



**RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:**

**Bid Receiving - PWGSC / Réception des
soumissions - TPSGC**

**Place du Portage, Phase III
Core 0B2 / Noyau 0B2
11 Laurier St./11, rue Laurier
Gatineau
Québec
K1A 0S5
Bid Fax: (819) 997-9776**

**REQUEST FOR PROPOSAL
DEMANDE DE PROPOSITION**

**Proposal To: Public Works and Government
Services Canada**

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

**Proposition aux: Travaux Publics et Services
Gouvernementaux Canada**

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

Comments - Commentaires

Title - Sujet Learning Platform	
Solicitation No. - N° de l'invitation 0X001-190594/B	Date 2019-08-28
Client Reference No. - N° de référence du client 0X001-190594	
GETS Reference No. - N° de référence de SEAG PW-\$\$XL-108-36755	
File No. - N° de dossier 108x1.0X001-190594	CCC No./N° CCC - FMS No./N° VME
Solicitation Closes - L'invitation prend fin at - à 02:00 PM on - le 2019-10-24	Time Zone Fuseau horaire Eastern Daylight Saving Time EDT
F.O.B. - F.A.B. Plant-Usine: <input type="checkbox"/> Destination: <input type="checkbox"/> Other-Autre: <input type="checkbox"/>	
Address Enquiries to: - Adresser toutes questions à: Fenwick, Wesley	Buyer Id - Id de l'acheteur 108x1
Telephone No. - N° de téléphone (613) 720-7443 ()	FAX No. - N° de FAX () -
Destination - of Goods, Services, and Construction: Destination - des biens, services et construction: Specified Herein Précisé dans les présentes	

Instructions: See Herein

Instructions: Voir aux présentes

Vendor/Firm Name and Address

**Raison sociale et adresse du
fournisseur/de l'entrepreneur**

Issuing Office - Bureau de distribution

Shared Systems Division (XL)/Division des systèmes
partagés (XL)
Terrasses de la Chaudière
4th Floor, 10 Wellington Street
4th etage, 10, rue Wellington
Gatineau
Québec
K1A 0S5

Delivery Required - Livraison exigée See Herein	Delivery Offered - Livraison proposée
Vendor/Firm Name and Address Raison sociale et adresse du fournisseur/de l'entrepreneur	
Telephone No. - N° de téléphone Facsimile No. - N° de télécopieur	
Name and title of person authorized to sign on behalf of Vendor/Firm (type or print) Nom et titre de la personne autorisée à signer au nom du fournisseur/ de l'entrepreneur (taper ou écrire en caractères d'imprimerie)	
Signature	Date

BID SOLICITATION
FOR A NEXT-GENERATION DIGITAL LEARNING ENVIRONMENT
SOLUTION
FOR
CANADA SCHOOL OF PUBLIC SERVICE

Table of Content

PART 1 – GENERAL INFORMATION	5
1.1 Introduction	5
1.2 Summary	5
1.3 Overview of the Project	6
1.4 Security Requirements	7
1.5 Debriefings	8
1.6 Conflict of Interest – Unfair Advantage	8
1.7 Bidder’s Conference	8
PART 2 – BIDDER’S INSTRUCTIONS	10
2.1 Standard Instructions, Clauses and Conditions	10
2.2 Submission of Bids	10
2.3 Former Public Servant.....	10
2.4 Enquiries – Bid Solicitation	12
2.5 Applicable Laws.....	12
2.6 Improvement of Requirement during Solicitation Period.....	12
PART 3 – BID PREPARATION INSTRUCTIONS.....	13
3.1 Bid Preparation Instructions	13
3.2 Submission of Multiple Bids	14
3.3 Joint Venture Experience	14
3.4 Section I: Technical Bid	15
3.5 Section II: Financial Bid	16
3.6 Section III: Certifications.....	18
3.7 Section IV: Additional Information	18
PART 4 – EVALUATION AND ASSESSMENT PROCEDURES.....	19
4.1 Evaluation Procedures	19
4.2 Rights of Canada.....	22
4.3 Rejection of Bids.....	23

4.4	Capability and Usability Assessment Procedures	23
PART 5 – CERTIFICATIONS AND ADDITIONAL INFORMATION		25
5.1	Certifications Required with Bid	25
5.2	Certifications Precedent to Contract Award and Additional Information	26
5.3	Integrity Provisions – Required Documentation	26
5.4	Federal Contractors Program for Employment Equity – Bid Certification	26
5.5	Sole Bid – Price Support	26
PART 6 – SECURITY AND FINANCIAL REQUIREMENT		27
6.1	Canadian Suppliers:	27
6.2	Foreign Supplier	27
6.3	Financial Capability	28
PART 7 – RESULTING CONTRACT CLAUSES		30
7.1	Requirement	30
7.2	Contract Term.....	31
7.3	Solution.....	32
7.4	Solution Operational Changes	33
7.5	Solution Maintenance and Support	33
7.6	Contractor Use of Canada’s Data	35
7.7	Services.....	35
7.8	Documentation	36
7.9	Optional Professional and Training Services	37
7.10	Remedies	38
7.11	Subcontracts.....	38
7.12	Excusable Delay.....	38
7.13	Right to Terminate.....	39
7.14	Inspection and Acceptance of the Work.....	39
7.15	Kick-Off Meeting	40
7.16	Progress Review Meeting	40
7.17	Task Authorization.....	40
7.18	Security Requirement.....	41
7.19	Contractor’s Sites or Premises Requiring Safeguarding Measures	50
7.20	Basis of Payment.....	51
7.21	Method of Payment	52
7.22	Invoicing	53
7.23	Taxes.....	54
7.24	Certifications and Additional Information.....	55
7.25	Federal Contractors Program for Employment Equity – Default by Contractor	55

7.26 Insurance Requirements	55
7.27 Limitation of Liability	55
7.28 General Provisions	56
7.29 Authorities.....	57
7.30 Proactive Disclosure of Contracts with Former Public Servants.....	57
7.31 Priority of Documents	58
7.32 Joint Venture Contractor	58
ANNEX A	60
ANNEX B	74
ANNEX C	79
ANNEX D	91
ANNEX E	98
ANNEX F.....	102
ANNEX G	104
ANNEX H	124
ANNEX I	142

List of Annexes to the Resulting Contract:

Annex A STATEMENT OF WORK

Appendix A – Capability and Usability Assessment

Annex B BASIS OF PAYMENT

Annex C SECURITY REQUIREMENT CHECK LIST

Appendix A – Security Classification Guide
Appendix B – Security Obligations
Appendix C – Additional Security Information for Foreign Contractor or Subcontractor

Annex D DEFINITION AND INTERPRETATIONS

Annex E PRIVACY OBLIGATIONS

Annex F TASK AUTHORIZATION FORMS

Annex G BID EVALUATION CRITERIA

Annex H BIDDER FORMS

Form 1 to Annex I – Bid Submission Form
Form 2 to Annex I – CSP Letter of Attestation Form
Form 3 to Annex I – Software Publisher Certification Form
Form 4 to Annex I – Software Publisher Authorization Form
Form 5 to Annex I – Declaration Form
Form 6 to Annex I – List of Names Form
Form 7 to Annex I – Federal Contractors Program for Employment Equity – Certification
Form 8 to Annex I – Electronic Payment Instruments

Solicitation No. - N° de l'invitation
0X001-190594/A
Client Ref. No. - N° de réf. du client
0X001-190594

