BID SOLICITATION EMERGENCY MANAGEMENT APPLICATION SYSTEM FOR EMPLOYMENT and SOCIAL DEVELOPMENT CANADA

TABLE OF CONTENTS

PART 1 – GENERAL INFORMATION

1.1 Introduction

The bid solicitation is divided into seven (7) 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 Statement Requirement, the Basis of Payment, the Security Requirements, the Supply Chain Integrity Process, the Non-Disclosure Agreement related to Supply Chain Integrity, the Software as a Service (SaaS) Service Level Agreement (SLA), the Certification for the Federal Contractors Program for Employment Equity, the Task Authorization Form, and the SaaS IT Security (ITS) Assessment Program onboarding process.

1.2 Summary

a) This bid solicitation is being issued to satisfy the requirement of Employment and Social Development Canada (ESDC) (the "Client") for a SaaS Emergency Management Application System (EMAS) solution. This includes configuration, training, and the ability for Canada to isolate Assets and Information Assets in data centers that are geographically located in Canada. It is intended to result in the award of a contract for 1 year plus 9 irrevocable one-year options allowing Canada to extend the term of the contract.

b) ESDC is the Initial Client that will use the EMAS (the "Software as a Service Solution"). However, this bid solicitation will also allow Canada to make the Software as a Service Solution available to any department or Crown corporation (as those terms are defined in the Financial Administration Act) or any other party for which the Department of Public Service and Procurement Canada is authorized to act from time to time under section 16 of the Department of Public Works and Government Services Act (each a "Client"). Although Canada may make the Software as a Service Solution available to any or all the Clients, this bid solicitation does not preclude Canada from using another method of supply for entities of the Government of Canada with the same or similar needs.

c) The requirement is subject to the provisions of the World Trade Organization Agreement on Government Procurement (WTO-AGP), the North American Free Trade Agreement (NAFTA), the Canada-Chile Free Trade Agreement (CCFTA), the Canada-Peru Free Trade Agreement (CPFTA),

the Canada-Colombia Free Trade Agreement (CColFTA), the Canada-Panama Free Trade Agreement (CPanFTA) if it is in force, and the Agreement on Internal Trade (AIT).

d) There is a Federal Contractors Program (FCP) for employment equity requirement associated with this procurement: see Part 5 - Certifications, Part 7 - Resulting Contract Clauses and the Form 4 named “Federal Contractors Program for Employment Equity - Certification".

e) There are security requirements associated with this requirement. For additional information, consult Part 6 - Security, Financial and Other Requirements, and Part 7 - Resulting Contract Clauses. 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 website.

f) This bid solicitation allows bidders to use the epost Connect service provided by Canada Post Corporation to transmit their bid electronically. Bidders must refer to Part 2 entitled Bidder Instructions, and Part 3 entitled Bid Preparation Instructions, of the bid solicitation, for further information.

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 of receipt of the results of the bid solicitation process. The debriefing may be provided in writing, by telephone or in person at the discretion of the Contracting Authority.

1.4 Conflict of Interest

a) Bidders are advised to refer to Conflict of Interest provisions of SACC 2035, General Condition – Higher Complexity – Services (dated 2018-06-21) available on the PWGSC Website:

https://buyandsell.gc.ca/policy-andguidelines/standard-acquisition-clauses-and-conditions-manual

b) Without limiting in any way the provisions described in 1.4(a) above, Bidders are advised that Canada has engaged the assistance of the following private sector contractor(s) and resource(s) who have provided services including the review of content in preparation of this RFP and/or who have had, or may have had, access to information related to the content of the RFP or other documents related to the EMAS solicitation:

Milos Simovic from:
Simke Consulting Inc.
75 Meadowbreeze Drive
Kanata, Ont.
K2M 2L9
613-240-2716
m.simovic@rogers.com

c) Any bid that is received from one of the above-noted contractors, whether as a sole Bidder, joint venture or as a sub-contractor to a Bidder; or for which one of the above-noted resources provided any input into the bid, will be considered to be in contravention of the Conflict of Interest clauses identified in subsection 1.4, and the bid will be declared non-responsive.

PART 2 – BIDDER INSTRUCTIONS

2.1 Standard Instructions, Clauses and Conditions

a) All instructions, clauses and conditions identified in the bid solicitation by number, date and title are set out in the Standard Acquisition Clauses and Conditions Manual issued by Public Works and Government Services Canada.

b) Bidders who submit a bid agree to be bound by the instructions, clauses and conditions of the bid solicitation and accept the clauses and conditions of the resulting contract.

c) The 2003 (*2019-03-04)* Standard Instructions - Goods or Services - Competitive Requirements, are incorporated by reference into and form part of the bid solicitation.

d) Subsection 5.4 of 2003, Standard Instructions - Goods or Services - Competitive Requirements, is amended as follows:

Delete: 60 days
Insert: 250 days

2.2 Submission of Bids

Bids must be submitted using epost Connect for bids closing at the Bid Receiving Unit in the National Capital Region (NCR) the email address is:

tpsgc.dgareceptiondessoumissions-abbidreceiving.pwgsc@tpsgc-pwgsc.gc.ca

**It should be noted that the use of epost Connect service requires a Canadian mailing address. Should a bidder not have a Canadian mailing address, they may use the Bid Receiving Unit address specified above in order to register for the epost Connect service.

Note: Bids will not be accepted if emailed directly to this email address. This email address is to be used to open an epost Connect conversation, as detailed in Standard Instructions 2003, or to send bids through an epost Connect message if the bidder is using its own licensing agreement for epost Connect.

2.3 Former Public Servant

a) 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.

b) **Definitions**

i) 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:

i. an individual;

ii. an individual who has incorporated;

iii. a partnership made of former public servants; or

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

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

"pension" means a pension or annual allowance paid under the *Public Service Superannuation Act* (PSSA), 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-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 FPS 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: 2012-2 and the Guidelines on the Proactive Disclosure of Contracts.

d) 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.

For all contracts awarded during the lump sum payment period, the total amount of fees that may be paid to a FPS who received a lump sum payment is $5,000, including Applicable Taxes.

2.4 Enquiries – Bid Solicitation

a) All enquiries must be submitted in writing to the Contracting Authority no later than **10 calendar** days before the bid closing date. Enquiries received after that time may not be answered.

b) 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, Canada.

Note to Bidders: Bidders may, at their discretion, substitute the applicable laws of a Canadian province or territory of its choice without affecting the validity of its bid, by deleting the name of the Canadian province or territory specified and inserting the name of the Canadian province or territory of its choice. If no change is made, it acknowledges that the applicable laws specified are acceptable to the Bidder. *Bidders are requested to indicate the Canadian province or territory they wish to apply to any resulting contract in their Bid Submission Form*.

2.6 Improvement of Requirement during Solicitation Period

Should bidders consider that the specifications or Statement of Requirements 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 reasons 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 in accordance with the article entitled "Enquiries - Bid Solicitation". Canada will have the right to accept or reject any or all suggestions.

2.7 Volumetric Data

The data has been provided to Bidders to assist them in preparing their bids. The inclusion of this data in this bid solicitation does not represent a commitment by Canada that Canada's future usage of EMAS will be consistent with this data. It is provided purely for information purposes.

PART 3 – BID PREPARATION INSTRUCTIONS

3.1 Bid Preparation Instructions

a) Bidders must submit its bid electronically. Canada requests that the Bidder submits its bid in accordance with section 08 of the 2003 standard instructions. The epost Connect system has a limit of 1GB per single message posted and a limit of 20GB per conversation.

b) The bid must present the following sections of their bid in one (1) PDF:

i) Section I: Technical Bid

ii) Section II: Financial Bid

iii) Section III: Certifications

iv) Section IV: Supply Chain Integrity Information

3.2 Submission of Only One Bid

a) A Bidder, including related entities, will be permitted to submit only one bid in response to this bid solicitation. If a Bidder or any related entities participate in more than one bid (participating means being part of the Bidder, not being a sub-contractor), Canada will provide those Bidders with 2 working days to identify the single bid to be considered by Canada. Failure to meet this deadline will result in all the affected bids being disqualified.

b) For the purposes of this Article, regardless of the jurisdiction where any of the entities concerned is incorporated or otherwise formed as a matter of law (whether that entity Is a natural person, corporation, partnership, etc), an entity will be considered to be **"related"** to a Bidder if:

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

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

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

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

v. Individual members of a joint venture cannot participate in another bid, either by submitting a bid alone or by participating in another joint venture.

c) **Joint Venture Experience:**

i. Where the Bidder is a joint venture with existing experience as that joint venture, it may submit the experience that it has obtained as that joint venture.

Example: A bidder is a joint venture consisting of members L and O. A bid solicitation requires that the bidder demonstrate experience providing maintenance and help desk services for a period of 24 months to a customer with at least 10,000 users. As a joint venture (consisting of members L and O), the bidder has previously done the work. This

bidder can use this experience to meet the requirement. If member L obtained this experience while in a joint venture with a third party N, however, that experience cannot be used because the third party N is not part of the joint venture that is bidding.

ii. A joint venture bidder may rely on the experience of one of its members to meet any given technical criterion of this bid solicitation.

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

iii. Joint venture members cannot pool their abilities with other joint venture members to satisfy a single technical criterion of this bid solicitation. However, a joint venture member can pool its individual experience with the experience of the joint venture itself. Wherever substantiation of a criterion is required, the Bidder is requested to indicate which joint venture member satisfies the requirement. If the Bidder has not identified which joint venture member satisfies the requirement, the Contracting Authority will provide an opportunity to the Bidder to submit this information during the evaluation period. If the Bidder does not submit this information within the period set by the Contracting Authority, its bid will be declared non-responsive.

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

(1) Contracts all signed by A;

(2) Contracts all signed by B; or

(3) Contracts all signed by A and B in joint venture, or

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

(5) Contracts signed by B and contracts signed by A and B in joint venture.

That show in total 100 billable days.

iv. Any Bidder with questions regarding the way in which a joint venture bid will be evaluated should raise such questions through the Enquiries process as early as possible during the bid solicitation period.

3.3 Section I: Technical Bid

a) 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 in a thorough, concise and clear manner for carrying out the work.

b) 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.

c) The technical bid consists of the following:

i. **Substantiation of Technical Compliance:** The Technical Bid must substantiate the compliance of the Bidder's EMAS Service with Annex A - Statement of Requirements.

ii. The Bidder must include a description of its maintenance and support services, which must be consistent with all the requirements described in the Resulting Contract Clauses, including the Statement of Requirements. At a minimum, the Bidder must describe its:

(1) Problem reporting and response procedures;

(2) Escalation procedures;

(3) Support availability; and

(4) Any enhancements to the basic functionality that the Bidder is offering.

iii. **Technical Documentation:** The Bidder must provide technical documentation such as user manuals, screenshots, design or system management documents (or other information sources) to support the Bidder's response to each requirement (a soft copy of the technical documents required to support the Technical Bid is acceptable). Links to websites are not acceptable and if provided to validate a mandatory requirement, it will render the bid response non-responsive. The Bidder should include the precise location of the reference material including the title of the document, the page and the paragraph numbers when addressing each criterion. Any reference material listed by the Bidder to demonstrate the compliance must be part of the bid (hard copy or soft copy). If it is not included in the bid, it will not be taken into consideration by Canada. Where the reference is not sufficiently precise, Canada may request that the Bidder direct Canada to the appropriate location in the bid documentation.

iv. **Service Level Agreements:** Contractors must submit their published Service Level Agreements (SLAs), to be included in Annex F – SaaS Solution Level Agreements (SLAs).

By presenting a Submission, the Contractor acknowledges and agrees that any terms contained in the Annex F – SaaS Solution Service Level Agreements that purport to interpret the Contract, are the same or similar subject matter, or are related to the terms contained in the Contract Clauses, are deemed stricken and are of no force or effect.

The service level commitments (detailed in the published SLAs) must provide commercial clients support which 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 Solution.

The following are examples of terms that may be addressed in the Bidder's SLA:

a. Period during which the Bidder will support the Client;

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 or email communications will be responded to;

f. Website support availability to Clients (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.)

3.4 Section II: Financial Bid

a) Pricing: Bidders must submit their financial bid in accordance with the Annex B – Pricing Tables without any conditions, assumptions, or restrictions. Any financial proposal that purports to restrict the way in which Canada acquires goods or services under the resulting contract, with the exception of those limitations that are expressly set out in this solicitation, will be considered non-responsive. The total amount of Goods and Services Tax or Harmonized Sales Tax must be shown separately, if applicable. Unless otherwise indicated, bidders must include a single, firm, all-inclusive price quoted in Canadian dollars in each cell requiring an entry in the pricing tables.

b) All Costs to be Included: The financial bid must include all costs for the requirement described in the bid solicitation for the entire Contract Period, including any option to extend the Contract Period. The identification of all necessary equipment, software, peripherals, cabling and components required to meet the requirements of the bid solicitation and the associated costs of these items is the sole responsibility of the Bidder.

c) Blank Prices: Bidders are requested to insert "$0.00" for any item for which it does not intend to charge or for items that are already included in other prices set out in the tables. If the Bidder leaves any price blank, Canada will treat the price as "$0.00" for evaluation purposes and may request that the Bidder confirm that the price is, in fact, $0.00. No bidder will be permitted to add or change a price as part of this confirmation. Any bidder who does not confirm that the price for a blank item is $0.00 will be declared non-responsive.

3.5 Section III: Certifications

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

3.6 Section IV: Supply Chain Integrity Requirements

a) Bidders must meet the SCI requirements outlined in Annex A – Statement of Requirements, M10 and M11of the RFP.

b) Bidders must submit Supply Chain Security Information detailed in Annex " F" – SCI Submission Template, and must keep current, or update, any SCSI as required by the Supply Chain Security Authority. The Supply Chain Security Information will be used by Canada to assess whether, in its opinion, a Bidder's proposed supply chain creates the possibility that the Bidder's proposed SaaS Solution could compromise or be used to compromise the security integrity of Canada's equipment, firmware, software, systems or information in accordance with the Supply Chain Integrity Process as described in Section 4.4, **Supply Chain Integrity Process**.

c) By submitting its SCSI, and in consideration of the opportunity to participate in this procurement process, the Bidder agrees to the terms of the non-disclosure agreement contained in Annex E Non-Disclosure Agreement related to Supply Chain Integrity.

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

b) An evaluation team composed of representatives of the Client and PSPC will evaluate the bids on behalf of Canada. Canada may hire any independent consultant, or use any Government resources, to evaluate any bid. Not all members of the evaluation team will necessarily participate in all aspects of the evaluation.

c) In addition to any other time periods established in the bid solicitation:

   i. **Requests for Clarifications:** If Canada seeks clarification or verification from the Bidder about its bid, the Bidder will have 3 working days (or a longer period if specified in writing by the Contracting Authority) to provide the necessary information to Canada. Failure to meet this deadline will result in the bid being declared non-responsive.

      1. **Requests for Further Information:** If Canada requires additional information in order to do any of the following pursuant to the Section entitled "Conduct of Evaluation" in 2003, Standard Instructions - Goods or Services - Competitive Requirements: verify any or all information provided by the Bidder in its bid; or

      2. contact any or all references supplied by the Bidder (e.g., references named in the résumés of individual resources) to verify and validate any information submitted by the Bidder,

      3. the Bidder must provide the information requested by Canada within 3 working days of a request by the Contracting Authority.

   ii. Extension of Time: If additional time is required by the Bidder, the Contracting Authority may grant an extension in his or her sole discretion.

