start-up)*** Project Authority, with the support of the Contractor will Kick-off the start of the project, and then ESDC and the Contractor will proceed with planning and design activities, as described in **Section 3 of the Statement of Work - Project Management and Governance Services**.	N/A	**One (1) week after IT Security clearance obtained by Contractor/TA signing**
2	**Project Planning** ***(Project Management Planning complete)*** ESDC and the Contractor has delivered the project management planning Deliverables as described **in Section 3 of the Statement of Work - Project Management and Governance Services**, and these have been accepted by ESDC.	$(TBD)	(TBD)
3	**Architecture and Design** ESDC and the Contractor has delivered the Architecture and Design planning Deliverables as describe in **Section 4.3 of the Statement of Work – Design and Configuration Services**	$(TBD)	(TBD)
4	**Core SaaS Solution Configuration and Integration Testing** Contractor has implemented and tested the SaaS Solution as described in **Section 5 of the Statement of Work – Testing and Implementation Services (Go-Live);** AND All Deliverables must be accepted by ESDC.	$(TBD)	(TBD)
5	**Operations** Contractor will commence performing operations, and related service activities, as described in **Section 8.2 of the Statement of Work - Operations**;	$(TBD) *Includes the Annual Subscription Fee during the 60-days stabilization step	One (1) day after the Milestone #4 *(Ongoing - Starts for each ESDC on-boarded application the day following its Go-live date)*

	Contractor has delivered, for the work required for this milestone, all the relevant elements of the plans described in **Section 3 of the Statement of Work - Project Management and Governance Services;** AND All Deliverables must be accepted by ESDC.		

8. Post Go-Live Activities

8.1 Post Go-Live Stabilization

8.1.1 Post Go-Live Stabilization describes the ongoing activities to support the SaaS Solution, in order to achieve operational stability of the SaaS Solution. These activities, described in sections 8.1.2 to 8.1.5 below, will apply for each release of the ESDC key benefits programs on boarded, and the activities will be governed by ESDC's acceptance processes and criteria. These activities will happen during the Error Free Stabilization period as described below prior to final acceptance of each release.

8.1.2 Final acceptance of all releases will be subject to a 60-calendar day Error Free Stabilization period from the Go-live date. Error free is defined as in operation without Severity 1 or Severity 2 Incidents (Major Incidents) as defined by ESDC. After the expiration of the 60-day Error Free Stabilization period, if the release conforms to the Acceptance Criteria, ESDC will accept the release. In the event that any release does not operate Error Free for 60 consecutive calendar days, ESDC will reject the release and provide the Contractor with a written notice requiring a resolution. In response, the Contractor must remediate the deficiency, at no additional cost to ESDC, and resubmit the release for acceptance. Additionally, the 60-calendar day Error Free Stabilization clock will reset to zero with each Major Incident, unless ESDC, at its sole discretion, waives this condition.

8.1.3 If the resubmitted release does not conform to the Acceptance Criteria, ESDC will require the Contractor, at no added cost to ESDC, to remediate the non-conformity and, until such time as there is a continuous 60-calendar day Error Free Stabilization period. ESDC, at its sole discretion, may choose to terminate the Contract for Default if there is no progress being made.

8.1.4 During the Stabilization period, the Contractor must provide support and maintenance services for each release of the SaaS Solution. The support and maintenance activities may include:

a) Resolution of post-Go-live configuration related issues;

b) Providing root Cause analysis and documentation of all issues identified, and resolutions provided post Go-live; and,

c) Providing fixes for any SaaS Solution product bugs identified post Go-live.

8.1.5 The Contractor must also:

a) Conduct Post go-live stabilization report within 5 business days following each stabilization;

b) Collect, analyze and report stakeholder feedback issues, comments and or requests;

c) Provide a post-Stabilization Lessons Learned Report for Project Authority approval no later than 30 business days after the end of each Stabilization period based on all lessons learned from the execution of the Implementation Plan; and,

d) Incorporate lessons learned into subsequent overall project activities for the on boarding of the remaining ESDC applications.

8.2 Operations

8.2.1 From the Go-live date of the first release, the Contractor must provide operations, and on-going support and maintenance services for the effective day-to-day management of the Organization Chart SaaS Solution for the duration of the contract. The Contractor must provide and deliver to the Project Authority an On-going Support and Maintenance Plan for the SaaS Solution which must include but not be limited to:

a) Providing status reports (weekly and monthly) detailing progress and updates to the ongoing support. The contents of the reports must include but not be limited to appropriate metrics for monitoring support and maintenance activities, including the number and types of incidents, and their resolution status and timelines, system access requirements for Contractor Support SMEs, and the Software platform update/downtime.

b) Providing modifications and updates to the SaaS Solution or its components thereof.

c) The Contractor must provide support for testing activities to ESDC when there are modifications or updates to the Organization Chart SaaS Solution, including:

i) Maintain SaaS Solution release configurations across development, quality assurance, and production environments and networks;

ii) Conduct integration and security testing for all data and networks based on requirements defined in the plan and ESDC policies and procedures;

iii) Evaluate all new and upgraded system components and services for compliance with ESDC security rules, regulations and procedures;

iv) Provide proposed integration and test plan;

v) Conduct User Acceptance Testing for all modifications and updates; and

vi) Assess and communicate the overall impact and potential risk to system components prior to implementing changes.