Amd. No. - N° de la modif.
-
File No. - N° du dossier
108xl0X001-190594

Buyer ID - Id de l'acheteur
108 XL
CCC No./N° CCC - FMS No./N° VME

Form 9 to Annex I - Financial Bid Presentation Sheet

Annex I SECURITY CONTROL PROFILE

BID SOLICITATION

FOR A NEXT-GENERATION DIGITAL LEARNING ENVIRONMENT SOLUTION

FOR

THE CANADA SCHOOL OF PUBLIC SERVICE

PART 1 – GENERAL INFORMATION

1.1 Introduction

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

- Part 1** General Information: provides a general description of the requirement;
- Part 2** Bidder Instructions: provides the instructions, clauses and conditions applicable to the bid solicitation;
- Part 3** Bid Preparation Instructions: provides Bidders with instructions on how to prepare their bid;
- Part 4** Evaluation and Assessment Procedures and Basis of Selection: indicates how the evaluation will be conducted, the evaluation criteria that must be addressed in the bid, the Capability and Usability Assessment to be conducted, 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.

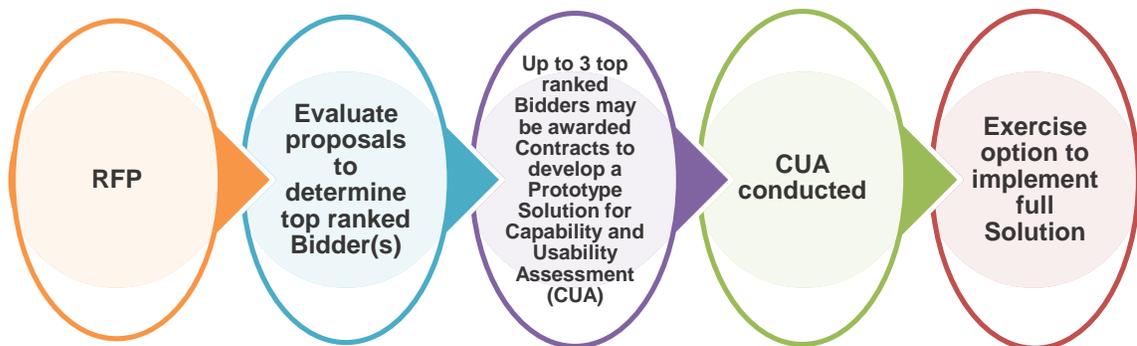
The annexes include the Statement of Work and any other annexes.

1.2 Summary

- (a) This bid solicitation is being issued to satisfy the requirement of the Canada School of Public Service (the "Client") for a Next Generation Digital Learning Environment Solution (the "Solution"). It is intended to result in the award of up to 3 Contracts to successful Bidders to each develop a Capability and Usability Assessment (CUA) Prototype Solution in accordance with Phase 1 of Annex A –Statement of Work and, at Canada's sole discretion, exercise the option on one Contract for the Contractor to deliver the production ready Solution in accordance with Phase 2 of Annex A – Statement of Work. The Contract will include 9 irrevocable options allowing Canada to extend the term of the Contract by one year each. While Canada intends to issue a Contract or Contract(s) of a specific duration, Canada reserves the right to continue to Contract for and leverage this Solution for as long as it makes business sense for Canada to do so. Canada also expects that this type of Solution will evolve with time and technology, including incorporation of functionality or technology that isn't

currently part of the requirement. Canada reserves the right to consider these evolutionary functionality or technology to be part of the ongoing scope of the work being done under the Contract, subject to Canada's internal approval processes. Canada reserves the right to, at a subsequent date and at its sole discretion, identify the solution either as a multi-departmental solution, or designate the solution as a Government of Canada Enterprise-wide standard if and when determined by the GC-Enterprise Architecture Review Board (GCEARB).

- (b) This bid solicitation and the resulting Contract(s) will follow an agile procurement approach in order to encourage more effective collaboration with vendors. Being agile means approaching projects with short phases at a fast pace, while assessing and addressing challenges along the way.
- (c) The anticipated multi-phase agile procurement process will be conducted as per the following phases:



1.3 Overview of the Project

- (a) The Government of Canada is seeking a solution delivered following the Software as a Service (SaaS) model hosted as a Protected B, Medium Integrity, Medium Availability (PBMM) cloud-based solution. The required solution may be comprised of any combination of commercial-off-the-shelf ("COTS") software or Pre-Existing software; the resulting configuration of such software would allow operation of the Solution at all times in accordance with Annex A – Statement of Work in the bid solicitation. The Contractor will configure the Solution such that it:
 - (i) Includes hosting services that meet Government of Canada data residency requirements;
 - (ii) Meets Government of Canada security requirements and industry best practices;
 - (iii) Includes secure maintenance and technical support;
 - (iv) Includes training and other professional services as and when requested;
- (b) Includes regularly updated training materials and solution documentation including all requisite software licenses and warranties; and

- (i) The Government of Canada will retain ownership of all data in the Solution including business data, monitoring data, and metadata.
- (c) For this solicitation, Canada may:
 - (i) Award up to three Contracts to successful Bidders to each develop a Capability and Usability Assessment (CUA) Prototype Solution in accordance with article 2. Phase 1 – Prototype Solution of Annex A – Statement of Work. At Canada's sole discretion, Canada may exercise the option on one Contract to deliver the production ready Solution in accordance with article 3. Phase 2 of Annex A – Statement of Work.
- (d) 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-Columbia Free Trade Agreement (CCFTA), the Canada-Panama Free Trade Agreement (CPFTA), the Canada-European Union Comprehensive Economic and Trade Agreement (CETA) if it is in force, the Canadian Free Trade Agreement (CFTA), Canada-Honduras Free Trade Agreement (CHFTA), Canada-Korea Free Trade Agreement (CKFTA), Canada-Peru Free Trade Agreement (CPFTA), Canada-Ukraine Free Trade Agreement (CUFTA), and the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP).
- (e) Canada reserves the right to, at a subsequent date and at its sole discretion, identify the solution either as a multi-departmental solution, or designate the solution as a Government of Canada Enterprise-wide standard if and when determined by the GC-Enterprise Architecture Review Board (GCEARB).
- (f) "The Federal Contractors Program (FCP) for employment equity applies to this procurement: refer to Part 5 – Certifications and Additional Information, Part 7 – Resulting Contract Clauses and the form titled Federal Contractors Program for Employment Equity – Certification."

1.4 Security Requirements

- (a) Before award of a contract, the following conditions must be met:
 - (i) the Bidder must hold a valid organization security clearance as indicated in Part 7 – Resulting Contract Clauses;
 - (ii) the Bidder's proposed individuals requiring access to classified or protected information, assets or sensitive work sites must meet the security requirements as indicated in Part 7 – Resulting Contract Clauses;
 - (iii) the Bidder must provide the name of all individuals who will require access to classified or protected information, assets or sensitive work sites;
 - (iv) the Bidder's proposed location of work performance and document safeguarding must meet the security requirements as indicated in Part 7 – Resulting Contract Clauses;
 - (v) the Bidder must provide the addresses of proposed sites or premises of work performance and document safeguarding as indicated in Part 3 – Section IV Additional Information.
- (b) Bidders are reminded to obtain the required security clearance promptly. Any delay in the award of a contract to allow the successful Bidder to obtain the required clearance will be at the entire discretion of the Contracting Authority.