4.2 Technical Evaluation

a) Mandatory Requirements

   i. Each bid will be reviewed for compliance with the mandatory requirements of the bid solicitation. Any element of the bid solicitation that is identified specifically with the words "must" or "mandatory" is a mandatory requirement. Bids that do not comply with each and every mandatory requirement will be declared non-responsive and be disqualified.

   ii. The mandatory requirements are described in Annex A – Statement of Requirements

b) Point Rated Requirements

   i. Each bid will be rated by assigning a score to the rated requirements, which are identified in the bid solicitation by the word "rated" or “should’ or by reference to a score. Bidders who fail to submit complete bids with all the information requested by this bid solicitation will be rated accordingly.

ii. The point-rated requirements are described in Annex A – Statement of Requirements

4.3 Financial Evaluation

a) The financial evaluation will be conducted by calculating the **Total Bid Price** using the Pricing Tables completed by the bidders.

b) The financial evaluation process is described in Annex B – Basis of Payment.

c) **Formulae in Pricing Tables:**

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

d) **Substantiation of Professional Services Rates**

In Canada's experience, bidders will from time to time propose rates at the time of bidding for one or more categories of resources that they later refuse to honour, on the basis that these rates do not allow them to recover their own costs and/or make a profit. When evaluating the rates bid for professional services, Canada may, but will have no obligation to, require price support in accordance with this Article. If Canada requests price support, it will be requested from all otherwise responsive bidders who have proposed a rate that is at least 20% lower than the median rate bid by all responsive bidders for the relevant resource category or categories. If Canada requests price support, the Bidder must provide the following information:

i. an invoice (referencing a contract serial number or other unique contract identifier) that shows that the Bidder has provided and invoiced a customer (with whom the Bidder deals at arm's length) for services performed for that customer similar to the services that would be provided in the relevant resource category, where those services were provided for at least three months within the twelve months before the bid solicitation closing date, and the fees charged were equal to or less than the rate offered to Canada;

ii. in relation to the invoice in (i), evidence from the Bidder's customer that the services identified in the invoice include at least 50% of the tasks listed in the Statement of Work for the category of resource being assessed for an unreasonably low rate. This evidence must consist of either a copy of the contract (which must describe the services to be provided and demonstrate that at least 50% of the tasks to be performed are the same as those to be performed under the Statement of Work in this bid solicitation) or the customer's signed certification that the services subject to the charges in the invoice included at least 50% of the same tasks to be performed under the Statement of Work in this bid solicitation;

iii. in respect of each contract for which an invoice is submitted as substantiation, a résumé for the resource that provided the services under that contract that demonstrates that, in relation to the resource category for which the rates are being substantiated, the resource would meet the mandatory requirements and achieve any required pass mark for any rated criteria; and

iv. the name, telephone number and, if available, e-mail address of a contact person at the customer who received each invoice submitted under (i), so that Canada may verify any information provided by the Bidder.

v. Once Canada requests substantiation of the rates bid for any resource category, it is the sole responsibility of the Bidder to submit information (as described above and as otherwise may be requested by Canada, including information that would allow Canada to

verify information with the resource proposed) that will allow Canada to determine whether it can rely, with confidence, on the Bidder's ability to provide the required services at the rates bid. If Canada determines that the information provided by the Bidder does not adequately substantiate the unreasonably low rates, the bid will be declared non-responsive

4.4 Supply Chain Integrity Process

a) During the RFP process, the Contract period and any resulting Option periods, the Supply Chain Security Authority identified by Canada, may, based on its National Security mandate to protect Canada's IT infrastructure as well as to assess threats, risks and vulnerabilities, assess the Bidder's SCSI.

b) Canada will assess whether, in its opinion, the Bidder's supply chain creates the possibility that the Bidder's supply chain or proposed solution could compromise or be used to compromise the security integrity of Canada's equipment, firmware, software, systems or information, or represents a threat to Canada's National Security, in accordance with Section 2 of Annex D - Supply Chain Integrity Process.

c) It is a condition precedent to any contract award that a Bidder successfully satisfy the Security Authority's Supply Chain Integrity assessment. Canada will assess whether, in its opinion, the Bidder's supply chain creates the possibility that Bidders' proposed solution could compromise or be used to compromise the security integrity of Canada's equipment, firmware, software, systems or information in accordance with Section 4 of Annex D - Supply Chain Integrity Process.

4.5 Basis of Selection

a) To be declared responsive, a bid must:

i. comply with the terms and conditions of the bid solicitation;
ii. comply with all the requirements of the bid solicitation;
iii. meet all mandatory technical evaluation criteria; and
iv. achieve a score of at least 75% of the Rated Requirements.

Bids not meeting (i) or (ii) or (iii) or (iv) will be declared non-responsive.

b) Price is given a rating value which is included in the total calculation of the bid. 70% of the points will be awarded to the technical bid and 30% of the points will be awarded to the financial bid.

To complete this calculation, the following formula is used:

$$\left(\frac{Score\ of\ the\ rated\ requirements\ of\ the\ Bid}{Maxumum\ score\ possible}\right) \times 70\% \ = Total\ 1$$

$$\left(\frac{Lowest\ Total\ Assessed\ Price}{Total\ Assessed\ Price\ of\ the\ bid}\right) \times 30\% \ = Total\ 2$$

$$(Total\ 1) + (Total\ 2) \ = Combined\ Rating\ of\ Technical\ Merit\ and\ Price$$

c) The top-ranked responsive bid will be determined based on the proposal which has met all mandatory criteria, has met or exceeded the required minimum pass marks of the rated requirements and offers the **Highest Responsive Combined Rating of Technical Merit and**

Price as calculated above. The Top-ranked responsive bid, will be recommended for Contract award.

d) Bidders should note that all contract awards are subject to Canada's internal approvals process, which includes a requirement to approve funding in the amount of any proposed contract. Despite the fact that the Bidder may have been recommended for contract award, a contract will only be awarded if internal approval is granted according to Canada's internal policies. If approval is not granted, no contract will be awarded.

e) If more than one bidder is ranked first because of identical overall scores, then the bidder with the best financial score will become the top-ranked bidder.

4.6 Proof of Proposal Test for Top-Ranked Bid

a) Through the Proof of Proposal (PoP) test, Canada may test the solution proposed in the top -ranked bid (identified after the financial evaluation) to confirm both that it will function as described in the bid and that it meets the technical functionality requirements described in Annex A. The PoP test will take place at a site in the National Capital Region provided by Canada that simulates the technical environment that is required to satisfy what is described in Annex A – Statement of Requirements.

b) After being notified by the Contracting Authority, the Bidder will be given a maximum of 5 working days to prepare the proposed solution. Canada will then conduct the PoP test. Representative(s) of the Bidder may be present during the PoP test. The representative(s) named in the bid are to provide technical support during the PoP test should be available in person or by telephone for technical advice and clarification during the PoP test; however, Canada is not required to delay the PoP test if an individual is unavailable.

c) Canada will document the results of the PoP Test. If Canada determines that the proposed solution does not meet any mandatory requirement of the bid solicitation, the bid will fail the PoP Test and the bid will be disqualified. Canada may, as a result of the PoP test, reduce the score of the Bidder on any rated requirement, if the PoP test indicates that the score provided to the Bidder on the basis of its written bid is not validated by the PoP test. The Bidder's score will not be increased as a result of the PoP test. If the Bidder's score is reduced as a result of the PoP test, Canada will reassess the ranking of all bidders.

d) In connection with the PoP testing, the Bidder grants to Canada user access to the Bidder's proposed solution for testing and evaluation purposes.

4.7 IT Assessment for Top-Ranked Bid

Prior to contract award, the top bidder must complete the Canadian Center for Cyber Security (CCCS) IT Assessment program.

4.8 Confirmation of Registration for the SaaS IT Security (ITS) Assessment:

The response must include documentation confirming that the bidder registered for the SaaS Security Assessment Process as described in Annex H – SaaS IT Security (ITS) Assessment Program: Onboarding Process.

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 Bidder 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.

(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, to be given further consideration in the procurement process.

5.2 Certifications Precedent to the 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.

a) **Integrity Provisions – Required Documentation**

In accordance with the section titled Information to be provided when bidding, contracting or entering into a real property agreement of the Ineligibility and Suspension Policy, the Bidder must provide the required documentation, as applicable, to be given further consideration in the procurement process.

b) **Federal Contractors Program for Employment Equity - Bid Certification**

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

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

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

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

the Bidder must provide the Contracting Authority with a completed Annex G - Federal Contractors Program for Employment Equity - Certification, for each member of the Joint Venture.

PART 6 – SECURITY, FINANCIAL AND OTHER REQUIREMENTS

6.1 Financial Capability

a) **Financial Capability Requirement**: The Bidder must have the financial capability to fulfill this requirement. To determine the Bidder's financial capability, the Contracting Authority may, by written notice to the Bidder, require the submission of some or all of the financial information detailed below during the evaluation of bids. The Bidder must provide the following information to the Contracting Authority within fifteen (15) working days of the request or as specified by the Contracting Authority in the notice:

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

ii. If the date of the financial statements in (a) above is more than five months before the date of the request for information by the Contracting Authority, the Bidder must also provide, unless this is prohibited by legislation for public companies, the last quarterly financial statements (consisting of a Balance Sheet and a year-to-date Income Statement), as of two months before the date on which the Contracting Authority requests this information.

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

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

2. the last quarterly financial statements (consisting of a Balance Sheet and a year-to-date Income Statement) as of two months before the date on which the Contracting Authority requests this information.

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

v. A confirmation letter from all of the financial institution(s) that have provided short-term financing to the Bidder outlining the total of lines of credit granted to the Bidder and the amount of credit that remains available and not drawn upon as of one month prior to the date on which the Contracting Authority requests this information.

vi. A detailed monthly Cash Flow Statement covering all the Bidder's activities (including the requirement) for the first two years of the requirement that is the subject of the bid solicitation, unless this is prohibited by legislation. This statement must detail the Bidder's major sources and amounts of cash and the major items of cash expenditures on a monthly basis, for all the Bidder's activities. All assumptions made should be explained as well as details of how cash shortfalls will be financed.

vii. A detailed monthly Project Cash Flow Statement covering the first two years of the requirement that is the subject of the bid solicitation, unless this is prohibited by legislation. This statement must detail the Bidder's major sources and amounts of cash and the major items of cash expenditures, for the requirement, on a monthly basis. All assumptions made should be explained as well as details of how cash shortfalls will be financed.

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

c) If the Bidder is a subsidiary of another company, then any financial information in 1. (a) to (f) above required by the Contracting Authority must be provided by the ultimate parent company. Provision of parent company financial information does not by itself satisfy the requirement for the provision of the financial information of the Bidder, and the financial capability of a parent cannot be substituted for the financial capability of the Bidder itself unless an agreement by the parent company to sign a Parental Guarantee, as drawn up by Public Works and Government Services Canada (PWGSC), is provided with the required information.

d) **Financial Information Already Provided to PWGSC**: The Bidder is not required to resubmit any financial information requested by the Contracting Authority that is already on file at PWGSC with the Contract Cost Analysis, Audit and Policy Directorate of the Policy, Risk, Integrity and Strategic Management Sector, provided that within the above-noted time frame:

1. the Bidder identifies to the Contracting Authority in writing the specific information that is on file and the requirement for which this information was provided; and
2. the Bidder authorizes the use of the information for this requirement.

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

e) **Other Information**: Canada reserves the right to request from the Bidder any other information that Canada requires to conduct a complete financial capability assessment of the Bidder.

f) **Confidentiality**: If the Bidder provides the information required above to Canada in confidence while indicating that the disclosed information is confidential, then Canada will treat the information in a confidential manner as permitted by the *Access to Information Act*, R.S., 1985, c. A-1, Section 20(1) (b) and (c).

g) **Security**: In determining the Bidder's financial capability to fulfill this requirement, Canada may consider any security the Bidder is capable of providing, at the Bidder's sole expense (for example, an irrevocable letter of credit from a registered financial institution drawn in favour of Canada, a performance guarantee from a third party or some other form of security, as determined by Canada).

6.2 Security Obligations Related to Protected B Cloud Security

a) General

i) 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**").

ii) Flow-Down of Security Obligations: The obligations of the Contractor contained in these Security Obligations must be flowed down by the Contractor to any Subcontractors to the extent applicable.

iii) Change Management:

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

(B) The Contractor must advise Canada of all changes that may have an adverse affect to the Solution, including technological, administrative or other types of changes or improvements.

(C) The Contractor agrees to offer all commercially available improvements as part of its standard service offering at no additional cost to Canada.

b) Acknowledgments

i) 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 Contract Award.

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

c) Securing Canada's Data

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

d) Roles and Responsibilities for Security

i) 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.

ii) The Contractor must provide to Canada an up-to-date document that delineates the roles and responsibilities: (i) at contract award; (ii) on an annual basis; (iii) when there

are changes to such roles and responsibilities as a result of a Change to the Cloud Services; or (iv) upon request of Canada.

e) Third-Party Assurance: Certifications and Reports

i) 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 in the Contractor's security practices and policies.

ii) 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 – certification achieved by an accredited certification body; AND

(C) ISO/IEC 27018:2019 Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

(D) 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.

iii) 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 there are any exclusions identified, or there is a need to separate a subservice organizations such as data centre hosting, the subservice organization's assessment report must be provided.

iv) 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 findings by the auditor.

v) 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).

vi) The Contractor is expected to maintain its certification of ISO 27001, ISO 27017, ISO/IEC 27018:2019, 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.

f) Auditing Compliance

i) 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.

ii) 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.

iii) 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.

g) Cloud Service Provider (CSP) IT Security Assessment Program

i) 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/modern-emergingtechnologies/cloud-computing/government-canada-security-control-profile-cloud-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 above in clause #5, and validated through independent third party assessments.

ii) Compliance will be assessed and validated by Employment and Social Development Canada (ESDC). (https://cyber.gc.ca/en/guidance/cloud-service-provider-information-technology-security-assessment-process-itsm50100).

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

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

(B) A copy of the most recent completed assessment report provided by the Government of Canada;; and

(C) A copy of the most recent summary report provided by the Government of Canada.

(D) The Contractor should contact the ESDC Innovation, Information and Technology Branch, Information Technology Security, for any additional information related to the CSP IT Security Assessment Program.

(E) It is the continuous obligation of the Contractor to notify ESDC when there are changes to the Cloud Service offerings.

iv) In the situation where the Contractor is a SaaS provider using a GC-approved SaaS Provider that already complies with Section 5 - Third-Party Assurance and Section 7 - Cloud Service Provider (CSP) IT Security Assessment Program, sub-sections (1) and (2) the SaaS provider must provide Canada with a copy of an email provided by the Government of Canada confirming that the Bidder has completed the CSP ITS Assessment Program.

h) Data Protection

i) The Contractor must:

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

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

(C) Implement security controls that restrict administrative access to Canada's Data and Systems by the Contractor to individuals on a need-to-know basis, including individuals that provide technical or customer support, and provide Canada with an approval process to grant the Contractor access to Canada's Data to perform support, maintenance or operational activities.

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

ii) 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. In addition, the Contractor must ensure that no Protected B information is processed outside of Canada.

iii) The Contractor must ensure that any processing performed outside of Canada including moving or transmitting approved copies of data are performed within the agreed upon service regions.