8.2.2 During the On-going Support and Maintenance period, the Contractor must:

a) Analyze and establish an action plan to remediate any issues identified by ESDC as high priority (Severity 1 or 2) within 5 calendar days. Resolution timelines of identified issues will be established as part of the plan, and resolution will occur within 10 calendar days of the identification of the issue identification.

b) Analyze and establish an action plan for any stabilization/post-transition issues identified by ESDC as non-high priority (Severity 3 and below) within 15 calendar days. Resolution timelines of identified issues will be established as part of the plan, and resolution will occur within 25 calendar days of issue identification.

8.2.3 Proving guidance to ESDC on the number of resources required for each of the categories of resources needed to operate, support and maintain the SaaS Solution.

8.2.4 Provide at ESDC's request, a roadmap of product growth and support for a duration between 5-7 years.

8.2.5 As part of these Services, the Contractor must provide the services associated with the roles and responsibilities identified in the following table:

No.	Roles and Responsibilities	Contractor	ESDC
1.	Monitor and report on application adoption, performance, incidents and problems;	X	
2.	Remediate any incidents and problems to restore application performance at desired levels;	X	
3.	Identify any bugs that may lead to ongoing incidents or performance degradation;	X	
4.	Remediate any bugs in accordance with ESDC needs;	X	
5.	Update system and provide support documentation at the end of the warranty period based on any changes made after Go-live;	X	
6.	Notify ESDC of user training material fixes related to post Go-Live stabilization efforts including dashboards, statistics and/or audit logs.	X	

9. Training

9.1 Training Plan

9.1.1 The Contractor must provide to the Project Authority a Training Plan within the detailed Project Plan for review and approval by the Project Authority.

9.1.2 As a minimum, the Training Plan must describe how the Contractor will:

a) Develop the training approach;

b) Support identification of key stakeholders (in conjunction with change management team) and creation of training materials for User Acceptance testing in conjunction with technical team;

c) Participate in ESDC-delivered instruction on the business and technical environment;

d) Provide ongoing training materials for service desk resources on ESDC business and technical environments as defined by ESDC;

e) Provide training requirements assessment by User type. This must address the initial training requirement for the Organization Chart SaaS Solution to “go live” and the ongoing training requirement for new Users or refresher training;

f) Provide training requirements for administration access;

g) Provide training module content that is copyright and royalty free for modification and redistribution by ESDC.

9.2 Training Delivery

9.2.1 The Contractor must perform the training as described in the Training Plan. The training material must be provided in Canada’s two official languages of English and French. Training must be held in English and may be held in French upon request. All required training will be authorized by TAs.

9.2.2 Training must include, but not be limited to the following activities, which includes thorough technical and User training, effective communication and successful stakeholder participation:

a) Provide and update training material as needed or concurrent with a major release to address new features and release changes. Training materials must comply with the approved Training Plan;

b) Conduct Authorized Administrator training, including training for ESDC technical resources for the express purpose of exploiting the functions and features of ESDC computing environment. Delivery

methods may include classroom-style, computer-based, individual or other appropriate means of instruction;

c) Conduct training of ESDC and appropriate third party technical resources to ESDC for the express purpose of ensuring seamless transfer of operations, maintenance and support of the Organization Chart SaaS Solution. Delivery methods may include classroom-style, computer-based, individual or other appropriate means of instruction;

d) Conduct User training as requested by ESDC, including selected online or classroom-style and computer-based training (case-by-case basis) for the Organization Chart SaaS Solution, including new employee training, upgrade classes and specific skills;

e) Conduct Train the Trainer training for Users as defined by ESDC;

f) Provide role-specific training to Project resources prior to each new product version release in order to facilitate full exploitation of all relevant functional features; and,

g) If requested by ESDC, inform and train Users about the end-to-end SaaS Solution that will support their business requirements.

h) Provide the training material in both official languages, if applicable.

9.3 Participant Information for In-Class and/or Online Training

9.3.1 To assist the Contractor in developing their training plan schedule, ESDC has provided the following details:

9.3.2 Training sessions (in-person or online) will be provided to the following group sizes:

- Group 1 – Investigators, Business Analysts and Data Scientists
  Class size: A minimum of 10 to a maximum of 30 participants
- Group 2 – IT Administrators and Security staff
  Class size: A minimum of 5 to a maximum of 15 participants

The number of training sessions will be determined based on the number of actual participants.

9.3.3 Training participants may include, but are not limited to, technical, system/application, delivery, systems and support personnel, as well as software administrators, data scientists, business analysts, and advanced Users (Investigators).

10. Mandatory, Functional and Non-Functional Requirements

Please refer to Part 4, under the clause 4.1 Evaluation Procedures.

10.1 ESDC Security & Accessibility Requirements

10.1.1 The Contractor must apply the security measures stipulated in Appendix A - Security Obligations for Tier 2 (up to Protected B) during the phase two of the implementation of the SaaS Solution.