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

1.5 Debriefings

Bidders may request a debriefing on the results of the bid solicitation process. Bidders should make the request to the Contracting Authority within 15 working days from receipt of the results of the bid solicitation process.

1.6 Conflict of Interest – Unfair Advantage

- (a) In order to protect the integrity of the procurement process, Bidders are advised that Canada may reject a bid in the following circumstances:
- (i) if the Bidder, any of its subcontractors, any of their respective employees or former employees was involved in any manner in the preparation of the bid solicitation or in any situation of conflict of interest or appearance of conflict of interest;
 - (ii) if the Bidder, any of its subcontractors, any of their respective employees or former employees had access to information related to the bid solicitation that was not available to other Bidders and that would, in Canada's opinion, give or appear to give the Bidder an unfair advantage.
- (b) The experience acquired by a bidder who is providing or has provided the goods and services described in the bid solicitation (or similar goods or services) will not, in itself, be considered by Canada as conferring an unfair advantage or creating a conflict of interest. This bidder remains however subject to the criteria established above.
- (c) Where Canada intends to reject a bid under this section, the Contracting Authority will inform the Bidder and provide the Bidder an opportunity to make representations before making a final decision. Bidders who are in doubt about a particular situation should contact the Contracting Authority before bid closing. By submitting a bid, the Bidder represents that it does not consider itself to be in conflict of interest nor to have an unfair advantage. The Bidder acknowledges that it is within Canada's sole discretion to determine whether a conflict of interest, unfair advantage or an appearance of conflict of interest or unfair advantage exists.

1.7 Bidder's Conference

- (a) A bidders' conference will be held online via WebEx on October 8th 2019. The conference will begin at 1:00 PM EST to 4:00 PM EST. The scope of the requirement outlined in the bid solicitation will be reviewed during the conference and questions will be answered. It is recommended that bidders who intend to submit a bid attend or send a representative.

Meeting number (access code): 555 269 233

Meeting password: NGDLE2019

1:00 pm | (UTC-05:00) Eastern Time (US & Canada) | 3 hrs

Join by phone

1-877-413-4782 Call-in toll-free number (Canada)

1-613-960-7511 Call-in number (Canada)

294 486 7 Attendee access code

Solicitation No. - N° de l'invitation
0X001-190594/A
Client Ref. No. - N° de réf. du client
0X001-190594

Amd. No. - N° de la modif.
-
File No. - N° du dossier
108xl0X001-190594

Buyer ID - Id de l'acheteur
108 XL
CCC No./N° CCC - FMS No./N° VME

- (b) Any clarifications or changes to the bid solicitation resulting from the bidders' conference will be included as an amendment to the bid solicitation. Bidders who do not attend will not be precluded from submitting a bid.

PART 2 – BIDDER'S 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](https://buyandsell.gc.ca/policy-and-guidelines/standard-acquisition-clauses-and-conditions-manual) (<https://buyandsell.gc.ca/policy-and-guidelines/standard-acquisition-clauses-and-conditions-manual>) issued by Public Services and Procurement 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 (2018-05-22) Standard Instructions – Goods or Services – Competitive Requirements, are incorporated by reference into and form part of the bid solicitation. If there is a conflict between the provisions of 2003 and this document, this document prevails.
- (d) Subsection 5(4) of 2003, Standard Instructions – Goods or Services – Competitive Requirements is amended as follows:
 - (i) Delete: 60 days
 - (ii) Insert: 120 days

2.2 Submission of Bids

- (a) Bids must be submitted only to Public Services and Procurement Canada (PSPC) Bid Receiving Unit by the date, time and place indicated on page 1 of the bid solicitation.
- (b) Due to the nature of the bid solicitation, bids transmitted by facsimile to PWGSC will not be accepted.

2.3 Former Public Servant

Contracts awarded to former 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 FPSs, Bidders must provide the information required below before contract award. If the answer to the questions and, as applicable the information required have not been received by the time the evaluation of bids is completed, Canada will inform the Bidder of a time frame within which to provide the information. Failure to comply with Canada's request and meet the requirement within the prescribed time frame will render the bid non-responsive.

Definitions

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

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

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

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

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

Former Public Servant in Receipt of a Pension

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

If so, the Bidder must provide the following information, for all FPSs in receipt of a pension, as applicable:

- (a) name of former public servant;
- (b) date of termination of employment or retirement from the Public Service.

By providing this information, Bidders agree that the successful Bidder's status, with respect to being a former public servant in receipt of a pension, will be reported on departmental websites as part of the published proactive disclosure reports in accordance with [Contracting Policy Notice: 2012-2](#) and the [Guidelines on the Proactive Disclosure of Contracts](#).

Work Force Adjustment Directive

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

If so, the Bidder must provide the following information:

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

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 5 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 with copies 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, and the laws of Canada, as applicable.

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

PART 3 – BID PREPARATION INSTRUCTIONS

3.1 Bid Preparation Instructions

- (a) If the Bidder chooses to submit its bid electronically, Canada requests that the Bidder submits its bid in accordance with section 08 of the SACC 2003 Standard Instructions – Goods or Services – Competitive Requirements. Bidders must provide their bid in a single transmission. The epost Connect service has the capacity to receive multiple documents, up to 1GB per individual attachment.
- (b) Prices must appear in the financial bid only. No prices must be indicated in any other section of the bid.
- (c) The bid must be gathered per section and separated as follows:
- Section I: Technical Bid
 - Section II: Financial Bid
 - Section III: Certifications
 - Section IV: Additional Information
- (d) If the Bidder chooses to submit its bid in hard copies, Canada requests that the Bidder submits its bid in separately bound sections as follows:
- Section I: Technical Bid (2 hard copies and 1 soft copy via USB key)
 - Section II: Financial Bid (2 hard copies and 1 soft copy via USB key)
 - Section III: Certifications (1 hard copy and 1 soft copy via USB key)
 - Section IV: Additional Information (1 hard copy and 1 soft copy via USB key)
- (i) use 8.5 x 11 inch (216 mm x 279 mm) paper;
 - (ii) use a numbering system that corresponds to the bid solicitation.
- (e) In April 2006, Canada issued a policy directing federal departments and agencies to take the necessary steps to incorporate environmental considerations into the procurement process Policy on Green Procurement (<https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32573>). To assist Canada in reaching its objectives, bidders should:
- (i) use 8.5 x 11 inch (216 mm x 279 mm) paper containing fibre certified as originating from a sustainably-managed forest and containing minimum 30% recycled content; and
 - (ii) use an environmentally-preferable format including black and white printing instead of colour printing, printing double sided/duplex, using staples or clips instead of cerlox, duotangs or binders.
- (f) If the Bidder is simultaneously providing its bidding hard and electronic copies, and if there is a discrepancy between the wordings of these copies, the wording of the electronic copy provided through epost Connect service will have priority over the wording of the hard copies.
- (g) If there is a discrepancy between the wording of the soft copy on electronic media and the hardcopy, the wording of the hard copy will have priority over the wording of the soft copy.