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

i) Data Isolation

i) 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.

ii) 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.

j) Data Location

i) The Contractor must 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.

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

iii) 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.

iv) 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 store Canada's Data at rest; 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.

v) 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 store Canada's Data at rest.

k) Data Transfer and Retrieval

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

(A) Extract all online, near-line, 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.bac-lac.gc.ca/eng/services/governmentinformation-resources/guidelines/Pages/guidelines-file-formats-transferring-informationresources-enduring-value.aspx).

l) Data Disposition and Returning Records to Canada

i) 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:

(A) National Industrial Security Program Operating Manual (DoD 5220.22-M6);

(B) (Guidelines for Media Sanitization (NIST SP 800-88); or

(C) Clearing and Declassifying Electronic Data Storage Devices (ITSP.40.006 v2). Upon request of Canada, the Contractor must provide a document that describes the Contractor's process for disposal or reuse of resources.

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

m) Cryptographic Protection

The Contractor must:

i) 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;

ii) Use cryptographic algorithms and cryptographic key sizes and crypto periods that have been validated by the Cryptographic Algorithm Validation Program

iii) (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-unclassifiedprotected-and-protected-b-information-itsp40111);

iv) 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/guidance/cryptographic-algorithms-unclassified-protected-and-protected-b-information-itsp40111), 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

v) 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.

n) Key Management

The Contractor must ensure that a key management service can be leveraged and provides capabilities, including but not limited to:

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

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

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

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

v) 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;

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

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

o) 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.

p) 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.

q) Identity and Access Management

i) 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://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.

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

r) Federation

i) 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, or subsequent versions, where the End User credentials and authentication to cloud services are under the sole control of Canada; and

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

s) Privileged Access Management

The Contractor must:

i) 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, incluning those that are used to host GC services;

ii) 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;

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

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

v) 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-information-technology-systems-itsp30031-v3);

vi) 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-guidance-information-technology-systems-itsp30031-v3);

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

viii) 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;

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

x) 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;

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

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

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

t) Remote Management

i) 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) (https://cyber.gc.ca/en/guidance/user-authentication-guidance-information-technology-systems-itsp30031-v3);

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

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

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

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

ii) 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.

u) Network and Communications Security

The Contractor must:

i) Enforce 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;

ii) 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/guidance-securelyconfiguring-network-protocols-itsp40062)and ITSP.40.111 (https://cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-andprotected-b-information-itsp40111);

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

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

v) Logging and Auditing

i) 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), Event Logging Guidance (https://www.canada.ca/en/government/system/digital-government/online-security-privacy/event-logging-guidance.html), 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.

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

iii) 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 providing APIs that provide the ability to inspect and interrogate data at rest in SaaS applications including assessing events such as user access and behaviour,

administrator access and behaviour, and changes to third-party API access stored in SaaS application logs.

w) Continuous Monitoring

i) 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 pre-emptive and responsive actions, to mitigate threats.

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

x) Security Incident Management

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

(A) A published and documented Security Incident Response Process for review by Canada that is aligned with one of the following standards: (i) ISO/IEC 27035:2011 Information technology -- Security techniques -- Information security incident management; or (ii) NIST SP800-612, Computer Security Incident Handling Guide; or (iii) GC Cyber Security Event Management Plan (GC CSEMP) (https://www.canada.ca/en/government/system/digital-government/online-security-privacy/security-identity-management/government-canada-cyber-security-event-management-plan.html); or (iv) other best practices from industry standards, if Canada determines, in its discretion, that they meet Canada's security requirements.

(B) Documented processes and procedures of how the Contractor will identify, respond, remediate, report, and escalate Security Incidents to Canada, including: (i) the scope of the information security incidents that the Contractor will report to Canada; (ii) the level of disclosure of the detection of information security incidents and the associated responses; (iii) the target timeframe in which notification of information security incidents will occur; (iv) the procedure for the notification of information security incidents; (v) contact information for the handling of issues relating to information security incidents; 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:

(1) 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;

(2) 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;

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

iii) 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.

iv) 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.

y) Security Incident Response

i) The Contractor must alert and promptly notify Canada (via phone and/or 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.

ii) If the Contractor becomes aware of any compromise, breach 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.

z) Information Spillage

i) 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 and Steps to Address Data Spillage in the Cloud (ITSAP.50.112) https://www.cyber.gc.ca/en/guidance/steps-address-data-spillage-cloud-itsap50112 ; 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.

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

aa) Security Testing and Validation

i) 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.

ii) 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.

bb) Personnel Security Screening

i) The Contractor must ensure that security measures are implemented to 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.

ii) 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.

iii) 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.

cc) Physical (Data Centre / Facilities) Security

i) The Contractor must ensure that physical security measures are implemented to protect the 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 Directive on Security Management, Appendix C: Mandatory Procedures for Physical Security Control (https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32611&section=procedure&p=C). The security measures required under this include, at a minimum:

(A) Sufficient redundancy and recovery capabilities within and between the

(B) 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;

(C) Proper handling of IT Media, in accordance with Annex B to Guidance on the Security Categorization of Cloud-Based Services (ITSP.50.103) - Canadian Centre for Cyber Security

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

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

(F) 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;

(G) Escorting visitors and monitoring visitor activity;

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

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

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

iii) If any physical security measures is to change in a way that degrades the physical security, the Contractor must inform Canada. Canada reserves the right to terminate the contract for default if Canada determines that the Contractor does not meet the physical security requirements specified in the contract.

dd) Supply Chain Risk Management

i) The Contractor must ensure that safeguards are implemented 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.

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

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

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

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

iii) 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.

iv) 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.

ee) Data Segregation

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

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

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

PART 7 – RESULTING CONTRACT CLAUSES

7.1 Requirement

The Contractor agrees to provide the Service and perform the Work described in the Contract, including the statement of requirements, in accordance with and at the prices set out in the Contract.

7.2 Services

The Contractor agrees to provide the Service identified in Annex A – Statement of Requirements, which includes, at a minimum:

(1) User access to the Software as a Service (SaaS) Solution described in the Contract;

(2) providing Solution Documentation;

(3) maintaining, upgrading, and updating the Solution(s);

(4) managing incidents and defects to ensure the Solution(s) operate at the applicable service levels;

(5) providing incidental and additionally required information technology infrastructure service;

(6) providing infrastructure service required to deliver the Solution; and,

(7) providing professional services and training, as and when requested by Canada.

7.3 Professional Services

The Contractor agrees to provide the following Professional Services (the "Work"), as and when requested by Canada, using the Task Authorization process:

(1) implementation services, including configuration, migration, rollout assistance, acceptance testing assistance and transition to live operational state, as defined in the Statement of Requirements; and,

(2) training services.

7.4 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.

7.5 Client

The initial Client is the Employment and Social Development Canada (ESDC). However, the Contracting Authority can add additional Clients from time to time, which may include any department or Crown corporation as described in the Financial Administration Act (as amended from time to time), and any other party for which the Department of Public Works and Government Services may be authorized to act from time to time under section 16 of the Department of Public Works and Government Services Act.

7.6 Reorganization of Clients

The Contractor's obligation to provide the Services and perform the Work will not be affected by (and no additional fees will be payable as a result of) any form of reorganization or restructuring of any Client. Canada may designate replacement Contracting Authority or Technical Authority.

7.7 Term and Auto Renewal

(1) **Contract Period.** The Contract Period includes the entire period of time during which the Contractor is obliged to provide the Services and perform the Work.

(2) **Initial Term.** This Contract begins on the date the Contract is awarded and ends one (1) year later.

(3) **Option Periods.** The Contractor grants to Canada the irrevocable option to extend the term of the Contract by up to nine 9 additional 1-year period(s) under the same terms and conditions The Contractor agrees that, during the extended period of the Contract, it will be paid in accordance with the applicable provisions set out in the Basis of Payment. Canada may exercise the option(s) at any time by sending a written notice to the Contractor at least 2 calendar days before the expiry date of the Contract. The option may be exercised only by the Contracting Authority, and will be evidenced, for administrative purposes only, through an amendment to the Contract.

(4) **Auto-Renewal Opt Out.** Canada hereby provides notice to the Contractor that it opts out of any auto-renewal of the term obligation. The Contractor acknowledges receipt of the notice, and represents that this Contract will be valid only until the end of the Contract Period, as defined above.

7.8 Time of the Essence

(1) It is essential that the Service be provided within or at the time stated in the Contract.

(2) It is essential that the Work be delivered within or at the time stated in a Task Authorization.

7.9 Termination for Convenience

(1) At any time before the completion of the Services, 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 Services 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, 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.

(5) The Contractor must ensure that EMAS data will be available to Canada, in CSV format suitable for repatriation to Canada, for three (3) months after access is cancelled.

7.10 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 any one 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.

https://laws-lois.justice.gc.ca/eng/acts/A-1/

7.11 Solution

(1) **Software as a Service.** The Contractor will deliver 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.

(2) **Commercially-Available Solution.** Canada acknowledges that the 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 Canada all the features and functionalities included in the commercially available version of the Solution, and the incidental and required information technology infrastructure services required to deliver the Solution, all of which is included in the subscription price.

(3) **Software Application Evolution; Features or Functionalities.** Canada acknowledges that the Solution, underlying software application or associated infrastructure may evolve during the course of the Contract Period. The Contractor agrees to continue to provide the Service as the commercially available Solution, with functionality or features and on with terms that are no less favourable than as at the time of Contract award.

(4) **Improvements to and Evolution of the Solution.** The parties acknowledge that technology and business models evolve quickly and that any 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 Solution and any potential peripherals are delivered to Canada 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 Solution and infrastructure throughout the Contract Period on a commercially reasonable basis, and must provide

those improvements and enhancements to Canada as part of Canada'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 Solution and offers those functions in any new or other services or products, the Bidder must continue to provide those functions to Canada as part of Canada'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. Contractor has no obligation to comply with this paragraph if the Solution acquired by Canada is still offered by Contractor in parallel with the new services offered to other customers.

(5) The Contractor must ensure that upgrades/updates to the EMAS system must:

(a) not result in additional work by Canada with the exception of applicable testing;

(b) not result in any loss of Canada's data, electronic documents, or user accounts.

7.12 Services

7.12.1 Solution Services

(1) **Software as a Service.** The Contractor will provide all Services required for Canada to access and use the Solution as specified in the Contract.

(2) **Authority.** The Contractor represents and warrants that it owns or has obtained and will maintain throughout the Contract Period, all necessary authority specifically including intellectual property rights required to provide the Services in accordance with the terms of this Contract.

(3) **Indemnification.** The Contractor agrees to indemnify Canada against all losses and expenses (including legal fees) arising out of any intellectual property infringement claim by a third party based on Canada's use of the Solution.

(4) **Accessibility:** The Contractor must ensure that the Solution does not interfere with accessibility standards compliance, as specified in the Standard on Web Accessibility: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=23601#

(5) **Usage Grant.** The Contractor grants to Canada the non-exclusive, non-assignable right to access and use the Solution from an unlimited number of locations, devices and operating environments, through secure, wireless, mobile or other connection, via the internet, a web browser or other access connection technology which may become available.

(6) **Included**. The Contractor represents and warrants that the Services include

(a) hosting and maintenance of the Solution,

(b) provision of all incidental and additional required information technology infrastructure services, in compliance with all required security standards,

(c) the technical infrastructure that complies with all required security standards, allowing Canada to use the Solution to process any of Client's Data in compliance with its expressed security standards, and

(d) unfettered access and use by the Client, regardless of the amount of data created, processed or stored by the Solution,

(e) all of which is included in the price.

(7) **Restricted Usage Rights**. Canada acknowledges that in providing the Services, the Contractor is not delivering ownership rights to any software product, component of the Solution or infrastructure used by the Contractor to provide the Services, except as expressly provided in a Task Authorization. Canada will not knowingly:

(a) distribute, license, loan, or sell the Solution;

(b) impair or circumvent the Solution's security mechanisms; or

(c) remove, alter, or obscure any copyright, trademark, or other proprietary rights notice on or in the Solution.

(8) **Applicable Terms and Conditions**. The Contractor has advised and Canada acknowledges that the Contractor may unilaterally modify the terms under which it provides its commercial offering of the Solution, without notice to its customers, including Canada. The Contactor represents and warrants that any such modification will not result in less favourable terms, specifically including price, service levels and remedies, regardless of any notification to the contrary.

(9) **Additional Terms and Conditions.** The parties agree that any terms and conditions, including any "click-through" or "pop-up" notices, that apply to the Contractor's commercial offering of the Solution, including third party tools or incidental infrastructure, will not apply to Canada's use of the Solution if those terms conflict with the express terms of this Contract. The terms and conditions of third party tools not specified the Contract are not subject to this section.

(10) **Commercial SaaS Offering.** Canada acknowledges that it will accept the Contractor's commercial SaaS offering, and states that, unless explicitly identified as Work or Services to be delivered under this Contract, Canada does not require custom development, alternative services, service levels, functionalities or features.

7.12.2 Service Levels

(1) **Annex I**. Service Level Agreement (provided by the Contractor) contains the specific information defining the levels and standards for processes and performance expectations for the Services to be delivered under the Contract, and must be read in conjunction with the following section:

(a) **Service Credits.** The Contractor will provide the applicable Service Credits to Canada for failing to achieve the uptime Solution Availability levels as defined in Annex F, Service Level Agreement.

(b) **Exclusions.** The Contractor will expressly specify any exclusions to the Solution Availability levels identified in Annex F, Service Level Agreement.

(c) **Support Services.** The Contractor will provide technical support assistance, **in both English and French**, in strict compliance with Annex F, Service Level Agreement.

(d) **Escalation.** The Contractor will provide an escalation process for dispute resolution, which is identified in Annex F, Service Level Agreement.

(e) **No Infringement.** The Contractor warrants that nothing in the Solution, or in Canada's use of the Solution, will infringe or constitute a misappropriation of the intellectual property or other rights of a third party.

7.12.3 Documentation

(1) **Solution Documentation**. The Contractor must provide or deliver access to the commercially available Solution Documentation to Canada, in English, upon Contract Award. The Contractor must update Solution Documentation on a commercially reasonable basis.

(2) **Other Documentation.** The Contractor must provide or deliver access to any documentation required in performance of the Work.

7.12.4 Translation Rights.

The Contractor agrees that Canada may translate any written deliverable, including the Solution Documentation or Training Materials into English or French. The Contractor acknowledges that Canada owns any translation and is under no obligation to provide it to the Contractor. Canada will include any copyright and/or proprietary right notice that was part of the original document in any translation. The Contractor will not be responsible for technical errors that arise as a result of any translation made by Canada.

7.12.5 Moral Rights.

At the request of Canada, the Contractor may provide a written permanent waiver of moral rights, in a form acceptable to Canada, from every author that contributed to the written deliverable. If the Contractor is unable or unwilling to obtain the requested waivers, the Contractor agrees to indemnify Canada against all losses and expenses (including legal fees) arising out of any moral rights infringement claim by a third party based on Canada's translation of written documentation.

7.12.6 Defective Documentation.

If at any time during the Contract Period, Canada advises the Contractor a defect or non-conformance in any part of the documentation delivered with the Work, the Contractor will correct the defect or non-conformance must as soon as possible and at its own expense. Canada may provide the Contractor with information about defects or non-conformance in other documentation, including the Solution Documentation, for information purposes only.