10.1.2 The Contractor must meet the Accessibility Requirements stipulated in TBS Standard on Web Accessibility in the implementation of the SaaS Solution.

10.1.3 The Contractor must demonstrate that the solution conforms to accessibility guidelines as defined under the ETSI EN 301 549 - V3.2.1 - Accessibility requirements for ICT products and services specifically clauses 9.1 – 9.4 – Web (includes WCAG 2.1 Level AA), 10.0 General – Non Web documents (ie. PDF) and 12.1 – Product documentation (training).

10.1.4 ***By submitting a bid to this request for proposals (RFP) #100021358, the vendor commits to conform with the accessibility requirements in a timely manner, if they do not already comply fully with the criterion R10. If required by the project authority, the vendor must provide an accessibility roadmap before the end of the period of the resulting contract.***

10.2 Solution Technical Architecture and Standards

10.2.1 The proposed SaaS Solution (or any of its components thereof) must meet the design requirement of the ESDC Cloud Centre of Excellence. This includes determining and adopting principles and standards for desired future architectures and environments related to both Government of Canada and industry trends in products and technologies. For a cloud-based Software as a Service Solution (or its components thereof), the Contractor must work with ESDC and Government of Canada to establish the necessary development, test, training, pre-production, load and performance test, staging, production and support environments as necessary to support the SaaS Solution. The SaaS Solution (or its components thereof) must be implemented as Software-as-a-Service (SaaS) in the protected-B Azure Cloud (ESDC/GoC Azure subscriptions), or other approved cloud services that have been pre-certified by CCCS (Canadian Centre for Cyber Security).

10.2.2 The SaaS Solution might be further assessed against any applicable GC Enterprise Architecture standards and frameworks such as GC Enterprise Hybrid Cloud High-Level Design, GC Zero Trust Security Reference Architecture and GC Cloud Tiered Assurance Model. Any cloud-based vendor should follow and meet the GC Secure Cloud Connectivity Requirements so that GC can maintain its visibility of the information stored, processed, and transmitted when using cloud-based services. The vendor should also fully support and assist ESDC in meeting GC cloud guardrail requirements which are the enterprise-wide mandatory baseline controls for cloud: including but not limited to the Direction on the Secure Use of Commercial Cloud Services: SPIN 2017-02 and the GC Security Control Profile for Cloud-based GC Solutions for Protected B, Medium Integrity, Medium Availability (PBMM).

10.3 Additional Training

10.3.1 When requested, the Contractor must develop and provide additional training to ESDC users through online or in-person training sessions, including training manuals and instructional videos. This additional training is above and beyond the training required as part of the Firm Requirements identified in Section 9, Training. This additional training may include designing and delivering training packages on topics that are different from the training delivered as part of the Firm Training Requirements training.

APPENDIX A to Annex B: Security Obligations for Tier 2 (up to Protected B)

1. General

1.1 *Purpose*

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

1.2 *Flow-Down of Security Obligations*

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

1.3 *Change Management*

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

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

2. Acknowledgments

The parties acknowledge that:

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

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

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

d) Security Obligations apply to Tier 2 (up to Protected B / Medium Integrity, Medium Availability or Medium Injury), unless otherwise specified.

3. Securing Canada's Data

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

4. Roles and Responsibilities for Security

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

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

5. Third-Party Assurance: Certifications and Reports

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

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

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

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

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

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

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

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

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

6. Auditing Compliance

(1) The Contractor 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 Canada's Data as follows:

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

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

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

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

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

7. Cloud Service Provider (CSP) IT Security Assessment Program

(1) The Contractor must demonstrate compliance 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) (https://www.canada.ca/en/government/system/digital-government/modernemergingtechnologies/cloud-computing/government-canada-security-control-profilecloud-based-itservices.html) for the scope of the Cloud Services provided by the Contractor. Compliance must be demonstrated through the mapping of security controls to the applicable industry certifications identified below, and validated through independent third party assessments.

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

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

i) A copy of the confirmation letter that confirms that they have on-boarded into the program;

ii) A copy of the most recent completed assessment report provided by CCCS; and

iii) A copy of the most recent summary report provided by CCCS.

The Contractor should contact the CCCS Client Services for any additional information related to the CSP IT Assessment Program.

It is the continuous obligation of the Contractor of the proposed Cloud Services to notify CCCS when there are significant changes to its delivery of the IT Security services supporting the Contractor offering.

8. Data Protection

(1) The Contractor must provide the capability to allow Canada to:

a) Implement encryption of data at rest for the Cloud Services hosting Canada's Data where the encryption of data at rest remains in effect, uninterrupted, and active at all times, even in the case of equipment or technology failure, in accordance with Section 13 - Cryptographic Protection.

b) Transmit Canada's Data in a secure manner including ability for the GC to implement encryption for data in transit for all transmissions of Canada's Data, in accordance with Section 13 - Cryptographic Protection and Section 21- Network and Communications Security.