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

3.2 Submission of Multiple Bids

- (a) A Bidder, including related entities, will be permitted to participate in the submission of:
- (i) one bid by the Bidder on its own and one bid from a related entity to the Bidder submitted in a joint venture that includes at least one party that is not related to the Bidder;
 - (ii) two bids submitted in joint venture, each of which contains one or more related entities, where at least one of the joint ventures includes at least one party that is not a related entity to the Bidder; or
 - (iii) two bids, each of which is from the Bidder and a related entity to the Bidder on its own.
 - (iv) 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:
 - (1) they are the same legal entity (i.e., the same natural person, corporation, partnership, limited liability partnership, etc.);
 - (2) they are "related persons" or "affiliated persons" according to the Canada Income Tax Act;
 - (3) 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
 - (4) 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.

3.3 Joint Venture Experience

- (a) 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.

- (b) 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.

- (c) 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 submitted 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:

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

That show in total 100 billable days.

- (d) 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.

3.4 Section I: Technical Bid

- a) In their technical bid, Bidders must demonstrate their understanding of the requirements contained in the bid solicitation and explain how they will meet these requirements. Bidders must demonstrate their capability in a thorough, concise and clear manner for carrying out the work.
- b) The technical bid consists of the following:
- (i) **Bid Submission Form:** Bidders are requested to include the Bid Submission Form – Form 1 with their bids. It provides a common form in which Bidders can provide information required for evaluation and contract award, such as a contact name and the Bidder's Procurement Business Number, etc. Using the form to provide this information is not mandatory, but it is recommended. If Canada determines that the information required by the Bid Submission Form is incomplete or requires correction, Canada will provide the Bidder with an opportunity to do so.
 - (ii) **Previous Similar Projects:** Where the bid must include a description of previous similar projects: (i) a project must have been completed by the Bidder itself (and cannot include the experience of any proposed subcontractor or any affiliate of the Bidder); (ii) a project must have been completed by the bid closing date; (iii) each project description must include, at minimum, the name and either the telephone number or e-mail address of a customer reference; and (iv) if more similar projects are provided than requested, Canada will decide in its discretion which projects will be evaluated. A project will be considered "similar" to the Work to be performed under any resulting contract if the project was for the performance of work that closely matches the descriptions identified in Annex A, Statement of Work. Work will be considered to "closely match" if the work in the provided project is described in at least 50% of the points of responsibility listed in the description of the given resource category.

(iii) **Customer Reference Contact Information:**

- i. The Bidder must provide customer references. The customer reference must each confirm, "if" requested by PSPC, the facts identified in the Bidder's bid.

The form of question to be used to request confirmation from customer references is as follows:

[Sample Question to Customer Reference: "Has [the Bidder] provided your organization with [describe the services and, if applicable, describe any required time frame within which those services must have been provided]?"

- Yes, the Bidder has provided my organization with the services described above.
- No, the Bidder has not provided my organization with the services described above.
- I am unwilling or unable to provide any information about the services described above.]

- ii. For each customer reference, the Bidder must, at a minimum, provide the name and e-mail address for a contact person. If only the telephone number is provided, it will be used to call to request the e-mail address and the reference check will be done by e-mail.

Bidders are also requested to include the title of the contact person. It is the sole responsibility of the Bidder to ensure that it provides a contact who is knowledgeable about the services the Bidder has provided to its customer and who is willing to act as a customer reference. Crown references will be accepted.

- (iv) **List of Proposed Software that will form part of the Solution:** The Bidder must include a complete list identifying both the name and the version number of each component of the Software required for the proposed Solution. If the list of proposed Licensed Software is not included with the bid, it must be delivered prior to Contract Award.
- (v) **Description of Evolution of Proposed Solution Components:** The Bidder is requested to describe when and how each of the components of the proposed **Solution** were conceived and how they have evolved, with the accomplishments of each release. This is requested for information purposes only and will not be evaluated.
- (vi) **Video Demonstration:** The Bidder must submit a video demonstration in accordance with section 1.1 Mandatory Criteria of Annex G – Bid Evaluation Criteria.
- (vii) **Sandbox Solution:** The Bidder should provide a sandbox Solution in accordance with section 1.2 Point Rated Technical Criteria of Annex G – Bid Evaluation Criteria.

3.5 Section II: Financial Bid

- (a) **Financial Bid:** Bidders must submit their financial bid in accordance with the Financial Bid Presentation Sheet in Form 9 to Annex H – Bidders Forms. The total amount of Applicable Taxes must be shown separately. 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) **Exchange Rate Fluctuation:** The requirement does not offer exchange rate fluctuation risk mitigation. Requests for exchange rate fluctuation risk mitigation will not be considered. All bids including such provision will render the bid non-responsive.
- (c) **Variation in Resource Rates By Time Period:** For any given resource category, where the financial tables provided by Canada allow different firm rates to be charged for a resource category during different time periods. The rate bid for the same resource category during any subsequent time period must not be lower than the rate bid for the time period that includes the first option year of the Contract.
- (d) **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.
- (e) **Financial Submission:** In the Financial Submission, Bidders must submit the proposed SaaS and hosted services pricing and applicable percentage discount, and any prices or rates applicable for professional services to be provided by the Bidder. It is required that the SaaS and hosted services and Prices section of the Submission be presented as per the template provided in Form 9 of **Annex H – Bidders Forms** firm prices of the RFP. The Financial Submission should address clearly and in sufficient depth the points that are subject to the evaluation criteria against which the Submission will be evaluated.
- (i) The following must be addressed in the Bidder's **Form 9 of Annex H – Bidders Forms** firm prices:
- (1) **SaaS Solution's Name:** Bidders must provide the commercial name that the SaaS Publisher uses to identify the SaaS Solution commercially;
 - (2) **SaaS Publisher's Name:** Bidders must provide the name of the SaaS Publisher that owns the Intellectual Property rights to the SaaS Solution;
 - (3) **Cloud Service Provider (CSP)'s name:** Bidders must identify the existing Cloud Service Provider (CSP) that hosts the proposed SaaS Solution.
- (ii) The prices must be:
- (1) the Bidder's commercial pricing less the applicable percentage discount,
 - (2) in Canadian dollars; and,
 - (3) exclusive of Goods and Services Tax or Harmonized Sales tax.
- (f) **Electronic Payment of Invoices – Bid:** If you are willing to accept payment of invoices by Electronic Payment Instruments, complete Annex H – Bidders Forms, Form 8 – Electronic Payment Instruments, to identify which ones are accepted.
- If Annex H – Bidders Forms, Form 8 – Electronic Payment Instruments is not completed, it will be considered as if Electronic Payment Instruments are not being accepted for payment of invoices.
- Acceptance of Electronic Payment Instruments will not be considered as an evaluation criterion.
- (g) The requirement does not offer exchange rate fluctuation risk mitigation. Requests for exchange rate fluctuation risk mitigation will not be considered. All bids including such provision will render the bid non-responsive.

3.6 Section III: Certifications

It is a requirement that Bidders submit the certifications and additional information required under Part 5.

3.7 Section IV: Additional Information

(a) **Bidder's Proposed Sites or Premises Requiring Safeguarding Measures**

As indicated in Part 1 under Security Requirements, the Bidder must provide the full addresses of the Bidder's and proposed individuals sites or premises for which safeguarding measures are required for Work Performance:

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

- (b) The Company Security Officer must ensure through the [Contract Security Program](#) that the Contractor and individuals hold a valid security clearance at the required level, as indicated in Part 1, clause 1.1, Security Requirements.