7.12.7 Conduct of the Work.

Warranty. 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, to effectively perform the Work.

7.12.8 Remedies

(1) **Work.** If at any time during the Contract Period the Work fails to meet its warranty obligations, the Contractor must as soon as possible correct at its own expense any errors or defects and make any necessary changes to the Work.

(2) **Documentation.** If at any time during the Contract Period, Canada discovers a defect or non-conformance in any part of the documentation delivered with the Work, the Contractor must as soon as possible correct at its own expense the defect or non-conformance.

(3) **Canada's Right to Remedy.** If the Contractor fails to fulfill any obligation described herein within a reasonable time of receiving a notice, Canada will have the right to remedy or to have remedied the defective or non-conforming Work at the Contractor's expense. If Canada does not wish to correct or replace the defective or non-conforming Work, an equitable reduction will be made in the Contract Price.

7.12.9 Subcontracts

(1) **Conditions to Subcontracting**. The Contractor may subcontract the performance of the Work, provided (a) the Contractor obtains the Contracting Authority's prior written consent, (b) the sub-contractor is bound by the terms of this Contract, and (c) the Contractor remains liable to Canada for all the Work performed by the sub-contractor.

(2) **Exceptions to Subcontracting Consent**. 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: (i) purchase "off-the-shelf" items and any standard articles and materials that are ordinarily produced by manufacturers in the normal course of business (ii) subcontract any incidental services that would ordinarily be subcontracted in performing the Work; and (iii) permit its sub-contractor at any tier to make purchases or subcontract as permitted in paragraphs (i) and (ii).

7.12.10 Excusable Delay

(1) **No Liability.** The Contractor will not be liable for performance delays nor for non-performance due to causes beyond its reasonable control that could not reasonably have been foreseen or prevented by means reasonably available to the Contractor, provided 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 (referred to as an "Excusable Delay").

(2) **Notice.** The Contractor must also advise the Contracting Authority, within 15 business 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.

(3) **Delivery and Due Dates.** 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.

(4) **Canada not responsible for Costs.** 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 sub-contractors or agents as a result of an Excusable Delay.

7.12.11 Right to Terminate.

If such an event prevents performance under the Contract for more than 30 calendar days, then the Contracting Authority may elect to terminate the TA, or part or all of this Contract on a "no fault" basis, meaning neither party will be liable to the other in connection with the Excusable Delay or resulting termination, and Canada will only be responsible for paying for those services received up to the effective date of the termination.

7.12.12 Professional Services : Transition Services

(1) **Migration.** The Contractor acknowledges that the nature of the Services provided under the Contract, Canada may require continuity. Prior to the transition to the new contractor or to Canada, the Contactor must provide all operational, technical, design and configuration information and documentation for all Services required to complete the transition, provided that it is not Contractor confidential information (including all EMAS data, information, and user credentials). The Contractor represents and warrants that it will not directly or indirectly interfere with or impede Canada's access to or transfer of Client's Data.

(2) **Migration and/or Transition Services.** The Contractor agrees that, in the period leading up to the end of the Contract Period, if Migration or Transition Services are requested by Canada, it will diligently assist Canada in the transition from the Contract to a new contract with another Contractor and or migrate Client's Data to a new contractor environment, that there will be no charge for the services below other than those charges set out in the Basis of Payment.

7.12.13 Inspection and Acceptance of the Work

(1) **Inspection by Canada**: All the Work is subject to inspection and acceptance by Canada. Canada's inspection and acceptance of the Work does 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 the Contractor is required to correct or replace it at its own expense.

(2) **Acceptance Procedures**: Unless provided otherwise in the Contract, the acceptance procedures are as follows:

(a) when the Work is complete, the Contractor must notify the Project Authority in writing, with a copy to the Contracting Authority, by referring to this provision of the Contract and requesting acceptance of the Work;

(b) Canada will have up to 30 days from receipt of the notice to perform its inspection (the "Acceptance Period").

(3) **Deficiencies and Resubmission of Deliverable:** If Canada provides notice of a deficiency during the Acceptance Period, the Contractor must address the deficiency as soon as possible and notify Canada in writing once the Work is complete, at which time Canada will be entitled to re-inspect the Work before acceptance and the Acceptance Period will begin again. If Canada determines that a deliverable is incomplete or deficient, Canada is not required to identify all missing items or all deficiencies before rejecting the deliverable.

(4) **Access to Locations:** The Contractor must provide representatives of Canada access to all locations where any part of the Work is being performed, other than multi-tenant data centres, 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.

(5) **Contractor Inspection for Quality:** The Contractor must inspect and approve any part of the Work before submitting it for acceptance or delivering it to Canada. All deliverables submitted by the Contractor must be of a professional quality, free of typographical and other errors, and consistent with the highest industry standards.

(6) **Inspection Records**: 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.

(7) **Informal Feedback:** Upon request by the Contractor, Canada may provide informal feedback prior to any deliverable being formally submitted for acceptance. However, this must not be used as a form of quality control for the Contractor's Work. Canada is not obliged to provide informal feedback.

7.13 Task Authorization

(1) **As-and-when-requested Task Authorizations**. 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. The Contractor must not commence work until a validly issued TA has been issued by Canada and received by the Contractor. The Contractor acknowledges that any work performed before such issuance and receipt will be done at the Contractor's own risk.

(2) **Form and Content of draft Task Authorization:**

(a) The Business Technical Authority will provide the Contractor with a description of the task using the "Task Authorization Form".

(b) The draft Task Authorization 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 draft TA will also include the applicable basis (bases) and method (methods) of payment as specified in the Contract.

(c) A draft Task Authorization must also contain the following information, if applicable:

a. the task number;
b. The date by which the Contractor's response must be received (which will appear in the draft Task Authorization, but not the issued Task Authorization);
c. the details of any financial coding to be used;
d. the categories of resources and the number required;
e. a description of the work for the task outlining the activities to be performed and identifying any deliverables (such as reports);
f. the start and completion dates;
g. milestone dates for deliverables and payments (if applicable);
h. the number of person-days of effort required;
i. whether the work requires on-site activities and the location;
j. the language profile of the resources required;
k. the level of security clearance required of resources;
l. the price payable to the Contractor for performing the task, with an indication of whether it is a firm price or a maximum TA price (and, for maximum price task

authorizations, the TA must indicate how the final amount payable will be determined; where the TA does not indicate how the final amount payable will be determined, the amount payable is the amount, up to the maximum, that the Contractor demonstrates was actually worked on the project, by submitting time sheets filled in at the time of the work by the individual resources to support the charges); and

m. any other constraints that might affect the completion of the task.

(3) **Contractor's Response to Draft Task Authorization**. The Contractor must provide to the Business Technical Authority, within 10 working days of receiving the draft Task Authorization (or within any longer time period specified in the draft TA), the proposed total price for performing the task and a breakdown of that cost, established in accordance with the Basis of Payment specified in the Contract. The Contractor's quotation must be based on the rates set out in the Contract. The Contractor will not be paid for preparing or providing its response or for providing other information required to prepare and validly issue the TA.

(4) **Task Authorization Limit and Authorities for Validly Issuing Task Authorizations**

To be validly issued, a TA must include the following signatures:

(a) for any TA with a value, inclusive of revisions, of less than or equal to $25,000 (including Applicable Taxes), the TA must be signed by:

a. the Business Technical Authority; and

b. a representative from the Contractor; and

(b) for any TA with a value greater than this amount, a TA must include the following signatures:

a. the Business Technical Authority; and

b. a representative from the Contractor; and

c. the Contracting Authority.

(5) Any TA that does not bear the appropriate signatures is not validly issued by Canada. Any work performed by the Contractor without receiving a validly issued TA is done at the Contractor's own risk. If the Contractor receives a TA that is not appropriately signed, the Contractor must notify the Contracting Authority. By providing written notice to the Contractor, the Contracting Authority may suspend the Client's ability to issue TAs at any time, or reduce the dollar value threshold described in sub-article (A) above; any suspension or reduction notice is effective upon receipt.

(6) **Periodic Usage Reports**. The Contractor must compile and maintain records on its provision of services to the federal government under the Task Authorizations validly issued under the Contract. The Contractor must provide this data to Canada 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 quarterly basis to the Contracting Authority. From time to time, the Contracting Authority may also require an interim report during a reporting period.

(7) The quarterly periods are defined as follows:

(a) 1st quarter: April 1 to June 30;

(b) 2nd quarter: July 1 to September 30;

(c) 3rd quarter: October 1 to December 31; and

(d) 4th quarter: January 1 to March 31.

(8) The data must be submitted to the Contracting Authority no later than 15 calendar days after the end of the reporting period.

(9) Each report must contain the following information for each validly issued TA (as revised):

(a) the Task Authorization number and the Task Authorization Revision number(s), if applicable;

(b) a title or a brief description of each authorized task;

(c) the name, Category of Personnel of each resource involved in performing the TA, as applicable;

(d) the total estimated cost specified in the validly issued TA of each task, exclusive of Applicable Taxes;

(e) the total amount, exclusive of Applicable Taxes, expended to date against each authorized task;

(f) the start and completion date for each authorized task; and

(g) the active status of each authorized task as applicable (e.g., indicate whether work is in progress or if Canada has cancelled or suspended the TA, etc.).

(10) Each report must also contain the following cumulative information for all the validly issued TAs (as revised):

(a) The amount exclusive of Applicable Taxes, specified in the Contract (as last revised, as applicable) as Canada's total liability to the Contractor for all authorized TA's; and

(b) the total amount, exclusive of Applicable Taxes, expended to date against all validly issued tasks.

(11) **Consolidation of TAs for Administrative Purposes.** The Contract may be amended from time to time to reflect all validly issued Task Authorizations to date, to document the Work performed under those TAs for administrative purposes.

7.14 Basis of Payment

(1) **Subscription.** For the Services, including access to and use of the Solution, Solution Documentation, Support Services, and incidental and additionally required information technology infrastructure services (all the Services described in this Contract that is not Work), Canada shall pay the prices detailed in Annex B – Basis of Payment, of the Contract.

(2) **Professional Services provided under a Task Authorization.** For professional services requested by Canada, in accordance with a validly issued Task Authorization, Canada will pay the Contractor, in arrears, the firm price set out in the Task Authorization, in accordance with the firm all-inclusive per diem rates set out in Annex B – Basis of Payment, of the Contract. Applicable Taxes extra.

(3) **On-Site Support Charges.** If approved in advance by Canada, the Contractor will be paid the daily labour rates specified in Annex B – Basis of Payment, of the Contract, together with reasonable and proper travel and living costs incurred by the Contractor in connection with on-site services. Any travel and living costs will only be reimbursed in accordance with the applicable meal and private vehicle allowances provided in the National Joint Council Travel Directive, as amended from time to time. All such pre-approved costs must be invoiced to Canada as a separate charge.

7.15 Payment

7.15.1 Invoices

(1) **Invoice Submission.** The Contractor must submit invoices, as applicable.

(2) **Invoice Requirements**. Invoices must be submitted in the Contractor's name and contain:

(a) the date, the name and address of the client department, item or reference numbers, deliverable/description of the service or work, contract number, Client Reference Number (CRN), Procurement Business Number (PBN), 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) Applicable Taxes must be shown as a separate line item along with corresponding registration numbers from the tax authorities and all items that are zero-rated, exempt or to which Applicable Taxes do not apply, must be identified as such on all invoices

(d) deduction for holdback, if applicable; and

(e) the extension of the totals, if applicable.

7.15.2 Taxes

(1) **Payment of Taxes**. 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 must remit to appropriate tax authorities any amounts of Applicable Taxes paid or due.

(2) **Withholding for Non-Residents.** 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.

(3) **Certification of Invoices.** By submitting an invoice, the Contractor certifies that the invoice is consistent with the Work delivered and is in accordance with the Contract.

7.15.3 Payment Period.

Canada will pay the Contractor's undisputed invoice amount within 30 days of receipt. In the event, an invoice is not in acceptable form and content, Canada will notify the Contractor and the 30 day payment period will begin on receipt of a conforming invoice.

7.15.4 Interest on Late Payments.

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, provided Canada is responsible for the delay in paying the Contractor. Canada will not pay interest on overdue advance payments.

7.15.5. Method of Payment.

Canada will make payment to the Contract for the Services either in advance or in arrears, in accordance with Annex F - Service Level Agreement or the Contractor's bid, as applicable. Where payment is made in advance, the advance payment period shall not exceed 12 months. Payment in advance does not prevent Canada from exercising any or all potential remedies in relation to this payment or the delivery of the Services.

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

7.15.6 Limitation of Expenditure.

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

7.15.7 Electronic Payment of Invoices.

The Contractor accepts to be paid using any of the following Electronic Payment Instrument(s):

(1) Visa Acquisition Card:
(2) MasterCard Acquisition Card;
(3) Direct Deposit (Domestic and International);
(4) Electronic Data Interchange (EDI);
(5) Wire Transfer (International Only);
(6) Large Value Transfer System (LVTS) (Over $25M)

7.15.8 Insurance Requirements.

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.

7.16 Price Stability

The Contractor acknowledges that it is important to Canada to be able to continue to access the SaaS products and services detailed in the Contract. The Contractor accordingly offers to continue to provide the SaaS products and services at reasonable rates and on all of the other terms and conditions set out in this Contract, subject to execution by the parties of a formal contract(s)

therefor. For each of the 2 years that follow the Term of Contract, the Contractor hereby offers annual rates that are the lesser of:

a) the Contractor's then current published rates; and

b) the previously contracted rates adjusted by the percentage difference in the Consumer Price Index (CPI) as determined by Statistics Canada, for the 12 month period immediately preceding the date on which the price change is to be effective; and

c) 3% more than the annual rates provided to Canada in the preceding year under this Contract or under any extension entered into pursuant to this Article;

and the Contractor's obligations under this Article shall survive termination or expiry of this Contract.

7.17 Price Certification

The Contractor certifies that the price quoted is not in excess of the lowest price charged anyone else, including the Contractor's most favoured customer, for the like quality and quantity of the goods, services or both.

7.18 Limitation of Liability

7.18.1 First Party Liability:

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

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

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

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

(a) wilful misconduct or deliberate acts of wrongdoing, and

(b) any breach of warranty obligations.

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

7.19 General Provisions

(1) **Applicable Laws.** This Contract will be interpreted and governed by the laws of _____.
(This will be filled in at Contract Award using the information from the bid)

(2) **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.

(3) **Severability.** If any provision of this Contract is declared unenforceable by an authoritative court, the remainder of this Contract will remain in force.

(4) **Waiver.** The failure or neglect by a party to enforce any of rights under this Contract will not be deemed to be a waiver of that party's rights.

(5) **No Bribe.** The Contractor warrants 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.

(6) **Contingency Fees.** The Contractor represents 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).

(7) **International Sanctions**

(a) 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.

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

(c) 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.

(8) **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.

(9) **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.

(10) **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.

(11) **Authorities**

(a) **Contracting Authority**

Name: Daniel Ferguson
Title: Procurement Team Lead
Telephone: 343-543-3961
E-mail address: Daniel.ferguson@tpsgc-pwgsc.gc.ca

The Contracting Authority must receive a copy of the Invoice for Canada's record and review.