(2) The Contractor must:

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

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

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

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

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

9. Data Isolation

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

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

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

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

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

10. Data Location

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

a) A data centre that meets all security requirements and certifications identified in Section 30 for Physical (Data Centre / Facilities) Security

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

c) Employs encryption to ensure that no data is written to disk in an unencrypted form, in accordance with Section 13 - Cryptographic Protection.

(2) The Contractor must certify that the delivery and provisioning of Cloud Services under this contract is from countries within the North Atlantic Treaty Organization (NATO) (https://www.nato.int/cps/en/natohq/nato_countries.htm) or the European Union (EU) (https://europa.eu/europeanunion/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: https://www.tpsgc-pwgsc.gc.ca/esc-src/international-eng.html and as updated from time to time.

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

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

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

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

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

11. Data Transfer and Retrieval

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

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

b) Securely transfer all Canada's Data, including content data and associated metadata, in a machine-readable and usable format, including CSV format, and in accordance with the Library and Archives Canada Guidelines on File Formats for Transferring Information Resources of Enduring Value (https://www.baclac.gc.ca/eng/services/governmentinformation-resources/guidelines/Pages/guidelines-fileformats-transferring-informationresources-enduring-value.aspx).

12. Data Disposition and Returning Records to Canada

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

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

13. Cryptographic Protection

The Contractor must:

a) Configure any cryptography used to implement confidentiality or integrity safeguards, or used as part of an authentication mechanism (e.g., VPN solutions, TLS, software modules, PKI, and authentication tokens where applicable), in accordance with Communications Security Establishment (CSE)-approved cryptographic algorithms and cryptographic 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-unclassifiedprotectedand-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://cyber.gc.ca/en/tools-services/cryptographic-module-validation-program-cmvp), 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 Contractor must provide Canada with a key management service that provides:

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

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

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

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

e) Ability to securely import GC generated keys from GC-managed on-premise hardware security module (HSM) without exposure of key plaintext during the import process;

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

g) Ability to delegate key use privileges for use by the Cloud Services used for the GCmanaged services.

15. Endpoint Protection

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

16. Secure Development

The Contractor must implement a software and system development lifecycle that applies information system security engineering principles throughout the information system life cycle and in the development of software and websites and services, and conforms to industry standards and best practices, such as (i) NIST, (ii) ISO 27034, (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. Upon request of Canada, the Contractor must provide a document that describes the Contractor's documented software and system development lifecycle approach and process.

17. Identity and Access Management

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

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

b) Role-based access;

c) Access controls on objects in storage; and

d) Granular authorization policies to allow or limit access.

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

18. Federation

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

a) Support for open standards for authentication protocols such as Security Assertion Markup Language (SAML) 2.0 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. Privileged Access Management

(1) The Contractor must:

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 Cloud Services and Canada's Data to only authorized devices and End Users with an explicit need to have access;

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

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

e) Implement password policies to protect credentials from compromise by either online or off-line attacks and to detect these attacks by logging and monitoring events such as (i) successful use of credentials,

(ii) unusual use of credential, and (iii) access to and exfiltration from the password database, in accordance with CSE's ITSP.30.031 V3 (or subsequent versions) (https://cyber.gc.ca/en/guidance/user-authentication-guidance-informationtechnology-systems-itsp30031-v3);

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

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

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 Cloud Services and Canada's Data;

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 Cloud Services and Contractor 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.

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

20. Remote Management

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

a) Implement multi-factor authentication mechanisms for authenticate remote access users, in accordance with CSE's ITSP.30.031 V3 (or subsequent versions) (User authentication guidance for information technology systems (ITSP.30.031 v3) - Canadian Centre for Cyber Security);

b) Employ cryptographic mechanisms to protect the confidentiality of remote access sessions, in accordance with Section 13 (Cryptographic Protection);

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

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

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

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

21. Network and Communications Security

The Contractor must:

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

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

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

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

22. Dedicated Connections

For IaaS, the Contractor must provide the ability for the GC to establish private redundant connectivity to the Cloud 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, or in a GC-approved location within the geographic boundaries of Canada;

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 10 Gbps with the option to add additional links that provide up to 40 Gbps in aggregate, with optional 100 Gbps 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.

23. Logging and Auditing

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

(2) The Contractor must provide the ability for Canada to export security event logs for the Cloud Services it consumes, in support of GC operations including monitoring of the Cloud Services and for e-discovery and legal holds.

(3) The Contractor must enable Canada to centrally review and analyze audit records from multiple components from the Cloud Services consumed by the customer. This includes the ability for Canada to:

a) log and detect audit events such as (i) successful and unsuccessful account login attempts, (ii) account management, (iii) object access and policy change, (iv) privilege functions and process tracking, (v) system events, (vi) deletion of data;

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

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

d) 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.).

(4) For SaaS, the Contractor must provide APIs that provide the ability to:

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

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

24. Continuous Monitoring

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

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

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

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

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

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

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

g) Where required, take proactive countermeasures, including taking both preemptive and responsive actions, to mitigate threats.