PART 4 – EVALUATION AND ASSESSMENT PROCEDURES

4.1 Evaluation Procedures

- (a) Proposals will be evaluated in accordance with the entire requirement of the bid solicitation including the Technical and Financial requirements. There are several stages in the evaluation and selection process, which are described below:

- (i) **Evaluation** – This process will evaluate Bids against the Technical and the Financial evaluation criteria and to rank the Bidders. Up to 3 top ranked responsive Bidders will be considered for the award of a Contract.

Even though the evaluation and selection will be conducted in stages, the fact that Canada has proceeded to a later stage in its evaluations does not mean that Canada has conclusively determined that the Bidder or Contractor has successfully passed all the previous stages.

- (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.

4.1.1 Evaluation Components

(a) **Technical Evaluation**

(i) **Mandatory Technical Criteria:**

- (1.) The mandatory criteria that will be evaluated as part of the bid evaluation are listed in Annex G, Bid Evaluation Criteria.

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

(b) **Point-rated Technical Criteria:**

- (i) The point-rated criteria that will be evaluated as part of the bid evaluation are listed in Annex G, Bid Evaluation Criteria.
- (ii) 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 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. The point-rated technical criteria are described in Annex H, Bid Evaluation Criteria.

(c) **Reference Checks:**

- (i) For reference checks, Canada will conduct the reference check in writing by e-mail. Canada will send all e-mail reference check requests to contacts supplied by all the Bidders on the same day using the e-mail address provided in the bid. Canada will not award any points and/or a bidder will not meet the mandatory experience requirement (as applicable) unless the response is received within 5 working days of the date that Canada's e-mail was sent.

-
- (ii) On the third working day after sending out the reference check request, if Canada has not received a response, Canada will notify the Bidder by e-mail, to allow the Bidder to contact its reference directly to ensure that it responds to Canada within 5 working days. If the individual named by a Bidder is unavailable when required during the evaluation period, the Bidder may provide the name and e-mail address of an alternate contact person from the same customer. Bidders will only be provided with this opportunity once for each customer, and only if the originally named individual is unavailable to respond (i.e., the Bidder will not be provided with an opportunity to submit the name of an alternate contact person if the original contact person indicates that he or she is unwilling or unable to respond). The Bidder will have 24 hours to submit the name of a new contact. That contact will again be given 5 working days to respond once Canada sends its reference check request.
- (iii) Wherever information provided by a reference differs from the information supplied by the Bidder, the information supplied by the reference will be the information evaluated.
- (iv) Points will not be allocated and/or a bidder will not meet the mandatory experience requirement (as applicable) if (1) the reference customer states he or she is unable or unwilling to provide the information requested, or (2) the customer reference is not a customer of the Bidder itself (for example, the customer cannot be the customer of an affiliate of the Bidder instead of being a customer of the Bidder itself). Nor will points be allocated or a mandatory met if the customer is itself an affiliate or other entity that does not deal at arm's length with the Bidder.
- (v) Whether or not to conduct reference checks is discretionary. However, if PSPC chooses to conduct reference checks for any given rated or mandatory requirement, it will check the references for that requirement for all Bidders who have not, at that point, been found non-responsive.
- (d) **Financial Evaluation**
- (i) Bidders must submit their financial bid in accordance with the Basis of Payment in Annex B and it is provided for bid evaluation price determination only. The estimates used to calculate the Total Bid Price in Annex B are estimates only and are not to be considered as a commitment from Canada.
- (ii) **Formulae in Pricing Tables.** If the pricing tables provided to Bidders in Annex B 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.
- (iii) **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:
- (1.) 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;

- (2.) 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;
- (3.) 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
- (4.) 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.

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.

- (e) **Number of Resource Categories Evaluated:** Only the resource categories proposed will be evaluated as part of this bid solicitation and as identified in Annex H – Bidders Forms, Form 9. Additional resources will only be assessed after Contract award once specific tasks are requested of the Contractor. After Contract award, the Task Authorization process will be in accordance with Part 7 - Resulting Contract Clauses, the Article titled "Task Authorization". When a Task Authorization Form (TA Form) is issued, the Contractor will be requested to propose a resource to satisfy the specific requirement based on the TA Form's Statement of Work.

4.1.2 Ranking Bids

- (a) **Highest Combined Rating of Technical Merit (70%) and Price (30%) – Evaluation Stage**

The top 3 ranked bids will be determined based on the highest responsive combined rating of technical merit and price. 70% weightage will be given to the technical bid and 30% weightage will be given to the financial bid as per the following formula:

$$\frac{\text{Points received for rated requirements}}{\text{Maximum score possible}} \times 70\% = \text{Total 1}$$

$$\frac{\text{Lowest Total Bid Price}}{\text{Total Bid Price of the bid being ranked}} \times 30\% = \text{Total 2}$$

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

Evaluation	Weightage	Overall weightage per evaluation
Technical Score	70%	70%
Financial Score	30%	30%
Total Rating:		100%

Top-ranked responsive bids will be determined based on the proposal which has met all mandatory criteria and offers the Highest Responsive Combined Rating of Technical Merit and Price as calculated above.

(b) **Basis of Selection**

To be declared responsive, a bid must:

- (i) comply with all the requirements of the bid solicitation;
- (ii) meet all mandatory technical requirements stipulated in Annex G, Bid Evaluation Criteria; and,
- (iii) obtain the required minimum of 70% score for the technical evaluation criteria stipulated in Annex G, Bid Evaluation Criteria which are subject to point rating.

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

- (c) Bids will be ranked by score from highest to lowest and the 3 top ranked responsive bids will be recommended for award of a Contract. Canada may award up to three Contracts of up to 6 months in duration with a value of up to \$30,000.00 CAD each, applicable taxes extra, to the top 3 ranked responsive Bidders to perform the Work defined in Phase 1 of Annex A – Statement of Work.
- (d) In the event that a Bidder withdraws their bid, or the bid is set aside, Canada may offer the next highest ranked responsive Bidder a Contract.
- (e) In the event of a tie score(s) that impacts the ranking, the responsive Bidder with the highest Technical Score will be recommended for award of a Contract.

4.2 Rights of Canada

Canada reserves the right to:

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

- (g) negotiate with the sole responsive Bidder to ensure the best value to Canada.

4.3 Rejection of Bids

- (a) Grounds for Rejection. Canada may reject a bid where the Bidder is bankrupt or where its activities are rendered inoperable for an extended period, or where the Bidder or an employee or subcontractor included as part of the bid:
 - (i) is subject to a Vendor Performance Corrective Measure, under the Vendor Performance Corrective Measure Policy, which renders the Bidder, employee or subcontractor ineligible to bid on the requirement;
 - (ii) has committed fraud, bribery, fraudulent misrepresentation or failed to comply with laws protecting individuals against any manner of discrimination;
 - (iii) has conducted himself/herself improperly; with respect to current or prior transactions with the Government of Canada;
 - (iv) has been suspended or terminated by Canada for default with respect to a contract;
 - (v) has performed other contracts in a sufficiently poor manner so as to jeopardize the successful completion of the requirement being bid on.
- (b) Notification of Rejection for Suspension or Termination. Where Canada intends to reject a bid due to suspension, termination or sufficiently poor performance of another contract, the Contracting Authority will so inform the Bidder and provide the Bidder 10 days within which to make representations, before making a final decision on the bid rejection.
- (c) Multiple Bids from Single Bidder or Joint Venture. Canada reserves the right to apply additional scrutiny, in particular, when multiple bids are received in response to a bid solicitation from a single bidder or a joint venture. Canada reserves the right to reject any or all of the bids submitted by a single bidder or joint venture if their inclusion:
 - (i) in the evaluation has the effect of prejudicing the integrity and fairness of the process, or
 - (ii) in the procurement process would distort the solicitation evaluation or would not provide good value to Canada.