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

(b) **Business Technical Authority**

Name: Jennifer Forsythe
Title: Manager of Emergency Management and Business Continuity
Telephone: 819-654-4672
E-mail address: Jennifer.forsythe@servicecanada.gc.ca

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

(c) **Administrative Contact**

Name: Jennifer Forsythe
Title: Manager, Emergency Management and Business Continuity
Phone: 819-654-4672
E-mail address: Jennifer.forsythe@servicecanada.gc.ca

(d) **Supply Chain Security Authority**
Name:
Title:
Phone:
E-mail address:

The Supply Chain Security Authority is the SSC representative and is responsible for all matters concerning the ongoing Supply Chain Integrity Process under the Contract. Neither the Contracting Authority nor the Technical Authority have any authority to advise or authorize any information in relation to the Supply Chain Integrity Process. All other security-related matters remain the responsibility of the Supply Chain Security Authority.

7.20 – Security Obligations

7.20.1 Purpose

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

7.20.2 Flow-Down of Security Obligations

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

7.20.3 Acknowledgments

(1) The parties acknowledge that:
   (a) All Assets and Information Assets are subject to these Security Obligations.

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

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

7.20.4 Securing Information Assets

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

7.20.5 Roles and Responsibilities for Security

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

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

7.20.6 Third-Party Assurance: Certifications and Reports

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

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

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

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

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

7.20.7 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 Assets and Information Assets as follows:

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

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

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

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

7.20.8 Cryptographic Protection

(1) The Contractor must:

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

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

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

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

7.20.9 Data Segregation

(1) The Contractor must implement controls to ensure appropriate isolation of resources such that Information Assets are not co-mingled with other tenant data, while in use, storage or transit, and throughout all aspects of the Contractor's Service's 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; and

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

7.20.10 Data Location and Protection Isolation

(1) The Software as a Service Solution must have the ability for Canada to store and protect its Information Assets, in transit and 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 29 Data Centre / Facilities (i.e. Physical Security)

(b) Employs a CSEC Approved Cryptographic Algorithms encryption to ensure that no data is written to disk in an unencrypted form: https://www.cse-cst.gc.ca/en/publication/itsa-11e

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

7.20.11 Data Protection

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

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

(3) Upon request, the Contractor must:

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

(b) expressly advising Canada of Contractor's future intent to use 3rd party services or API as part of the Service that could be delivered, from outside of Canada, specifying all such locations abroad (country, province, city) where data would be stored and processed and where they manage the service from, in order for Canada to take an appropriate decision whether to accept that modification or not.

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

7.20.12 Data Transfer and Retrieval

(1) The Contractor must, upon request by Canada:

(a) Extract all online, nearline, and offline information assets, including, but not limited to, databases, object and file storage, system configurations, cloud activity logs, 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 Information Assets, including metadata, in a machine-readable and usable format acceptable to Canada, in accordance with the Library and Archives Canada Guidelines on File Formats for Transferring Information Resources of Enduring Value (https://www.bac-lac.gc.ca/eng/services/government-information-resources/guidelines/Pages/guidelines-file-formats-transferring-information-resources-enduring-value.aspx).

7.20.13 Data Disposition and Returning Records to Canada

(1) In the event of contract termination or expiry, the Contractor must return all Government of Canada data as outlined in requirement M45 of the Statement of Requirements.

(2) The Contractor must upon request, securely dispose or reuse resources (e.g. equipment, data storage, files, and memory) that contain Information Assets and ensure that previously stored data cannot be accessed by others customers after it is released. This includes all copies of Information Assets that are made through replication for high availability and disaster recovery. The 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).

(3) The Contractor must provide evidence that demonstrates successful erasing, purging or destruction of all resources, as appropriate, and an ability to prevent re-instantiation of any removed or destroyed system, capability (software or process), data, or information instances once removed from the Canada instance.

7.20.14 Access Control

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

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

(b) Role-based access;

(c) Access controls on objects in storage; and

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

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

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

7.20.15 Federation of Identity

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

(a) Implement multi-factor authentication mechanisms to authenticate end users with privileged access, in accordance with CCCS ITSP.30.031 V2 (or subsequent versions)

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

(c) Ability to associate Canada unique identifiers (e.g. a Canada unique ID, a Canada email address, etc.) with the corresponding cloud service user account(s).

7.20.16 Endpoint Protection

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

7.20.17Secure 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, (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.

7.20.18 Application Programming Interface (API)

(1) The Contractor must:

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

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

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

(a) Interrogate data at rest in SaaS applications; and

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

7.20.19 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 Services and Canada's Information Assets to only authorized devices and End Users with an explicit need to have access;

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

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

(e) Implement password policies to protect credentials from compromise by either on-line or off-line attacks and to detect these attacks by logging and monitoring events such as (i) successful use of credentials, (ii) unusual use of credential, and (iii) access to and exfiltration from the password database, in accordance with CSE's ITSP.30.031 V2 (or subsequent versions) (https://www.cse-cst.gc.ca/en/node/1842/html/26717);

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

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

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

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

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

7.20.20 Contractor Remote Management

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

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

(b) Employ a CSEC Approved Cryptographic Algorithms mechanisms to protect the confidentiality of remote access sessions: https://www.cse-cst.gc.ca/en/publication/itsa-11e ;

(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.

7.20.21 Network and Communications Security

(1) The Contractor must:

(a) Provide the ability for Canada to establish secure connections to the Services, including providing data-in-transit protection between Canada and the Service using TLS 1.2, or subsequent versions, and using supported cryptographic algorithms and certificates, as outlined in CSE's ITSP.40.062 (https://cyber.gc.ca/en/guidance/guidance-securely-configuring-network-protocols-itsp40062) and ITSP.40.111 (https://cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-and-protected-b-information-itsp40111);

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

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

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

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

7.20.22 Logging and Auditing

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

(2) The Contractor must maintain a log of reported issues (trouble tickets) with at least the following data included (Reporter/Requestor name, Resolution description, Number of issues requiring escalation, Resolution's estimated turnaround time

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

(a) log and detect audit events such as a minimum of (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 time-stamped 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 Service provided to it by the Contractor or a Contractor 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.).

7.20.23 Continuous Monitoring

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

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

(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 Services, data and components relevant to Canada's IaaS, PaaS or SaaS 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 Services or libraries that the 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 Services; and

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

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

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

7.20.24 Notifications

(1) The Contractor must provide:

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

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

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

7.20.25 Security Incident Management

(1) The Contractor's Security Incident response process for the Services must encompass the IT security incident management lifecycle and supporting practices for preparation, detection, analysis, containment, and recovery activities, aligned with one of the following standards: (i) ISO/IEC 27035:2011 Information technology -- Security techniques -- Information security incident management; or (ii) NIST SP800-612, Computer Security Incident Handling Guide; or (iii) GC Cyber Security Event

Management Plan (GC CSEMP) (https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/government-canada-cyber-security-event-management-plan.html); or (iv) other best practices of Leading Service Providers if Canada determines, in its discretion, that they meet Canada's security requirements.

(2) The Contractor's Security Incident response process must include the following:

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

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

7.20.26 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 multifunction in any asset, (iii) irregular or unauthorized access to any Asset, (iv) large scale copying of an Information Asset, or (v) another irregular activity identified by the 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 24 hours.

(2) If the Contractor becomes aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data or Personal Data while processed by the 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 effects and to minimize any damage resulting from the Security Incident.

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

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

a. request and receive information associated with the Security Incident and any compromised Information Assets (including user data, system/security event logs, network or host packet captures, logs from security components such as

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

b. track the status of a reported information security event or Security Incident.

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

(4) The Contractor must:

(a) 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

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

7.20.27 E-discovery and Legal Holds

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

7.20.28 Information Spillage

(1) The Contractor must provide Canada with a document that outlines the process it follows to respond to an Information Spillage Incident. The process must be aligned with: (i) ITSG-33 Security Control for IR-9 Information Spillage Response; or (ii) another best practice of Leading Service Providers 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 Information Asset that is involved in an Asset's or System's contamination;

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

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

(2) The Contractor must provide an up-to-date information spillage process to Canada on an annual basis, or promptly following any Change to the Contractor's information spillage process.

7.20.29 Security Assessment and Authorization Evidence

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 Service components within the Contractor environment.

7.20.30 Personal Security Screening

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

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

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

(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. This includes, at a minimum:

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

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

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

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

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

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

7.20.31 Data Centre Facilities

(1) The Contractor must implement physical security measures that ensure the protection of IT facilities and information system assets on which Assets and Information Assets are stored and processed against all forms of tampering, loss, damage, and seizure. Physical protection of all facilities that host Canada data and information assets, must be applied in accordance with, or use an adequate risk-based approach based on a prevent-detect-respond-recover approach to physical security, aligned with the physical security controls and the practices in the Royal Canadian Mounted Police (RCMP) guidance and standards on physical security. The security measures required under this include, at a minimum:

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

(b) Proper handling of IT Media;

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

(d) Controlled access to information system output devices to prevent unauthorized access to GC data and Information Assets;

(e) Controlling and managing physical access devices;

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

(g) Escorting visitors and monitoring visitor activity;

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

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

7.20.32 Supply Chain Management

(1) The Contractor of the Services must implement safeguards to mitigate supply chain threats and vulnerabilities to IT services in order to maintain confidence in the security of the sources of information systems and the IT components used to provide Services. This includes, but is not limited to designing and implementing controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privilege access for all personnel within the supply chain.

(2) The Contractor must provide Canada with a "Supply Chain Risk Management (SCRM) Plan" that describes the Contractor's approach to supply chain risk management (SCRM) and demonstrates how the Contractor's approach to SCRM will reduce and mitigate supply chain risks. The SCRM Plan must be aligned with one of the following best practices and be assessed and validated by an independent third party certified under AICPA or CPA Canada, and/or ISO certification regime: (i) ISO/IEC 27036 Information technology -- Security techniques -- Information security for Contractor 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 an update 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 Publisher using a GC-approved IaaS Provider that already complies with Section 13 - Supply Chain Risk Management requirements, within 90 days of contract award, the SaaS Publisher 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.

7.20.33 On-going Supply Chain Integrity Process

(1) The Parties acknowledge that security is a critical consideration for Canada with respect to this Contract and that on-going assessment of SaaS will be required throughout the Contract Period.

(2) The parties acknowledge that Canada reserves the right to review the native SaaS of any Contractor in whole or in part at any time for supply chain integrity concerns. This acknowledgement does not obligate the Contractor to support the SCI review.

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

7.20.34 Change of Control

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

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

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

(4) Despite the foregoing, Canada's right to terminate on a "no-fault" basis will not apply to circumstances in which there is an internal reorganization that does not affect the ownership of the ultimate parent corporation or parent partnership of the Contractor or sub-contractor, as the case may be; that is, Canada does not have a right to terminate the CONTRACT pursuant to this Article where the Contractoror sub-contractor continues, at all times, to be controlled, directly or indirectly, by the same ultimate owner.

7.20.35 Sub-processors

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

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

7.20.36 Master / Root Account Management

(1) The Contractor must ensure the adequate protection of the account management and billing management process used by Canada, Services for Canada including Services provided or enabled through a Cloud Reseller. Security measures include but is not limited to:

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

(b) Ensuring the separation of duties of individuals;

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

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

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

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

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

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

(i) Ensuring that credentials remain within the geographical boundaries of Canada.

7.21 – Privacy Obligations

7.21.1 Purpose

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

7.21.2 Flow-Down of Privacy Obligations

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

7.21.3 Change Management

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

The Contractor must advise Canada of all improvements that affect the Services in this Contract, including technological, administrative or other types of 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.

7. 21.4 Acknowledgments

(1) The parties acknowledge that:

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

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

(c) The Contractor must not have or attempt to gain custody of any Information Asset, nor permit any Services Personnel to access any Information Asset prior to the implementation of the Privacy Requirements as required under this Schedule on or before the go live date.

7. 21.5 Protecting Information Assets

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

7. 21.6 Third-Party Assurance: Certifications

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

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

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

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

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

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

7. 21.7 Privacy Compliance

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

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

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

(2) This applies to all information, data and metadata in the Contractors possession or under its care acquired pursuant to, or arises in any other way out of Contractor's responsibilities and obligations under the Contract. The Contractor acknowledges that this is required in order to ensure that Canada can rely on the information, data and metadata and so that Canada can meet its own legal obligations, including statutory obligations. This is also required to ensure the information, data and metadata can be used as persuasive evidence in a court of law.

7. 21.8 Auditing Compliance

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

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

(3) 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 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 qualified, independent, third party security auditors that (i) is qualified under the AICPA, CPA Canada, or ISO certification regime, and (ii) conforms to the

ISO/IEC 17020 quality management system standard at the Contractor's selection and expense.

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

(5) 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 Contractor Sub-processor to supplement the certification and audit reports described in this in order to demonstrate the Contractor's compliance with the required industry certifications.

7.21.9 Data Ownership and Privacy Requests

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

(2) All data that it stores, hosts or processes on behalf of Canada remains the property of Canada. When requested by the Contracting Authority, the Contractor must provide Personal Information records within two Federal Government Working Days (or five Federal Government Working Days if it must be retrieved from offsite backup/replication) in a Word or Excel document.

7. 21.10 Privacy Officer

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

7. 21.11 Assist in Delivery of Canada's Privacy Impact Assessment

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

7. 21.12 Privacy Breach

(1) The Contractor must alert and promptly notify the Technical Authority (via phone and email) of any compromise, breach or of any evidence that leads the Cloud Service Provider to reasonably believe that risk of compromise, or a breach, is or may be imminent, or if existing safeguards have ceased to function, over the following period (7 days x 24 hours x 365 days), and within the Cloud Service Provider's service level commitments**.**

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

a. notify Canada of the Security Incident;

b. investigate the Security Incident and provide Canada with detailed information about the Security Incident; and

c. take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

(3) The Contractor must:

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

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

7. 21.13 Ownership of Personal Information and Records

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

7. 21.14 Use of Personal Information

The foreign recipient Contractor/Sub-contractor agrees to create, collect, receive, manage, access, use, retain and dispose of the Personal Information and the Records only to perform the Work in accordance with the contract/subcontract.

7. 21.15 Collection of Personal Information

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

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

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

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

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

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

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

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

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

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

7. 21.16 Maintaining the Accuracy, Privacy, and Integrity of Personal Information

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

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

(b) segregate all Records from the foreign recipient Contractor's/Sub-contractor's own information and records;

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

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

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

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

(g) include a notation on any Record(s) that an individual has requested be corrected if the foreign recipient Contractor/Sub-contractor has decided not to make the correction for any reason.

Whenever this occurs, the foreign recipient Contractor/Sub-contractor must immediately advise the Contracting Authority of the details of the requested correction and the reasons for the foreign recipient Contractor's/Sub-contractor's decision not to make it. If directed by the Contracting Authority to make the correction, the Contractor must do so;

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

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

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

7. 21.17 Safeguarding Personal Information

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

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

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

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

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

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

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

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

7. 21.18 Statutory Obligations

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

(2) The foreign recipient Contractor/Sub-contractor acknowledges that its obligations under the contract/subcontract are in addition to any obligations it has under the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, or similar legislation in effect from time to time in any province or territory of Canada. If the foreign recipient Contractor/Sub-contractor believes that any obligations in the contract/subcontract prevent it from meeting its obligations under any of these laws,

the foreign recipient Contractor/Sub-contractor must immediately notify the Contracting Authority of the specific provision of the contract/subcontract and the specific obligation under the law with which the foreign recipient Contractor/Sub-contractor believes it conflicts.