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

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

25. Security Incident Management

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

a) A published and documented Security Incident Response Process for review by Canada that is aligned with one of the following standards:

i) ISO/IEC 27035:2011 Information technology - Security techniques -- Information security incident management; or

ii) NIST SP800-612, Computer Security Incident Handling Guide; or

iii) GC Cyber Security Event Management Plan (GC CSEMP) (https://www.canada.ca/en/government/system/digital-government/online-security-privacy/security-identity-management/government-canada-cyber-security-event-management-plan.html); or

iv) other best practices from industry standards, if Canada determines, in its discretion, that they meet Canada's security requirements.

b) Documented processes and procedures of how the Contractor will identify, respond, remediate, report, and escalate Security Incidents to Canada, including:

i) the scope of the information security incidents that the Contractor will report to Canada;

ii) the level of disclosure of the detection of information security incidents and the associated responses;

iii) the target timeframe in which notification of information security incidents will occur;

iv) the procedure for the notification of information security incidents;

v) contact information for the handling of issues relating to information security incidents; and

vi) any remedies that apply if certain information security occur.

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

d) Allows only designated representatives of Customer (e.g. SSC Security Operations Center) authorized by the Technical Authority:

i) to request and receive discrete access and information associated with Customer's Data (user data, system/security event logs, network or host packet captures, logs from security components

such as IDS/IPS/Firewalls, etc.), in an unencrypted fashion, for the purposes of conducting investigations;

ii) the ability for Customer to track the status of a reported information security event.

e) Procedures to respond to requests for potential digital evidence or other information from within the Cloud Services environment and includes forensic procedures and safeguards for the maintenance of a chain of custody;

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

(3) The Contractor must:

a) Work with Canada's Security Operations Center(s) (e.g. CCCS, Departmental SOC) on Security Incident containment, eradication and recovery in accordance with the Security Incident Response process.

b) Maintain a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data or the service; and

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

(4) Canada may require forensic evidence from the Contractor to assist in a GC investigation. The Contractor agrees to provide assistance to the GC on a best effort basis.

26. Security Incident Response

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

(2) If the Contractor becomes aware of and determines a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data or Personal Data while processed by the Contractor (each a "Security Incident"), the Contractor must promptly and without undue delay (i) notify Canada of the Security Incident; (ii) investigate the Security Incident and provide Canada with detailed information about the Security Incident; and (iii) take reasonable steps to mitigate the cause and to minimize any damage resulting from the Security Incident.

27. Information Spillage

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

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

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

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

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

28. Security Testing and Validation

(1) The Contractor 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 Cloud Service components within the Contractor environment.

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

29. Personnel Security Screening

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

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

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

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

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

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

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

e) The approach to detecting 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 Canada's data.

30. Physical (Data Centre / Facilities) Security

(1) The Contractor must implement physical security measures that ensure the protection of IT facilities and information system assets on which Canada's Data are stored and processed against all forms of tampering, loss, damage, and seizure. Physical protection of all facilities that host Canada's Data, must be applied in accordance with, or use an adequate risk-based approach based on a prevent-detect-respond-recover approach to physical security, aligned with the physical security controls and the practices in the Treasury Board Operational Security Standard on Physical Security (http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12329). The security measures required under this include, at a minimum:

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

ii) Proper handling of IT Media;

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

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

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

vi) Escorting visitors and monitoring visitor activity;

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

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

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

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

31. Supply Chain Risk Management

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

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

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.

(3) Within 90 days of contract award, the Contractor must:

a) Provide proof that the SRCM approach and plan has been independently assessed and validated by an independent third party certified under AICPA or CPA Canada, and/or ISO certification regime

OR

b) Provide Canada with a copy of the SRCM Plan on an annual basis, or upon request of Canada.

(4) In the situation where the Contractor is a SaaS provider using a GC-approved IaaS Provider that already complies with the Section 31 - Supply Chain Risk Management requirements, within 90 days of contract award, the SaaS provider using a GC-approved IaaS provider must provide an information communication technology (ICT) product list that describes the ICT equipment that is being deployed in the GC-approved IaaS provider environment for a supply chain integrity (SCSI) review. This SCSI review will be conducted no sooner than every three years.

32. Industrial Security Program – Security Requirement for Canadian Suppliers

(1) The Contractor must, at all times during the performance of the Contract/Standing Offer/Supply Arrangement, hold a valid Designated Organization Screening (DOS) with approved Document Safeguarding at the level of PROTECTED B, issued by the Industrial Organization Security Services Directorate (OSS), **Public Services and Procurement Canada** (**PSPC**).

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

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

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

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

b) Industrial Security Manual (Latest Edition);

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

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

33. Industrial Security Program – Security Requirements for Foreign Suppliers

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

(1) The Contractor/Subcontractor certifies that the delivery and provisioning of Cloud Services under the terms of this contract must be from a country within the North Atlantic Treaty Organization (NATO), the European Union (EU) or from a country with which Canada has an international bilateral security instrument. The Contract Security Program (CSP) has international bilateral security instruments with the countries listed on the following PSPC website: http://www.tpsgc-pwgsc.gc.ca/esc-src/international-eng.html and as updated from time to time.