4.4 Capability and Usability Assessment Procedures

- (a) Capability and Usability Assessment (CUA): Based on the results of the Technical and Financial evaluation results, Canada will award Contracts to up to 3 top ranked responsive Bidders for an estimated amount of \$30,000.00 CAD, applicable taxes excluded. These Contracts will cover a period of 6 months, and will require that each Contractor submit a CUA Prototype Solution within 6 weeks of Contract Award in accordance with the parameters of the CUA described in Appendix A to Annex A – Statement of Work, for assessment in accordance with the CUA.
- (b) Following Canada's receipt of the Contractor's CUA Prototype Solution, a Capability and Usability Assessment (CUA) will be conducted by Canada. The Capability and Usability Assessment (CUA) Prototype Solution deliverables provided under the Contract will be assessed by Canada against the criteria detailed at Appendix A to Annex A – Statement of Work.
- (c) The Contractor's CUA Prototype Solution will be assessed against mandatory and point rated CUA criteria. The point rated CUA criteria will be scored and the sum of the scores for each individual category will be calculated in accordance with the assessment criteria and maximum points listed in each category of Appendix A to Annex A – Statement of Work.

(d) The overall assessment score for the CUA will be calculated based on the highest responsive combined rating of technical merit, price and CUA.

(e) **Basis of Canada's Decision to Exercise the Phase 2 Solution Option**

(i) The top ranked responsive CUA Prototype Solution will be determined based on the highest responsive combined rating of technical merit, price and CUA. 30% weighting will be given to the Technical Evaluation Score. 20% weighting will be given to the Financial Evaluation Score. 50% weighting will be given to the CUA Score, as per the following table:

Assessment	Weightage
Technical Evaluation Score	30%
Financial Evaluation Score	20%
Capability and Usability Assessment Score	50%

(ii) In the event of a tie, the CUA Score will be used to rank the Contractors from highest to lowest score. If there are further ties, the lowest Financial Score will be used to rank the Contractor.

(iii) Canada will, at its sole discretion, exercise its irrevocable option to select a Contractor to perform all or a portion of the Work under article 3. Phase 2 - Solution of Annex A – Statement of Work. Canada may also, at its discretion, exercise its irrevocable option with other Contractors who participated in the CUA for all or a portion of the Work if it is determined that this would best meet the needs of Canada.

PART 5 – CERTIFICATIONS AND ADDITIONAL INFORMATION

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

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

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

5.1 Certifications Required with Bid

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

(a) **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 (Form 5) for the Integrity Regime website (<http://www.tpsgc-pwgsc.gc.ca/ci-if/declaration-eng.html>) to be given further consideration in the procurement process.

(b) **Software Publisher Certification, Software Publisher Authorization and Software Contributor Certification**

- (i) If the Bidder is the Software Publisher for any of the proprietary software products it bids, Canada requires that the Bidder confirm in writing that it is the Software Publisher. Bidders are requested to use the Software Publisher Certification Form included with the bid solicitation. Although all the contents of the Software Publisher Certification Form are required, using the form itself to provide this information is not mandatory. For Bidders who use an alternate form, it is in Canada's sole discretion to determine whether all the required information has been provided. Alterations to the statements in the form may result in the bid being declared non-responsive.
- (ii) Any Bidder that is not the Software Publisher of all the proprietary software products proposed in its bid is required to submit proof of the Software Publisher's authorization, which must be signed by the Software Publisher (not the Bidder). No Contract will be awarded to a Bidder who is not the Software Publisher of all of the proprietary software it proposes to supply to Canada, unless proof of this authorization has been provided to Canada. If the proprietary software proposed by the Bidder originates with multiple Software Publishers, authorization is required from each Software Publisher. Bidders are requested to use the Software Publisher Authorization Form included with the bid solicitation. Although all the contents of the Software Publisher Authorization Form are required, using the form itself to provide this information is not mandatory. For Bidders/Software Publishers who use an alternate form, it is in Canada's sole discretion to determine whether all the required information has been provided. Alterations to the statements in the form may result in the bid being declared non-responsive.
- (iii) In this bid solicitation, "Software Publisher" means the owner of the copyright in any software products proposed in the bid, who has the right to license (and authorize others to license/sub-license) its software products.
- (iv) The following certification documents are required as part of the Submission:

Form 2 Software as a Service Publisher Certification Form
Form 3 Software as a Service Publisher Authorization Form
Form 4 Cloud Service Provider ("CSP") Letter of Attestation

5.2 Certifications Precedent to Contract Award and Additional Information

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

5.3 Integrity Provisions – Required Documentation

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

5.4 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. (<https://www.canada.ca/en/employment-social-development/programs/employment-equity/federal-contractor-program.html>).

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 (Form 7) titled Federal Contractors Program for Employment Equity – Certification, before contract award. If the Bidder is a Joint Venture, the Bidder must provide the Contracting Authority with a completed annex Federal Contractors Program for Employment Equity – Certification, for each member of the Joint Venture.

5.5 Sole Bid – Price Support

In the event that your bid is the sole bid received, Government Contract Regulations require price support be submitted in conjunction with the offer. Acceptable price support is one or more of the following:

- (a) a current published price list indicating the percentage discount available to Canada; or
- (b) copies of paid invoices for the like quality and quantity of the goods, services or both sold to other customers; or
- (c) a price breakdown showing the cost of direct labour, direct materials, purchased items, engineering and plant overheads, general and administrative overhead, transportation, etc., and profit; or
- (d) price or rate certifications; or
- (e) any other supporting documentation as requested by Canada.

PART 6 – SECURITY AND FINANCIAL REQUIREMENT

Prior to award of contract, the following conditions must be met:

6.1 Canadian Suppliers:

- (a) The Contractor/Offeror must, at all times during the performance of the Contract/Standing Offer, hold a valid Designated Organization Screening (DOS) with approved Document Safeguarding at the level of PROTECTED B, issued by the Canadian Industrial Security Directorate (CISD), Public Works and Government Services Canada (PWGSC).
- (b) The Contractor/Offeror personnel requiring access to PROTECTED information, assets or work site(s) must EACH hold a valid RELIABILITY STATUS, granted or approved by the CISD/PWGSC.
- (c) The Contractor MUST NOT utilize its Information Technology systems to electronically process, produce or store PROTECTED information until the CISD/PWGSC has issued written approval. After approval has been granted or approved, these tasks may be performed at the level of PROTECTED B, including an IT Link at the level of PROTECTED B.
- (d) Subcontracts which contain security requirements are NOT to be awarded without the prior written permission of CISD/PWGSC.
- (e) The Contractor/Offeror must comply with the provisions of the:
 - (i) Security Requirements Check List and security guide (if applicable), attached at Annex C
 - (ii) Industrial Security Manual (Latest Edition)

6.2 Foreign Supplier

The Canadian Designated Security Authority (Canadian DSA) for industrial security matters in Canada is the

Industrial Security Sector (ISS), Public Works and Government Services Canada (PWGSC), administered by International Industrial Security Directorate (IISD), PWGSC. The Canadian DSA is the authority confirming Bidder compliance with the security requirements for foreign suppliers. The following security requirements apply to the foreign recipient Bidder incorporated or authorized to do business in a jurisdiction other than Canada and delivering/performing the Solution, in addition to the Privacy and Security Requirements. These security requirements are in addition to those requirements identified below in Protection and Security of Data Stored in Databases.