7. 21.19 Legal Requirement to Disclose Personal Information

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

7. 21.20 Complaints

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

7. 21.21 Exception

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

7.22 Federal Contractors Program for Employment Equity - Default by the Contractor

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

7.23 Priority of Documents

(1) 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; including any individual SACC Manual clauses incorporated by reference in these Articles of Agreement;

(b) Annex A, Statement of Requirements;

(c) Annex B, Basis of Payment;

(d) Annex C, Security Requirements Check List;

(e) Annex D, Supply Chain Integrity Process;

(f) the signed Task Authorizations (including all of their annexes, if any);

(g) the Contractor's bid dated _____, (*insert date of bid*)

(h) Annex "H" SaaS IT Security (ITS) Assessment Program: Onboarding Program

(i) the Contractor's SaaS Service Level Agreement (SLA);

(j) Annex G, Non-Disclosure Agreement.

7.24 Foreign Nationals (Canadian Contractor)

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

Note to Bidders: *Either this clause or the one that follows, whichever applies (based on whether the successful Bidder is a Canadian Contractor or Foreign Contractor), will be included in any resulting contract*

7.25 Foreign Nationals (Foreign Contractor)

(a) SACC Manual clause A2001C (2006-06-16) Foreign Nationals (Foreign Contractor)

APPENDIX A - DEFINITIONS AND INTERPRETATIONS

In this Contract, unless the context otherwise requires, the following terms shall have the following meanings:

"Asset" means all information technology resources used, accessed or managed by the Contractor to provision and deliver the Services described in this Agreement (including, without limitation, all technology resources at the Contractor's Service Locations or at the Contractor's or a Sub-contractor's data centre, networking, storage, servers, virtualization platforms, operating systems, middleware, and applications).

"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.

"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.

"Canada", "Crown", "Her Majesty" or "the Government" means Her Majesty the Queen in right of Canada as represented by the Minister of Public Works and Government Services and any other person duly authorized to act on behalf of that minister or, if applicable, an appropriate minister to whom the Minister of Public Works and Government Services has delegated his or her powers, duties or functions and any other person duly authorized to act on behalf of that minister.

"Canada Data" means information or data, regardless of form or format:

A. disclosed by or related to the Canada's personnel, clients, partners, joint venture participants, licensors, vendors or contractors;
B. disclosed by or related to End Users of the Services; or
C. collected, used or processed by, or stored for, the Services; which is directly or indirectly:
    i. disclosed to the Contractor or Sub-contractors by or on behalf of the Canada or End Users;
    ii. to which the Contractor or any Sub-contractors obtains access, intentionally or inadvertently;
    iii. resident on any Asset, or on any other network, System or Hardware used or managed for Canada by the Contractor for the Services and Contractor's services, including Contractor Infrastructure; or
    iv. generated, developed, acquired or otherwise obtained by the Contractor or any Sub-contractor or Sub-processor as part of or in the course of providing the Services; and includes all information derived from such information and all metadata forming part of or associated with such information. For greater certainty, "Canada Data" includes all information and data stored in or processed through the Services, Assets, or Contractor Infrastructure.

"Client" means the department or agency for which the Work and/or Services are performed under the Contract. In such respect, Client may refer to any Government Department, Departmental Corporation or Agency, or other Crown entity described in the Financial Administration Act (as amended from time to time), and any other party for which the Department of Public Works and Government Services may be authorized to act from time to time under section 16 of the Department of Public Works and Government Services Act.

"Client Data" means (i) any data provided to the Contractor by Client or at its direction in connection with the Solution and (ii) all content that the Contractor develops and delivers to Client, and that Client accepts, in accordance with this Contract.

"Cloud Computing" means a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

"Cloud Infrastructure" means the collection of hardware and software that enables the five essential characteristics of cloud computing. The cloud infrastructure can be viewed as containing both a physical layer and an abstraction layer. The physical layer consists of the hardware resources that are necessary to support the cloud services being provided, and typically includes server, storage and network components. The abstraction layer consists of the software deployed across the physical layer, which manifests the essential cloud characteristics. Conceptually the abstraction layer sits above the physical layer. [NIST]

"Cloud Service Provider ("CSP")" means the entity that owns, operates and maintains the physical infrastructure on which a Solution is hosted and from which a Solution is distributed. A CSP may also be SaaSP if they host and distribute their own and third-party solutions. "Commercially Available" means a product and/or service available to the public to obtain for use or consumption and requires no special modification or maintenance over its life cycle.

"Contract" means the Articles of Contract, any general conditions, any supplemental general conditions, annexes, appendices 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.

"Contractormeans the entity named in the Contract to provide the Services and/or the Work 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.

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

"Deliverable" or "Deliverables", when used generically, refers to any discrete part of the Work to be performed for Canada.

"Device" means equipment having a physical central processor unit (CPU), mass storage and input output devices such as keyboard and monitor and includes servers, desktops, workstations, notebooks, laptops, personal digital assistants and mobile computing equipment.

"Error" means any instruction or statement contained in or absent from the Solution, which, by its presence or absence, prevents the Solution from operating in accordance with the Specifications.

"Federal Government Working Day" is defined as Monday to Friday, 8:00 am to 4:00 pm Eastern Time, excluding statutory holidays observed by Canada.

"IaaS" or "Infrastructure as a Service" means "(t)he capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does

not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls)."

"IaaS Infrastructure" means Infrastructure managed by the Contractor and provided as a Service (e.g. Data Center, Networking, Storage, Servers, Virtualization platform). This also includes the Systems, Hardware and Software that are used to manage, operate and provision an IaaS Infrastructure.

"Information Assets" means any individual data element of such Canada Data.

"Information Spillage" means incidents where an Information Asset is inadvertently placed on an Asset or System that is not authorized to process it (e.g. ITSG-33, IR-9).

"PaaS" or "Platform as a Service" means "(t)he capability provided to the consumer to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. [NIST]

"PaaS Infrastructure" means the platform infrastructure managed by the Contractor and provided as a Service (e.g. Data Center, Networking, Storage, Servers, Virtualization platform, O/S, Middleware, and Runtime). This also includes the Systems, Hardware and Software that are used to manage, operate and provision the PaaS Infrastructure.

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

"Public Cloud" means the cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

"Public Services and Procurement Canada" or "Public Works and Government Services Canada" means the Department of Public Works and Government Services as established under the Department of Public Works and Government Services Act.

"Overdue" means the time when an amount is unpaid on the first day following the day on which it is due and payable according to the Contract.

"Personal Information" means information that is about an identifiable individual and recorded in any form, as defined in section 3 of the Privacy Act. Examples include, but is not limited to the information relating to race, nationality, ethnic origin, religion, age, marital status, address, education as well as the medical, criminal, financial or employment histories of an individual. Personal information also includes any identifying number or symbol, such as the social insurance number, assigned to an individual. Definition from Government of Canada Justice Laws Website : https://laws-lois.justice.gc.ca/eng/acts/P-21/section-3.html

"Processor" means a natural or legal person, public authority, agency or other body that processes Personal Information on behalf of, and in accordance with the instructions of, Canada.

"Product Manufacturer" means the entity which assembles the component parts to manufacture a Product.

"Public Cloud" means the cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

"Public Cloud Services" means a shared pool of configurable Cloud Computing service models made available to users as a rapid, on demand, elastic self service via the Internet from a Cloud Service Provider's servers as opposed to being provided from a company's own on-premises servers, but does not include managed services, training, private or on-premise cloud services, or professional or consulting services that exceed standard public commercially available support services.

"Record" means any hard copy document or any data in a machine-readable format containing Personal Information or Canada data

"Security Event Log" means any event, notification or alert that a device, systems or software is technically capable of producing in relation to its status, functions and activities. Security Events Logs are not limited to security devices, but are applicable to all devices, systems and software that are technically capable of producing event logs that can be used in security investigations, auditing and monitoring. Examples of Systems that can produce security event logs are, but not limited to: firewalls, intrusion prevention systems, routers, switches, content filtering, network traffic flow logs, network, authentication services, directory services, DHCP, DNS, hardware platforms, virtualization platforms, servers, operating systems, web servers, databases, applications, application/layer 7 firewalls.

"Security Incident" means any observable or measurable anomaly occurring with respect to an Asset, which results, or which may result, in:

(A) a violation of the Canada's Security Policies, a Specific Security Measure, the Contractor's or Sub-contractor's security policies or procedures, or any requirement of these Security Obligations or the Privacy Obligations; or

(B) the unauthorized access to, modification of, or exfiltration of any Authorized Personnel's credentials, Users' credentials, or Information Asset.

"Service Level Agreement (SLA)" means an agreement between the Contractor and Canada that defines the level of service expected from the Contractor.

"Service Location(s)" means any facility, site or other physical location owned, leased, provisioned or otherwise occupied by the Contractor or any Contractor Sub-processor from which the Contractor or any Contractor Sub-processor provides any Public Cloud Services.

"Services" means

i) granting usage rights to the software application(s) ("Solutions")
ii) providing Solution Documentation;
iii) maintaining, upgrading, and updating the Solution(s);
iv) managing incidents and defects to ensure the Solution(s) operate at the applicable service levels; and,
v) providing incidental and additionally required information technology infrastructure services required to deliver the Solution.

"Software as a Service" or "SaaS" means the service model through which the capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. [NIST]

"SaaS Publisher" ("SaaSP")" means the entity that owns, operates, maintains and distributes SaaS Solutions.

"Solution Availability" means the percentage of minutes in a month that the Solution is operational.

"Solution Documentation" means all of the manuals, handbooks, user guides and other human-readable material to be provided by the Contractor to Canada under the Contract for use with the Solution.

"SaaS Solution or "Solution" means the software application delivered through a SaaS distribution model in which an Application Service Provider or Cloud Service Provider makes centrally hosted software applications available to customers over the Internet, providing access to and use of a fully maintained, automatically upgraded, up-to-date Solution, technical support services, as well as physically and electronically secure information technology infrastructure, all included in the subscription service.

"Specifications" means the description of the essential, functional or technical requirements of the Services in Annex F - Service Level Agreement, including the procedures for determining whether the requirements have been met.

"Bid" means the documents that the Contractor submits in response to the Request for Proposal (RFP).

"Sub-processor" means any natural or legal person, public authority, agency or other body which processes personal information on behalf of a data controller.

"Usage rights" means granting access to and use of a Solution, also sometimes known as a subscription license.

"User" means any individual, or system process acting on behalf of an individual, authorized by the Canada to access the Services.

"Value-Added Reseller" or "VAR" means a Contractor who is an affiliate, partner, value-added reseller or other channel distributor of SaaS. VAR does not include a Software Publisher, an SaaSP, or a CSP who is also an SaaSP.

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

"Workplace Technology Devices" means desktops, mobile workstations such as laptops and tablets, smartphones, phones, and peripherals and accessories such as monitors, keyboards, computer mouse, audio devices and external and internal storage devices such as USB flash drives, memory cards, external hard drives and writable CD or DVD.

ANNEX "A" - STATEMENT OF REQUIREMENTS

(*insert if applicable*)

ANNEX "B" - BASIS OF PAYMENT

Table 1 : Initial Requirements				
Column (A)	**Column (B)**	**Column (C)**	**Column (D)**	**Column (E)**
Item No.	**Description**	**Firm Unit Price**	**No. of Users for Evaluation Purposes**	**Extended Price for Evaluation Purposes**
1	User Acces to SaaS	$	3000	1(C) * 1(D)
2	Implementation: including configuration, legacy data migration, and rollout.	$	Flat Rate	2(C)
		Firm Price		
3	Training for initial 20 users	$		3(C)
			Extended Price for Evaluation Purposes	Sum of 1(E) to 3(E)

TABLE 2: Optional Additional Users Access				
Column (A)	Column (B)	Column (C)	Column (D)	Column (E)
Item No.	**Description**	**FIRM USER PRICE**	**No. OF USERS FOR EVALUATION PURPOSES**	**EXTENDED PRICE FOR EVALUATION PURPOSES**
1. Optional Additional Software Users				
1.0	Additional Users Access for Initial Contract Period	$	500	1.0(C) * 1.0(D)
1.1	Additional Users for Option Year 1	$	500	1.1(C) * 1.1(D)
1.2	Additional Users for Option Year 2	$	500	1.2(C) * 1.2(D)
1.3	Additional Users for Option Year 3	$	500	1.3(C) * 1.3(D)
1.4	Additional Users for Option Year 4	$	500	1.4(C) * 1.4(D)
1.5	Additional Users for Option Year 5	$	500	1.5(C) * 1.5(D)
1.6	Additional Users for Option Year 6	$	500	1.6(C) * 1.6(D)
1.7	Additional Users for Option Year 7	$	500	1.7(C) * 1.7(D)
1.8	Additional Users for Option Year 8	$	500	1.8(C) * 1.8(D)
1.9	Additional Users for Option Year 9	$	500	1.9(C) * 1.9(D)
			EXTENDED PRICE FOR EVALUATION PURPOSES	**Sum of 1.0(E) to 1.9(E)**

TABLE 3 Training on an "As and When Requested" Basis				
Column (A)	Column (B)	Column (C)	Column (D)	Column (E)
Item No.	**Description**	**FIRM PER DIEM RATE**	**No. OF DAYS FOR EVALUATION PURPOSES**	**EXTENDED PRICE FOR EVALUATION PURPOSES**
1.Basic (End User)				
1.0	Rate for the Initial Contract Period	$	10	1.0(C) * 1.0(D)
1.1	Rate for Option Year 1	$	10	1.1(C) * 1.1(D)
1.2	Rate for Option Year 2	$	10	1.2(C) * 1.2(D)
1.3	Rate for Option Year 3	$	10	1.3(C) * 1.3(D)
1.4	Rate for Option Year 4	$	10	1.4(C) * 1.4(D)
1.5	Rate for Option Year 5	$	10	1.5(C) * 1.5(D)
1.6	Rate for Option Year 6	$	10	1.6(C) * 1.6(D)
1.7	Rate for Option Year 7	$	10	1.7(C) * 1.7(D)
1.8	Rate for Option Year 8	$	10	1.8(C) * 1.8(D)
1.9	Rate for Option Year 9	$	10	1.9(C) * 1.9(D)
2. Train the Trainer				
2.0	Rate for the Initial Contract Period	$	10	2.0(C) * 2.0(D)
2.1	Rate for Option Year 1	$	10	2.1(C) * 2.1(D)
2.2	Rate for Option Year 2	$	10	2.2(C) * 2.2(D)
2.3	Rate for Option Year 3	$	10	2.3(C) * 2.3(D)
2.4	Rate for Option Year 4	$	10	2.4(C) * 2.4(D)
2.5	Rate for Option Year 5	$	10	2.5(C) * 2.5(D)
2.6	Rate for Option Year 6	$	10	2.6(C) * 2.6(D)
2.7	Rate for Option Year 7	$	10	2.7(C) * 2.7(D)
2.8	Rate for Option Year 8	$	10	2.8(C) * 2.8(D)
2.9	Rate for Option Year 9	$	10	2.9(C) * 2.9(D)
			Total Price for Evaluated Purposes	**Sum Of 1.0(E) to 1.9(E) + 2.0(E) to 2.9(E)**