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

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

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

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

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

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

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

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

(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** 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** hold an equivalence to an approved Document Safeguarding Capability (DSC) at the level of **CANADA PROTECTED B**.

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

(8) Canada has the right to reject any request made separate and apart from the authorization in this Contract in connection with the Contractor delivering Cloud Services to electronically access, process, produce, transmit

or store CANADA PROTECTED data related to the Cloud Services in any other country if there is any reason to be concerned about the security, privacy, or integrity of the information.

ANNEX C

BASIS OF PAYMENT

Professional Services

The Contractor will be paid firm hourly rates as follows, for work performed in accordance with the Contract. Customs duties are included and Applicable Taxes are extra.

Period	Estimated Level of Effort	Resource Category	Firm Hourly Rate
Initial Period	''As and When Requested'' Basis	Subject Matter Expert	$ (TBD)
		Training Expert	$ (TBD)

Total Estimated Cost: $ (TBD)

Option to Extend the Contract
During the extended period of the Contract, the Contractor will be paid the following firm hourly rates to perform all the Work in relation to the contract extension.

Period	Resource Category	Firm Hourly Rate
Option Period - 1	Subject Matter Expert	$ (TBD)
	Training Expert	$ (TBD)
Option Period - 2	Subject Matter Expert	$ (TBD)
	Training Expert	$ (TBD)
Option Period – 3	Subject Matter Expert	$ (TBD)
	Training Expert	$ (TBD)
Option Period – 4	Subject Matter Expert	$ (TBD)
	Training Expert	$ (TBD)
Option Period – 5	Subject Matter Expert	$ (TBD)
	Training Expert	$ (TBD)
Option Period – 6	Subject Matter Expert	$ (TBD)
	Training Expert	$ (TBD)

**Training Expert, as per Part 10 of the Statement of Work.*

Training Services (As per Part 9 of the Statement of Work)

In consideration of the Contractor satisfactorily completing all of its obligations under the authorized Task Authorization (TA), the Contractor will be paid the firm unit price as detailed in the Basis of Payment below, as specified in the authorized TA. Customs duties are included and Applicable Taxes are extra.

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

Period	Group Type	Estimated Quantity	Firm Unit Price	Subtotal
Initial Period	Group 1 (From 10 to 30 participants)	7	$ (TBD)	$ (TBD)
	Group 2 (From 5 to 15 participants)	12	$ (TBD)	$ (TBD)
Option Period - 1	Group 1 (From 10 to 30 participants)	5	$ (TBD)	$ (TBD)
	Group 2 (From 5 to 15 participants)	5	$ (TBD)	$ (TBD)
Option Period - 2	Group 1 (From 10 to 30 participants)	1	$ (TBD)	$ (TBD)
	Group 2 (From 5 to 15 participants)	1	$ (TBD)	$ (TBD)
			Total – Training Services	**$ (TBD)**

Software as a Service Solution – Annual Subscription

In consideration of the Contractor satisfactorily completing all of its obligations under the contract, the Contractor will be paid the firm unit price in accordance with the basis of payment, in Annex C. Customs duties are included and Applicable Taxes are extra.

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

This basis of payment will begin the day following ESDC's acceptance of the release.** As per the Statement of work, after the expiration of the 60-days Error Free Stabilization period, if the release conforms to the Acceptance Criteria, ESDC will accept the release. **The amount to be paid will be calculated proportionally as per the amount of days left in the year and the firm annual unit price of the associated period for each user.

Period	**Firm Annual Unit Price** **Annual Subscription fees per user*				
	From 0 up to 150 users	More than 150 up to 1,000 users	More than 1,000 up to 6,500 users	More than 6,500 up to 10,500 users	Subtotal
Initial Period	C1.1 $ ____	C1.2 $ ____	C1.3 $ ____	C1.4 $ ____	**C1 $ _____**
Option Period – 1	C2.1 $ ____	C2.2 $ ____	C2.3 $ ____	C2.4 $ ____	**C2 $ _____**
Option Period – 2	C3.1 $ ____	C3.2 $ ____	C3.3 $ ____	C3.4 $ ____	**C3 $ _____**
Option Period – 3	C4.1 $ ____	C4.2 $ ___	C4.3 $ ____	C4.4 $ ____	**C4 $ _____**
Option Period – 4	C5.1 $ ____	C5.2 $ ____	C5.3 $ ____	C5.4 $ ____	**C5 $ _____**
Option Period – 5	C6.1 $ ____	C6.2 $ ___	C6.3 $ ____	C6.4 $ ____	**C6 $ _____**
Option Period – 6	C7.1 $ ____	C7.2 $ ____	C7.3 $ ____	C7.4 $ ____	**C7 $ _____**

**We are estimating the quantity of users to start at 80 users for the first month(s), but to go up to 10,400 users during the period of the contract including the option periods.*

SaaS Solution Configuration and Implementation – Phase 1 Unclassified Data

Canada will make milestone payments in accordance with the Schedule of Milestones detailed below and the payment provisions of the Contract if:

a. an accurate and complete claim for payment and any other document required by the Contract have been submitted in accordance with the invoicing instructions provided in the Contract;

b. all work associated with the milestone and as applicable any deliverable required has been completed and accepted by Canada.