- (a) The foreign recipient Bidder must be from a Country within the North Atlantic Treaty Organization (NATO), the European Union (EU) or from a country with which Canada has an international bilateral security instrument. The Contract Security Program (CSP) has international bilateral security instruments with the countries listed on the following PWGSC website: <http://www.tpsgc-pwgsc.gc.ca/esc-src/international-eng.html>.
- (b) The foreign recipient Bidder must provide proof that they are incorporated or authorized to do business in their jurisdiction as indicated in Part 7 – Resulting Contract Clauses.
- (c) The foreign recipient Bidder must be registered with the appropriate government administered supervisory authority responsible for Personal Information in the country(ies) in which it is

incorporated or operating and authorized to do business, as indicated in Part 7 – Resulting Contract Clauses, 7.5(b) Security Requirement for Foreign Suppliers.

- (d) The foreign recipient Bidders must provide assurance that it can receive and store CANADA PROTECTED B/Personal information/assets on its site or premises as indicated in Part 7 – Resulting Contract Clauses and the listed IT Security Requirements.
- (e) The foreign recipient Bidder's proposed location of work performance must meet the security requirement as indicated in Part 7 and as listed in the IT Security Requirements.
- (f) The foreign recipient Bidder must provide the address(es) of proposed location(s) of work performance and document safeguarding.
- (g) The successful foreign recipient Bidder's proposed individuals requiring access to CANADA PROTECTED/Personal information/assets or restricted work sites must EACH hold a valid Criminal Record Check, with favorable results, from a recognized governmental agency or private sector organization in their country, as well as a Background Verification, validated by the Canadian DSA.
- (h) The successful foreign recipient Bidder's proposed individuals must not begin the Work until all requisite security requirements have been met.
- (i) In the case of a joint venture Bidder, each member of the joint venture must meet the security and privacy requirements.
- (j) The foreign recipient Bidders must provide proof that all the databases including the backup database used by organizations to provide the services described in the SOW containing any CANADA PROTECTED/Personal Information, related to the Work, are located in Canada.
- (k) The successful foreign recipient Bidder MUST NOT utilize its Information Technology (IT) systems to electronically process, produce, or store on a computer system any CANADA PROTECTED B/Personal information/assets until authorization to do so has been confirmed by the Canadian DSA.
- (l) The Bid must clearly indicate the Work which the foreign recipient Bidder plans to subcontract. All subcontracting arrangements which provide the subcontractor with access to any CANADA PROTECTED/Personal Information are subject to approval by Canada. The description of subcontracting arrangements should demonstrate how the foreign recipient Bidder will ensure that all requirements, terms, conditions, and clauses of the subcontract are met.
- (m) In the event that a foreign recipient Bidder is chosen as a Contractor for this contract, subsequent country-specific foreign security requirement clauses must be generated and promulgated by the Canadian DSA, and provided to the Government of Canada Contracting Authority, to ensure compliance with the security provisions.

6.3 Financial Capability

SACC Manual clause A9033T (2012-07-16) Financial Capability applies, except that subsection 3 is deleted and replaced with the following: "If the Bidder is a subsidiary of another company, then any financial information required by the Contracting Authority in 1(a) to (f) must also be provided by each level of parent company, up to and including the ultimate parent company. The financial information of a parent company does not satisfy the requirement for the provision of the financial information of the Bidder; however, if the Bidder is a subsidiary of a company and, in the normal course of business, the required financial information is not generated separately for the subsidiary, the financial information of the parent company must be provided. If Canada determines that the Bidder is not financially capable but the parent company is, or if Canada is unable to perform a separate

Solicitation No. - N° de l'invitation
0X001-190594/A
Client Ref. No. - N° de réf. du client
0X001-190594

Amd. No. - N° de la modif.
-
File No. - N° du dossier
108xl0X001-190594

Buyer ID - Id de l'acheteur
108 XL
CCC No./N° CCC - FMS No./N° VME

assessment of the Bidder's financial capability because its financial information has been combined with its parent's, Canada may, in its sole discretion, award the contract to the Bidder on the condition that one or more parent companies grant a performance guarantee to Canada.”

PART 7 – RESULTING CONTRACT CLAUSES

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

This Contract is made on [CONTRACT DATE] between [CONTRACTOR NAME] (the “Contractor”) and [GOVERNMENT OF CANADA ENTITY] (“Canada”).

7.1 Requirement

- (a) The Contractor agrees to provide the Services and perform the Work described in the Contract in accordance with and at the prices set out in the Contract. This include:
- (b) Services: The Contractor agrees to provide the following Services:
 - (i) providing the Services identified in Annex A – Statement of Work, which includes, at a minimum:
 - i. granting online access and use of the Solution;
 - ii. providing any Solution-related software applications required for online access and use of the Solution;
 - iii. hosting the Solution;
 - iv. performing any Work required to design or develop features or functionality, and develop and implement any commercially available or custom software components in accordance with the Contract;
 - v. providing professional and training services, as and when requested by Canada, in accordance with the Task authorization (TA) process described herein; and
 - vi. providing Software Documentation.
- (c) **Optional Goods and Services.** The Contractor grants to Canada the irrevocable options to acquire the goods, services or both described at:
 - (i) Phase 2 – Solution Work as detailed under section 3 Phase 2 of Annex A – Statement of Work and at the prices set out under Annex B – Basis of Payment;
 - (ii) Annual Software as a Service Subscription Solution Authorized User Access for work under section 3 Phase 2 of Annex A – Statement of Work and at the prices set out under Annex B- Basis of Payment;
 - (iii) Professional Services on an as-and-when-requested basis as detailed under article 4 of Annex A Statement of Work and at the prices set out under Annex B – Basis of Payment;
 - (iv) Training Services on an as-and-when-requested basis as detailed under article 4 of Annex A Statement of Work and at the prices set out under Annex B – Basis of Payment; and

under the same conditions and at the prices and/or rates stated in Annex B – Basis of Payment. The option will only be exercised by the Contracting Authority and will be evidenced, through a contract amendment.

The Contracting Authority may exercise any option at any time before the expiry of the Contract by sending a written notice to the Contractor.
- (d) **Client:** Under the Contract, the “Client” is the Canada School of Public Service. 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. Canada reserves the right to, at a subsequent date and at its sole discretion, identify the solution either as a multi-departmental solution, or designate the solution as a Government of Canada Enterprise-wide standard if and when determined by the GC-Enterprise Architecture Review Board (GCEARB).

- (e) **Reorganization:** 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.
- (f) **Definitions and Interpretations:** The definitions and interpretations are included in the Annex D – Definitions and Interpretations.
- (g) **General Conditions and Supplemental General Conditions**
 - (i) **General Conditions**
 - i. All clauses and conditions identified in the Contract by number, date and title are set out in the Standard Acquisition Clauses and Conditions Manual (<https://buyandsell.gc.ca/policy-and-guidelines/standard-acquisition-clauses-and-conditions-manual>) issued by Public Services and Procurement Canada.
 - ii. 2035 (2018-06-21), General Conditions - Higher Complexity - Services are incorporated in the resulting Contract.
 - (ii) **Supplemental General Conditions**
 - i. The following Supplemental General Conditions below are incorporated in the resulting Contract:
 - ii. 4008, (2008-12-12) Personal Information.