TABLE 4 Professional Services on an "As and When Requested" Basis				
Column (A)	Column (B)	Column (C)	Column (D)	Column (E)
Item No.	**Description**	**FIRM PER DIEM RATE (per Day)**	**No. OF DAYS FOR EVALUATION PURPOSES**	**EXTENDED PRICE FOR EVALUATION PURPOSES**
1.0	Rate for the Initial Contract Period	$	10	1.0(C) * 1.0(D)
1.1	Rate for Option Year 1	$	10	1.1(C) * 1.1(D)
1.2	Rate for Option Year 2	$	10	1.2(C) * 1.2(D)
1.3	Rate for Option Year 3	$	10	1.3(C) * 1.3(D)
1.4	Rate for Option Year 4	$	10	1.4(C) * 1.4(D)
1.5	Rate for Option Year 5	$	10	1.5(C) * 1.5(D)
1.6	Rate for Option Year 6	$	10	1.6(C) * 1.6(D)
1.7	Rate for Option Year 7	$	10	1.7(C) * 1.7(D)
1.8	Rate for Option Year 8	$	10	1.8(C) * 1.8(D)
1.9	Rate for Option Year 9	$	10	1.9(C) * 1.9(D)
			Total Price for Evaluated Purposes	**Sum Of 1.0(E) to 1.9(E)**

Table 5: Total Assessed Price for Calculation			
Column (A)	**Column (B)**	**Column (C)**	**Column (D)**
Item No.	**Description**	**Price Calculations**	**Extended Price**
1	Initial Requirements	Total from Table 1	$
2	Optional Additional User Acess	Total from Table 2	$
3	Training on an "As and When Requested" Basis	Total from Table 3	$
4	Services on an "As and When Requested" Basis	Total from Table 4	$
		Total Assessed Price (TAP) for Evaluation Purposes	$

ANNEX "C" - SECURITY REQUIREMENTS CHECK LIST

(*insert if applicable*)

ANNEX "D" SRCL Security Classification Guide

#	Role/Function	Expected Type of Data Accessed	Data Access Location (Canada / Foreign / Both)	Screening Required	Details
1.	Any Contractor personnel with physical access to the Contractor data centers	• Physical hardware • Data Center facilities • Data as stored on the Contractor's local Backup Media	Canada	Reliability	This is for any Contractor personnel including facilities management resources that have physical access to the Cloud Services hardware equipment at the Contractor data centers.
2.	Any Contractor personnel who have limited logical access to the Contractor services.	• All Business Data • Data as stored on the Contractor's compute, storage, and network components • Security Data including audit logs for Contractor Infrastructure components	Both	Reliability	This is for any Contractor personnel that has logical access to the GC data hosted in the Contractor data centers and any sensitive system and security incident data. This can include Level 1 – Service Desk type resources.
3.	Any Contractor personnel with privileged roles and unrestricted logical access to GC assets within the Contractor services	• All Business Data • GC Data as stored on the Contractor's compute, storage, and network components • Security Data including audit logs for Contractor Infrastructure components • Assets include GC data and credentials	Both	Secret	This is for any Contractor personnel that has elevated privileges with unrestricted logical access to the GC assets hosted in the Contractor data centers, any sensitive system and security incident data. This includes authorized access through an established process such as legal requests.

#	Role/Function	Expected Type of Data Accessed	Data Access Location (Canada / Foreign / Both)	Screening Required	Details
4.	Any contractor personnel with physical or logical access to detailed design documents.	• Detailed design documents including but not limited to detailed logical and physical application, technology infrastructure solution architectures, security architecture and controls, detailed component diagrams, source code, detailed use-cases and business process maps, detailed application, data flows and data models, database designs, system interfaces, internal controls, test plans and test results	Both	Reliability	This is mainly architecture and detailed design documentation access.
5.	Contractor Security Operations Center Personnel	• Data as stored on the Contractor's compute, storage, and network components • Security Data including audit logs for Contractor Infrastructure components	Both	Reliability	This is the Contractor SOC Personnel.

#	Role/Function	Expected Type of Data Accessed	Data Access Location (Canada / Foreign / Both)	Screening Required	Details
6.	4th Level OEM Support	• Physical hardware • Data Center facilities • Data as stored on the Contractor's local Backup Media	Canada	N/A	The Contractor will use sub-contractors for some of their services as it related to data center operations. Any subcontractor should be properly engaged by the Contractor by having a contract and clear definition of work. This resource type will not have direct physical access to GC Data however they can work on issues/problems specific to their expertise level with security cleared Contractor resources who has access to the data. If the 4th Level OEM Support resource is at Contractor Data Centers, they will be escorted by cleared Contractor Operators. For example: Networking equipment support, HVAC support.

In addition to the roles above, the following covers roles related to transition/migration related services:

Track	Role	Responsibilities	Access to	Location (other than meetings)	Personnel Clearance Requirements (working assumption)
Governance	Delivery Executive, Program Manager or Project Manager	Governance / project management of the engagement	No access to physical systems (hands on keyboards) May attend meetings where protected system configuration data is displayed and/or discussed No access to user data	Onsite - N/A Remote - Yes	Reliability or equivalent
IT Service Management (Operational Guidance)	Architect and Consultant	Leading workshops, creation of documents (service maps, monitoring, etc.)	No access to physical systems (hands on keyboards) May attend meetings where protected system configuration data is displayed and/or discussed No access to user data	Onsite - N/A Remote - Yes	Reliability or equivalent
End User Adoption & Change Management	Architect and Consultant	Leading workshops, creation of documents, other change management activities required to onboard Office 365	No access to physical systems (hands on keyboards) May attend meetings where protected system configuration data is displayed and/or discussed No access to user data	Onsite - N/A Remote - Yes	None (assumes escorted when on Partner premises)
Microsoft Exchange Online Onboarding	Architect	Technical oversight of engagement, general guidance, document and deliverables review	No access to physical systems (hands on keyboards) Potential access to GoC documentation of various classifications No access to user data	Onsite - N/A Remote - Yes	Reliability or equivalent

	Deployment Consultant	**Remediation Phase** - Working side-by-side with SSC/GoC SME's to remediate any issues with on-premises Active Directory, lingering Exchange configuration on-premises, network and client readiness (desktop) **Enable Phase** - Working side-by-side with SSC/GoC SME's to deploy the various components (AAD Connect for synchronization, establishing Federation for authentication, Enabling Conditional Access, Azure Information Protection and Exchange Online configuration in the tenant)	Access to Systems (Office 365 tenant, on-premises Active Directory and Exchange) Access to GoC documentation as required to assist in the remediation and enablement Potential access to user data	Onsite - (if required by SSC) Remote - Yes	Reliability or equivalent (assumes SSC managing the environments independent of Partner email being migrated)
	Migration Consultant	Migration of data from YES to Exchange Online including creating the migration projects. Post-migration support to assist SSC/Partner Service Desks	Access to Systems (Office 365 tenant as Global Admin, on-premises Active Directory and Exchange, YES as either Organization Management or Recipient Management) Access/Potential Access to data (Full mailbox access in both YES and Exchange Online) Access to GoC documentation as required to complete migrations	Onsite - (if required by SSC) Remote - Yes	Secret or equivalent

ANNEX "E" – Supply Chain Integrity Process

Supply Chain Integrity Process

1. Mandatory Requirements

1.1. Contractors must submit, with their Submission, the following SCSI:

1.2.1 IT Product List: Contractors must identify the SaaS Solutions over which Canada's Data would be transmitted and/or stored that will be used and/or installed to perform any part of the Work and/or Services described in the resulting contract, in regards to each SaaS Solution, by completing the Form 6-SCI Submission Template as provided in the RFP, which includes following information:

a) **OEM Name**: Enter the name of the original equipment manufacturer (OEM) of the product that is being ordered.

b) **OEM DUNS Number:** Enter the DUNS number of the OEM. The Data Universal Numbering System (DUNS) is a unique nine-digit number assigned to each physical location of a businesses. It is a worldwide standard and is used to determine the credit score of a company. If the company does not have a DUNS number, or you are unable to find one, please fill out the requested information on "C - Ownership Information". Ownership information consists of the top 5, by percentage, investors and owners of the company. The names provided for investors and owners should be those found in investment or ownership documents for the company in question.

c) **Product Name:** Enter the OEM's name for the product.

d) **Model Number:** Enter the OEM's model and/or version number of the product.

e) **Product URL:** Enter the URL of the OEM's webpage for the product.

f) **Vulnerability Information:** Enter information concerning the last 5 security issues that were reported about the product. If the OEM posts this information to the CVE website, list the CVE numbers separated by semi-colons (;). If the OEM does not post this information to the CVE website, you will need to ask the OEM directly for security vulnerability information and provide this information to the Canadian Centre for Cyber Security. If this is the case for a particular product, enter "see attached information" in the Vulnerability Information field, and include the filename(s) in the additional information column which provide the required vulnerability information.

1.2.2 Ownership Information: Contractors must identify the original equipment manufacturer (OEM) of the product(s) or service(s) ordered, as well as the name of any contractor (i.e. sub-contractors (individuals or companies), sub-contractors of sub-contractors (individuals or companies) down the chain, re-seller, distributor, sub-processors, etc.) of the product(s) or service(s) that are being ordered.

This list must identify all third parties who may perform any part of the Work, whether they would be sub-contractors to the Contractor, or sub-contractors to sub-contractors of the Contractor down the chain. Any sub-contractor that could have access to Canada's Data must be identified. For the purposes of this requirement, a third party who is merely a contractor of goods to the Contractor, but who does not perform any portion of the Work, is not considered to be a sub-contractor. Sub-contractors would include, for example, technicians who might be deployed or maintain the Contractor's solution. If the Contractor does not plan to use any sub-contractors to perform any part of the Work, the Contractor is requested to indicate this in its response.

Contractors are requested to provide their information on form [insert]. It is requested that Contractors indicate their legal name on each page, insert a page number as well as the total number of pages. Contractors are also requested to insert a separate row for each sub-contractor and additional rows as may be necessary.

For each of these entities listed, provide either:

a) **OEM DUNS Number**: Enter the DUNS number of the OEM. The Data Universal Numbering System (DUNS) is a unique nine-digit number assigned to each physical location of a businesses. It is a worldwide standard and is used to determine the credit score of a company. If the company does not have a DUNS number, or you are unable to find one, fill out the requested information on "C - Ownership Information". Ownership information consists of the top 5, by percentage, investors and owners of the company. The names provided for investors and owners should be those found in investment or ownership documents for the company in question.

b) **Country / Nationality**: The country which an individual listed has their primary nationality or the country in which a corporate entity is registered.

c) **Corporate website link**: For each of OEM or Contractor name, Ownership, Investors, and Executives listed above provide a URI / URL to the information that supports the claims listed in each of the fields.

1.2.3 Network Diagrams: one or more conceptual network diagrams that collectively show the complete network proposed to be used to deliver the services described in the draft Statement of Work. The network diagrams are only required to include portions of the Contractor's network (and its sub-contractor network(s)) over which Canada's Data, would be transmitted in performing any resulting contract. As a minimum the diagram must show:

a) The following key nodes for the delivery of the services under the resulting contract of this solicitation process, if applicable the role of the Contractor or sub-contractor;

i. Service delivery points;

ii. Core network

iii. Sub-contractor network (specifying the name of the sub-contractor as listed in the **Ownership Information**);

b) The node interconnections, if applicable

c) Any node connections with the Internet; and

d) For each node, a cross-reference to the product that will be deployed within that node, using the Excel row number from the IT Product List.

2. Assessment of Supply Chain Security Information

2.1 Canada will assess whether, in its opinion, the Supply Chain Security Information creates the possibility that the Contractor's solution could compromise or be used to compromise the security of Canada's equipment, firmware, software, systems or information.

2.2 In conducting its assessment:

(a) Canada may request from the Contractor any additional information that Canada requires to conduct a complete security assessment of the Supply Chain Security Information. The Contractor will have 2 working days (or a longer period if specified in writing by the Supply Chain Security Authority) to provide the necessary information to Canada. Failure to meet this deadline will result in the response being disqualified.

(b) Canada may use any government resources or consultants to conduct the assessment and may contact third parties to obtain further information. Canada may use any information, whether it is included in the response or comes from another source, that Canada considers advisable to conduct a comprehensive assessment of the Supply Chain Security Information.

2.3 If, in Canada's opinion, any aspect of the Supply Chain Security Information, if used in a solution, creates the possibility that the Contractor's solution could compromise or be used to compromise the security of Canada's equipment, firmware, software, systems or information:

(a) Canada will notify the Contractor in writing (sent by email) and identify which aspect(s) of the Supply Chain Security Information is subject to concern(s) or cannot be assessed (for example, proposed future releases of products cannot be assessed). Any further information that Canada might be able to provide to the Contractor regarding its concerns will be determined based on the nature of the concerns. In some situations, for reasons of national security, it may not be possible for Canada to provide further information to the Contractor; therefore, in some circumstances, the Contractor will not know the underlying reasons for Canada's concerns with respect to a product, sub-contractor or other aspect of the Contractor's Supply Chain Security Information.

(b) The notice will provide the Contractor with one opportunity to submit revised Supply Chain Security Information within the 10 calendar days following the day on which Canada's written notification is sent to the Contractor, (or a longer period specified in writing by the Supply Chain Security Authority).

(c) If the Contractor submits revised Supply Chain Security Information within the allotted time, Canada will perform a second assessment. If Canada determines that any aspect of the Contractor's revised Supply Chain Security Information could compromise or be used to compromise the security of Canada's equipment, firmware, software, systems or information, no further opportunities to revise the Supply Chain Security Information will be provided and the response will be disqualified.

2.4 By participating in this process, the Contractor acknowledges that the nature of information technology is such that new vulnerabilities, including security vulnerabilities, are constantly being identified. Also, the Contractor acknowledges that Canada's security assessment does not involve the assessment of a proposed solution. As a result:

(a) qualification pursuant to this RFP does not constitute an approval that the products or other information included as part of the Supply Chain Security Information will meet the requirements of the subsequent bid solicitation or any resulting contract or other instrument that may be awarded as a result of any subsequent bid solicitation;

(b) qualification pursuant to this RFP does not mean that the same or similar Supply Chain Security Information will be assessed in the same way for future requirements;

(c) at any time during the subsequent bid solicitation process, Canada may advise a Contractor that some aspect(s) of its Supply Chain Security Information has become the subject of security concerns. At that point, Canada will notify the Respondent and provide the Contractor with an opportunity to revise its Supply Chain Security Information, using the same process described above.

(d) during the performance of a subsequent contract, if Canada has concerns regarding certain products, designs or sub-contractors originally included in the Supply Chain Security Information, the terms and conditions of that contract will govern the process for addressing those concerns.

2.5 All Contractors will be notified in writing regarding whether or not they have qualified under this RFP to proceed to the next stage of the procurement process.

2.6 Any Contractor that has qualified under this RFP will be required, when responding to any subsequent bid solicitation under this solicitation process, to propose a solution consistent with the final version of the Supply Chain Security Information it submitted with its response to this RFP (subject to revision only pursuant to the paragraph below). Except pursuant to the paragraph below, no alternative or additional Products or sub-contractors may be proposed in the Contractor's solution. This is a mandatory requirement of this solicitation process. The proposed solution during any subsequent bid solicitation does not need to contain all the Products within the final Supply Chain Security Information.