The schedule of milestones for which payments will be made in accordance with the Contract is as follows:

Milestone No.	Description or "Deliverable"	Firm Amount	Due Date or "Delivery Date"
1	**Kick-off** ***(Project Start-up)*** Project Authority, with the support of the Contractor will Kick-off the start of the project, and then ESDC and the Contractor will proceed with planning and design activities, as described in **Section 3 of the Statement of Work - Project Management and Governance Services**.	N/A	One (1) week after Contract/TA signing **Mid-September**
2	**Project Planning** ***(Project Management Planning complete)*** ESDC and the Contractor has delivered the project management planning Deliverables as described **in Section 3 of the Statement of Work - Project Management and Governance Services**, and these have been accepted by ESDC.	$(TBD)	(TBD) **Mid-October**
3	**Architecture and Design** ESDC and the Contractor has delivered the Architecture and Design planning Deliverables as describe in **Section 4.3 of the Statement of Work – Design and Configuration Services**	$(TBD)	(TBD) ***Must be before December 16, 2022**
4	**Core Solution Configuration and Integration Testing** Contractor has implemented and tested the SaaS Solution as described in **Section 5 of the Statement of Work – Testing and Implementation Services (Go-Live);** AND All Deliverables must be accepted by ESDC.	$(TBD)	(TBD) ***Must be before January 16, 2023**
5	**Operations** Contractor will commence performing operations, and related service activities, as described in **Section 8.2 of the Statement of Work - Operations**; Contractor has delivered, for the work required for this milestone, all the relevant elements of the plans described in **Section 3 of the Statement of Work - Project Management and Governance Services;** AND All Deliverables must be accepted by ESDC.	$(TBD) *Includes the Annual Subscription Fee during the 60-days stabilization step	One (1) day after the Milestone #4 *(Ongoing - Starts for each ESDC on-boarded application the day following its Go-live date)*
	Total – Phase 1	$(TBD)	

SaaS Solution Configuration and Implementation – Phase 2 Protected Data

***Phase 2 is conditional to the vendor obtaining all necessary Security Clearances under this Contract, as per the clauses in 7.3 of the contract and the APPENDIX A to Annex B: Security Obligations for Tier 2 (up to Protected B) AND will occur if/when ESDC decides to move forward with this phase.**

Canada will make milestone payments in accordance with the Schedule of Milestones detailed in the Contract and the payment provisions of the Contract if:

a. an accurate and complete claim for payment and any other document required by the Contract have been submitted in accordance with the invoicing instructions provided in the Contract;

b. all work associated with the milestone and as applicable any deliverable required has been completed and accepted by Canada.

The schedule of milestones for which payments will be made in accordance with the Contract is as follows:

Milestone No.	Description or "Deliverable"	Firm Amount	Due Date or "Delivery Date"
1	**Kick-off** ***(Project Start-up)*** Project Authority, with the support of the Contractor will Kick-off the start of the project, and then ESDC and the Contractor will proceed with planning and design activities, as described in **Section 3 of the Statement of Work - Project Management and Governance Services**.	N/A	**One (1) week after IT Security clearance obtained by Contractor/TA signing**
2	**Project Planning** ***(Project Management Planning complete)*** ESDC and the Contractor has delivered the project management planning Deliverables as described **in Section 3 of the Statement of Work - Project Management and Governance Services**, and these have been accepted by ESDC.	$(TBD)	(TBD)
3	**Architecture and Design** ESDC and the Contractor has delivered the Architecture and Design planning Deliverables as describe in **Section 4.3 of the Statement of Work – Design and Configuration Services**	$(TBD)	(TBD)
4	**Core Solution Configuration and Integration Testing** Contractor has implemented and tested the SaaS Solution as described in **Section 5 of the Statement of Work – Testing and Implementation Services (Go-Live);** AND All Deliverables must be accepted by ESDC.	$(TBD)	(TBD)
5	**Operations** Contractor will commence performing operations, and related service activities, as described in **Section 8.2 of the Statement of Work - Operations**; Contractor has delivered, for the work required for this milestone, all the relevant elements of the plans described in **Section 3 of the**	$(TBD) *Includes the Annual Subscription Fee during the 60-days	One (1) day after the Milestone #4 *(Ongoing - Starts for each ESDC on-boarded application*

	Statement of Work - Project Management and Governance Services; AND All Deliverables must be accepted by ESDC.	stabilization step	*the day following its Go-live date)*
	Total – Phase 2		$(TBD)

ANNEX D

SECURITY REQUIREMENTS CHECK LIST (Phase 2)

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat	
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: Employment and Social Development Canada	2. Branch or Directorate / Direction générale ou Direction: Human Resources Services Branch
3. a) Subcontract Number / Numéro du contrat de sous-traitance	3. b) Name and Address of Subcontractor / Nom et adresse du sous-traitant

4. Brief Description of Work / Brève description du travail
HRSB is requesting an Organization Chart solution; an automated and user-friendly approach for creating, developing and maintaining organization charts based on real-time PeopleSoft data that could be used by both HRSB and the clients.

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

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

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

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

Canada ☑	NATO / OTAN ☐	Foreign / Étranger ☐

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

Canada	NATO / OTAN	Foreign / Étranger
No release restrictions / Aucune restriction relative à la diffusion ☑ Type text here	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) ☐

TBS/SCT 350-103(2004/12)

Security Classification / Classification de sécurité

Canada

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
Security Classification / Classification de sécurité

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

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

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

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

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

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

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

Special comments:
Commentaires spéciaux : _____

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
Security Classification / Classification de sécurité

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

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

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

SUMMARY CHART / TABLEAU RÉCAPITULATIF

Category / Catégorie	PROTECTED / PROTÉGÉ			CLASSIFIED / CLASSIFIÉ			NATO				COMSEC					
	A	B	C	CONFIDENTIAL / CONFIDENTIEL	SECRET	TOP SECRET / TRÈS SECRET	NATO RESTRICTED / NATO DIFFUSION RESTREINTE	NATO CONFIDENTIAL / NATO CONFIDENTIEL	NATO SECRET	COSMIC TOP SECRET / COSMIC TRÈS SECRET	PROTECTED / PROTÉGÉ A	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).

ANNEX E

ELECTRONIC PAYMENT INSTRUMENTS

Canada requests that Bidders complete option 1 or 2 below:

1. ( ) Electronic Payment Instruments will be accepted for payment of invoices.

   The following Electronic Payment Instrument(s) are accepted:

   - ( ) Direct Deposit (Domestic and International);

2. ( ) Electronic Payment Instruments will not be accepted for payment of invoices.

The Bidder is not obligated to accept payment by Electronic Payment Instruments.

Acceptance of Electronic Payment Instruments will not be considered as an evaluation criterion.

ANNEX F

TASK AUTHORIZATION FORM

TASK AUTHORIZATION (TA) FORM	
Contractor:	**Contract No.**
Task Authorization No.: 450000XXXX	**Date:**
Financial coding:	**Amendment #:**
AMENDMENT INFORMATION (if applicable) Amendment # has been issued to… Amendment # has been issued to… ***All other terms and conditions remain the same***	
1. Statement of Work (Work Activities, Certifications and Deliverables)	
BACKGROUND **TASKS** **DELIVERABLES** **ESDC Contracting Authority:** Email: The ESDC Contracting Authority (or delegated representative) is responsible for the management of this TA. Any changes to the TA must be authorized in writing by the ESDC Procurement Representative. The Contractor is not to perform work in excess of or outside the scope of this TA based on verbal or written requests or instructions from any government personnel other than the aforementioned officer. **PLEASE SEND INVOICES TO:** The Project Authority: Email: The Project Authority (or delegated representative) is responsible for all matters concerning the technical content of the Work under this TA. Any proposed changes to the scope of the Work are to be discussed with the Project Authority, but any resulting change is only effective and enforceable if a written contract amendment is issued by the ESDC Procurement Representative or the PWGSC Contracting Authority.	

2. Period of Services:	**From:**	**To:**
3. Work Location:		
4. Travel Requirements:		
5. Language Requirements:		
6. Level of Security Clearance required:		

7. Cost Breakdown

Category	Name of Resource	Per Diem Rate	Estimated # of Days	Total Cost

	Estimated Cost	
	Applicable taxes	
	Total Estimated Cost	
	Total Travel & Living Cost	
	Maximum Total of TA	

8 SIGNATURES		
Project Authority:	**Signature:**	**Date:**
Contract Authority:	**Signature:**	**Date:**

Check Either Option:

___ The Contractor hereby accepts this task authorization

___ The Contractor does not accept this task authorization

Name of Contractor authorized to sign (type or print):	**Title of Contractor authorized to sign (type or print):**	**Date:**
Signature:		

ANNEX G

SERVICE LEVEL AGREEMENTS (SLA)

Bidders must submit published service level agreements (SLA) that outline the service level agreements.

The service level commitments (detailed in the published service level agreements) must provide commercial clients support that includes, at the minimum, any published and commercially available support (i.e. warranty, maintenance and support services) typically provided to customers who provision the SaaS.

Service Level Agreements may consist of a single document which applies to all SaaS Solutions or may consist of multiple SaaS Solution specific documents. Should a Bidder submit multiple SaaS Solution specific SLA documents, the Bidder must clearly define the SaaS Solution and the corresponding Ceiling Prices, the SLA applies to. If SLA terms are already specified in the SaaS Usage Terms and Conditions, duplicate terms need not be provided. The following are examples of terms that may be addressed in the Bidder's Service Level Agreement:

a) period during which the Bidder will support the SaaS users;
b) contact and procedure information for accessing Support;
c) procedures for resolution of problems;
d) response times;
e) procedures on how and when all telephone, fax or email communications will be responded to;
f) support web site availability to Canada's users (e.g. 24 hours a day, 365 days a year, and 99.9% of the time); and
g) Maintenance entitlements (e.g. patches, updates, major/minor releases, etc.)