2.7 Once a Contractor has been qualified in response to this RFP, no modifications are permitted to the Supply Chain Security Information except under exceptional circumstances, as determined by Canada. Given that not all the exceptional circumstances can be foreseen, whether changes may be made and the process governing those changes will be determined by Canada on a case-by-case basis.

ANNEX "F" – Supply Chain Security Information (SCSI) Vendor Submission Form

PART A - BIDDER INFORMATION	
Procurement Name:	
Date submitted:	
Solicitation Number:	
Bidder Name:	
Bidder DUNS Number:	

Government of Canada / Gouvernement du Canada

PROTECTE
D B
When filled

B -Product List

Example IT
Product List

Item	OEM Name	OEM DUNS Number	Product Name	Model / Version	Product URL	Vulnerability Information	Contractor Name	Contractor DUNS Number	Contractor URL	Additional Information
1										
2										
3										
4										
5										
6										
7										
8										
9										
10										
11										
12										
13										
14										
15										
16										
17										
18										
19										

Government of Canada / Gouvernement du Canada

TLP AMBER
When Filled

C - Ownership Information

F - Example Ownership Information

Use this form only for OEM and Contractors that do not have a DUNS number.

Item	OEM or Contractor name	Ownership	Investors	Executives	Country / Nationality	Corporate website link
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						
17						

D - Help

Field	Guide	Notes
SCSI Form 2 Cover		
PROCUREMENT NAME	If not applicable, leave blank. Otherwise, provide any name associated with this multi-line procurement (i.e. WTD Print, Project Telesto).	
Date submitted:	YYYY-MM-DD	
SOLICITATION #:	If not applicable, leave blank. Otherwise, provide the solicitation number for this multi-line procurement.	
BIDDER NAME	If not applicable, leave blank. Enter the name of the lead organization providing the bid submission.	
BIDDER DUNS Number	If not applicable, leave blank. Enter the DUNS number of the lead organization providing the bid submission. If the company does not have a DUNS number, or you are unable to find one, please fill out the requested information on "C - Ownership Information". Ownership information consists of the top 5, by percentage, investors and owners of the company. The names provided for investors and owners should be those found in investment or ownership documents for the company in question.	
IT PRODUCT LIST		
OEM Name	Enter the name of the original equipment manufacturer (OEM) of the product that is being ordered.	**Only products that qualify for supply chain integrity assessments should be included in this list. Power cables, rack blanking panels, warranty**

OEM DUNS Number	Enter the DUNS number of the OEM. The Data Universal Numbering System (DUNS) is a unique nine-digit number assigned to each physical location of a business. It is a worldwide standard and is used to determine the credit score of a company. If the company does not have a DUNS number, or you are unable to find one, please fill out the requested information on "C - Ownership Information". Ownership information consists of the top 5, by percentage, investors and owners of the company. The names provided for investors and owners should be those found in investment or ownership documents for the company in question.	**costs, shipping costs, and similar other non-ICT items should not be included. If these products are found in this form, it will be sent back as incorrect and no assessment will be performed.** **This should follow the "Product" definition of "hardware (or software) that operates at the data link layer of the Open Systems Interconnection model (OSI Model) Layer 2 and above"**
Product Name	Enter the OEM's name for the product.	
Model Number	Enter the OEM's model and/or version number of the product.	
Product URL	Enter the URL of the OEM's webpage for the product.	
Vulnerability Information	Enter information concerning the last 5 security issues that were reported about the product. If the OEM posts this information to the CVE website, list the CVE numbers **separated by semi-colons (;)**. If the OEM does not post this information to the CVE website, you will need to ask the OEM directly for security vulnerability information and provide this information to the Canadian Centre for Cyber Security. If this is the case for a particular product, enter "see attached information" in the relevant field(s).	
Contractor Name	Enter the name of the contractor (i.e. sub-contractors, re-seller, distributor, sub-processors, etc.) of the product that is being ordered. This includes any business entity involved in producing products or services to help complete the bidding requirements. **For PISA, NMSO, or similar lists, this field may be left blank.**	

Contractor DUNS Number	Enter the DUNS number of the Contractor. The Data Universal Numbering System (DUNS) is a unique nine-digit number assigned to each physical location of a businesses. It is a worldwide standard and is used to determine the credit score of a company. If the company does not have a DUNS number, or you are unable to find one, please fill out the requested information on "C - Ownership Information". Ownership information consists of the top 5, by percentage, investors and owners of the company. The names provided for investors and owners should be those found in investment or ownership documents for the company in question. **For PISA, NMSO, or similar lists, this field may be left blank.**	
Contractor URL	Enter the URL of the contractor's webpage for the product. **For PISA, NMSO, or similar lists, this field may be left blank.**	
OWNERSHIP INFORMATION		
OEM or Contractor name	Enter the name of the original equipment manufacturer (OEM) of the product that is being ordered, or enter the name of the contractor (i.e. sub-contractors, re-seller, distributor, sub-processors, etc.) of the product or service that is being ordered.	**It is only necessary to fill out entries in "C- Ownership Information" if a DUNS number cannot be supplied for the OEM and/or contractor.** **Each piece of provided information must be found on its own line in its own cell in the spreadsheet.**
Ownership	Ownership information consists of the top 5, by percentage, owners of the OEM or Contractor. The names provided for owners should be those found in ownership documents for the company in question.	
Investors	Investor information consists of the top 5, by percentage, investor in the OEM or Contractor. The names provided for owners should be those found in investment documents for the company in question.	
Executives	List the executives and members of the board of directors for the company in question.	
Country / Nationality	The country which an individual listed has their primary nationality or the country in which a corporate entity is registered.	

Corporate website link	For each of OEM or Contractor name, Ownership, Investors, and Executives listed above provide a URI / URL to the information that supports the claims listed in each of the fields.	

E - Example IT Product List

Item	OEM Name	OEM DUNS Number	Product Name	Model / Version	Product URL	Vulnerability Information	Contractor Name	Contractor DUNS Number	Contractor URL	ADDITIONAL INFORMATION
1	Cie. ABC	137660665	1941	K9	Insert URL here	CVE-2018-XXXXX; CVE-2018-YYYYY; CVE-2018-XXXXX; CVE-2017-WWWWW				PISA Example
2	Cie. ABC	137660665	1941	K9	Insert URL here	CVE-2018-XXXXX; CVE-2018-YYYYY; CVE-2018-XXXXX; CVE-2017-WWWWW	LocalHardware	4567891234	https://www.lhinc.ca	ROC / Single Procurement Example

F - Example Ownership Information

OEM or Contractor name	Ownership	Investors	Executives	Country / Nationality	Corporate website link
newkid software	Mr. A (60%)			Canada	newkid.com/profiles/mra
newkid software	Ms. B (30 %)			France	newkid.com/profiles/msb
newkid software	Mr. C (10%)			United States	newkid.com/profiles/mrc
newkid software		Company A (10%)		United States	newkid.com/investor_relations/filings
newkid software		Company B (9%)		China	newkid.com/investor_relations/filings
newkid software		Company C (8%)		South Korea	newkid.com/investor_relations/filings
newkid software		Company D (5%)		Canada	newkid.com/investor_relations/filings
newkid software		Company E (5%)		Spain	newkid.com/investor_relations/filings
newkid software			Mr. A	Canada	newkid.com/profiles/mra
newkid software			Ms. B	France	newkid.com/profiles/msb
newkid software			Mr. Q	Portugal	newkid.com/profiles/mrq

ANNEX "G" – PSPC Non-Disclosure Agreement related to Supply Chain Integrity

Note to Contractors: Please note that this Non-Disclosure Agreement only covers SCI requirements under Section 3.6: Supply Chain Integrity Requirements. Contractors will be asked to enter into a bi lateral non-disclosure agreement (NDA) with the CCCS once they onboard on the SaaS ITS Program.

Non-Disclosure Agreement

By presenting a Submission, the Contractor agrees to the terms of the non-disclosure agreement below (the "**Non-Disclosure Agreement**"):

1. The Contractor agrees to keep confidential any information it receives from Canada regarding Canada's assessment of the Contractor's Supply Chain Security Information (the "**Sensitive Information**") including, but not limited to, which aspect of the Supply Chain Security Information is subject to concern, and the reasons for Canada's concerns.

2. Sensitive Information includes, but is not limited to, any documents, instructions, guidelines, data, material, advice or any other information whether received orally, in printed form or otherwise and whether or not that information is labeled as classified, proprietary or sensitive.

3. The Contractor agrees that it will not reproduce, copy, divulge, release or disclose, in whole or in part, in whatever way or form any Sensitive Information to any person other than a person employed by the Contractor who has a security clearance commensurate with the level of Sensitive Information being accessed, without the prior written consent of the Supply Chain Security Authority. The Contractor agrees to immediately notify the Supply Chain Security Authority if any person, other than those permitted by this Article, accesses the Sensitive Information at any time.

4. All Sensitive Information will remain the property of Canada and must be returned to the Supply Chain Security Authority or destroyed, at the option of the Supply Chain Security Authority, if requested by the Supply Chain Security Authority, within 30 days following that request.

5. The Contractor agrees that a breach of this Non-Disclosure Agreement may result in disqualification of the Contractor at SA stage, or immediate termination of any resulting Contract(s). The Contractor also acknowledges that a breach of this Non-Disclosure Agreement may result in a review of the Contractor's security clearance and review of the Contractor's status as an eligible Contractor for other requirements.

6. This Non-Disclosure Agreement remains in force indefinitely.

ANNEX "H" – SaaS IT Security (ITS) Assessment Program: Onboarding Process

1. Making a Submission to the SaaS IT Security Assessment Program

(a) To make a submission to the program, a Bidder must complete the following steps:

(b) Contact the CCCS Contact Centre: contact@cyber.gc.ca or 613-949-7048 or 1-833-CYBER-88.

(c) Prepare to enter into a bi lateral non-disclosure agreement (NDA) with the CCCS.

(d) Provide all documentation for the assessment to the CCCS Contact Centre. When providing documents, Pretty Good Privacy (PGP) encryption program credentials should be used to encrypt the documents. See section 2 – PGP Key for a copy of the PGP key.

2. PGP Key

(a) Email or phone the CCCS Contact Centre to request the necessary public key for the CCCS PGP key. Use this key to encrypt sensitive documents that you are submitting for the SaaS ITS Assessment Program.

3. Contacts and Assistance

(a) The CCCS Contact Centre is the point of contact for all document submissions related to the SaaS ITS Assessment Program. The SaaS Assessment team lead, or an authorized delegate, has access to this mailbox. All SaaS ITS Assessment documentation will be managed and protected using PGP encryption during transmission (see section 2 for a copy of the PGP key). All documentation will also be handled and managed following CCCS information management policies.

CCCS Contact Centre
contact@cyber.gc.ca
613-949-7048 or 1-833-CYBER-88

ANNEX "I" – SaaS Service Level Agreements (SLA)

Only terms and conditions in the SLA, detailed under 3.3 Section I: Technical Submission (d), related to service levels and service delivery will be part of the Contract.

By presenting a Bid, the Bidder acknowledges and agrees that any terms contained in Annex G - SaaS Solution Service Level Agreements that purport to interpret the Contract, are the same or similar subject matter, or are related to the terms contained in the Contract Clauses, are deemed stricken and are of no force or effect. Similarly, any terms contained in Annex G – SaaS Solution Service Level Agreements which include pricing information, such as (but not limited to) those that attempt to impose financial conditions, pricing terms, or compliance penalties, shall be deemed stricken and are of no force or effect.

No terms purporting to abridge or extend the time to commence an action for breach, tort, or other action are of any effect.

ANNEX "J" to PART 5 OF THE BID SOLICITATION

FEDERAL CONTRACTORS PROGRAM FOR EMPLOYMENT EQUITY – CERTIFICATION

(insert if applicable)

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

For further information on the Federal Contractors Program for Employment Equity visit Employment and Social Development Canada (ESDC) – Labour's website.

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

Complete both A and B.

A. Check only one of the following:

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

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

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

( ) A4. The Bidder certifies having a combined work force in Canada of less than 100 permanent full-time and/or permanent part-time employees.

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

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

OR

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

B. Check only one of the following:

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

OR

( ) B2. The Bidder is a Joint venture and each member of the Joint Venture must provide the Contracting Authority with a completed Annex G Federal Contractors Program for Employment Equity - Certification. (Refer to the Joint Venture section of the Standard Instructions)

ANNEX "K" TASK AUTHORIZATION FORM PWGSC-TPSGC 572

TASK AUTHORIZATION FORM FOR
EMAS CONTRACT
AUTHORIZATION OF SERVICES TO BE PERFORMED
ON AN AS-AND-WHEN-REQUESTED BASIS

Contractor:	Contract No.
Financial Code:	GST Financial Code:
Task Authorization No.:	Date:
1.0 DESCRIPTION OF THE TASK / WORK TO BE PERFORMED	
2.0 PERIOD OF SERVICES	
From:	To:
3.0 SERVICES TO BE PERFORMED FOR: (LOCATION / ADDRESS)	
4.0 AUTHORITIES	
Project Authority: _____	**Responsibility Centre:** _____

5.0 COST

Category and Level of Personnel / Category of Course	**Per Diem Rate / Rate per Course**	**No. of Days to Perform the Tasks/Work**	**Total**
	$		$
	$		$
	$		$
	$		$
	$		$
		ESTIMATED PRICE	$
		GST/HST	$
		TOTAL	$
Travel and Living Expenses: Travel and living are a direct charge on a cost reimbursable basis. All expenses shall incurred in accordance with the then-current Treasury Board guidelines. Invoices for Travel and Living costs of the Contractor's employees are to be supported by documentation (receipts) and will be reimbursed in accordance with the Treasury Board Policy and Guidelines on Travel in effect at the time of travel at actual cost with on allowance for mark-up. Charges for air travel shall not exceed that for economy class.		**ESTIMATED PRICE**	$
		GST/HST	$0
		TOTAL	$0
		GRAND TOTAL	$

You are requested to sell to Her Majesty The Queen in right of Canada, in accordance with the terms and conditions set out herein, referred to herein or attached hereto, the services listed herein and on any attached sheets at the price set out therefore.

ANNEX "L" SaaS Publisher Authorization Form

(to be used where the Contractor is not the SaaS Publisher)

This confirms that the SaaS Publisher identified below understands and acknowledges that the Contractor named below has submitted a Submission in response to the Request for Supply Arrangement dated _____, reference number _____ issued by PSPC.

The SaaS Publisher hereby confirms that

(i) The Contractor named below is authorized to supply the SaaS Publisher listed below or attached, through its SA; and
(ii) The SaaS Publisher agrees to grant all licenses to be acquired under the SA in accordance with the resulting Contract's terms and conditions set out in the SA.

The SaaS Publisher acknowledges that the reseller has proposed to the Crown, in response to the RFSA, the following SaaS Solutions and other proprietary products of the Corporation.

[*Identify all of the proprietary SaaS Solutions that are proposed by the Contractor*]
_____
_____
_____
_____
[*Contractors should add or remove lines as needed,* or attach the product list as an appendix.]

Name of Contractor _____

Name of SaaS Publisher _____

Signature of authorized signatory of SaaS Publisher_____

Print Name of authorized signatory of SaaS Publisher_____

Print Title of authorized signatory of SaaS Publisher_____

Address for authorized signatory of SaaS Publisher_____

Telephone no. for authorized signatory of SaaS Publisher
_____

Email for authorized signatory of SaaS Publisher _____

Date signed _____