7.2 Contract Term

- (a) **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.
- (b) **Initial Term – CUA Prototype Solution.** This Contract begins on the date the Contract is awarded for a period of 6 months from contract award date.
- (c) **Delivery Dates:**
 - i. The Contractor must provide all deliverables in accordance with the associated delivery dates as detailed under Annex A – Statement of Work.
- (d) **Additional Options:**
 - (i) **Option to Exercise Phase 2:** The Contractor grants to Canada the irrevocable option to authorize the Contractor to perform the Work detailed under article 3. "Phase 2 – Solution" of Annex A – Statement of Work. The Contractor agrees that it will be paid in accordance with the applicable provisions set out in Annex B – Basis of Payment.
 - (ii) **Option to purchase Annual Software as a Service Subscription Solution Authorized User Access:** The Contractor grants to Canada the irrevocable option to acquire Annual Software as a Service Subscription Solution Authorized User Access under the same terms and conditions. The Contractor agrees that it will be paid in accordance with the applicable provisions set out in Annex B – Basis of Payment.

- (iii) Option to acquire Professional Services on an as-and-when-requested basis as detailed under article 4 of Annex A Statement of Work and at the prices set out under Annex B – Basis of Payment;
- (iv) Option to acquire Training Services on an as-and-when-requested basis as detailed under article 4 of Annex A Statement of Work and at the prices set out under Annex B – Basis of Payment; and
- (v) Option to Extend Contract Period: The Contractor grants to Canada the irrevocable option to extend the term of the Contract by up to 9 additional one-year periods 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 Annex B – Basis of Payment. Canada may exercise the option(s) at any time before the expiry of the Contract by sending a written notice to the Contractor. The option may be exercised only by the Contracting Authority, and will be evidenced, for administrative purposes only, through an amendment to the Contract.

7.3 Solution

- (a) **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.
- (b) **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 Services 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.
- (c) **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:
 - i. 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.
 - ii. 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 Contractor 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.
- (d) **Downgrade.** If the Contractor is unable to provide the Services with no less favourable features and functionality, the Contractor will provide written Notice to Canada identifying the circumstance, and alternative options, specifically including a reduction in pricing. If no proposed alternative option is acceptable to Canada, the Contractor agrees to consent to a

termination of the Contract, and pay all identifiable direct costs incurred by Canada to migrate and store Client's Data, and to procure equivalent replacement services.

- (e) **Maintenance Releases.** During the Software Support Period, the Contractor must provide to Canada all Maintenance Releases, in object-code form, at no additional cost. All Maintenance Releases will become part of the Solution and will be subject to the conditions of Canada's license with respect to the Solution. Unless provided otherwise in the Contract, Canada will receive at least one Maintenance Release during any twelve (12) month maintenance period.

7.4 Solution Operational Changes

- (a) The Government of Canada is seeking an innovative **Solution** that can adapt and evolve with technological advances throughout the duration of the Contract. The Contractor-delivered **Solution** must be extensible and adaptable to harness future technology innovations that the Contractor may use to upgrade their Licensed Software. The Contractor will be required to provide to the Government of Canada all technological upgrades to the **Solution** free of charge where:
- (i) The upgrade has been made to their Licensed Software; and
 - (ii) The upgrade has been given free of charge to the Contractor's other client(s).
- (b) The Government of Canada also requires the Contractor to ensure that the **Solution** remains compatible with all future versions of iOS, Android and the following Web browsers:
- Internet Explorer
 - Google Chrome
 - Firefox
 - Safari
- (c) The Government of Canada requires that the Solution remains compliant with the WET and WCAG, as defined in the Statement of Work, throughout the duration of the Contract.
- (d) **On-going Maintenance of Software Code:** The Contractor must continue to maintain the **Solution** (i.e., the version or "build" originally accepted and licensed under the Contract). For clarity, the Contractor or the software publisher must be continuing to develop new code in respect of the components of the **Solution** to maintain its functionality, enhance it, and deal with Software Errors for at least 1 year from the date the **Solution** is accepted in accordance with the Acceptance Criteria of Annex A – Statement of Work. After that time, if the Contractor or the software publisher decides to discontinue or no longer maintain the then-current version or "build" of any component of the **Solution** and, instead, decides to provide upgrades to any Licensed Software component as part of the Software Support, the Contractor must provide written notice to Canada at least 12 months in advance of the discontinuation.

7.5 Solution Maintenance and Support

- (a) The Contractor must continuously maintain and support the Solution.
- (b) **Solution Support.** The Solution Support includes the following Technical Hotline Support and Web Support services:
- i. **Technical Hotline Support:** the Contractor must provide the Technical Hotline Support through the Contractor's toll-free hotline at (INSERT AT CONTRACT AWARD), in English and French, from 8:00 A.M. to 5:00 P.M. Eastern Time, Monday to Friday (excluding statutory holidays observed by the federal government in the province from which the call is made). The Contractor must answer or return all calls (with a live service agent) within 60 minutes of the initial time of the Client or User's initial call. The Contractor's personnel must be qualified and able to respond to the Client's and any Client User's questions and,

to the extent possible, be able to resolve user problems over the telephone and provide advice regarding configuration problems relating to the Licensed Software.

- ii. **Web Support:** The Contractor must provide Canada with technical web support services through a website that must include, as a minimum, frequently asked questions and on-line software diagnostic routines, support tools, and services. The Contractor's website must provide support in English. The Contractor's website must be available to Canada's users 24 hours a day, 365 days a year, and must be available 99% of the time. The Contractor's website address is (INSERT AT CONTRACT AWARD).

(c) **Software Error Correction Services**

- i. Canada may report to the Contractor any failure of the Licensed Programs to operate in accordance with the Software Documentation or, if applicable, the Specifications during the Software Support Period. Canada may report failures either in writing or by telephone or other remote communication. Upon receipt of a report of a failure from Canada, unless provided otherwise in the Contract, the Contractor must use all reasonable efforts to provide Canada within the time frames established in subsections 2 and 3, with a correction of the Software Error which caused the failure. Any such software correction must cause the Solution to meet the Software Documentation or, if applicable, the Specifications during the Software Support Period. The Contractor must use all reasonable efforts to provide permanent corrections for all Software Errors and the Contractor warrants that the Solution will meet the functional and performance criteria set out in the Specifications. All Software Error corrections will become part of the Solution and will be subject to the conditions of Canada's license with respect to the Solution.

- ii. Unless provided otherwise in the Contract, the Contractor must respond to a report of a Software Error in accordance with the severity of the Software Error, as detailed in subsection 3. The severity will be reasonably determined by Canada, and communicated to the Contractor, based on the following definitions:

"Severity 1":

indicates total inability to use a Licensed Program, resulting in a critical impact on user objectives;

"Severity 2":

indicates ability to use a Licensed Program but user operation is severely restricted;

"Severity 3":

indicates ability to use a Licensed Program with limited functions which are not critical to overall user operations;

"Severity 4":

indicates that the problem has been by-passed or temporarily corrected and is not affecting user operations.

- iii. Unless provided otherwise in the Contract, the Contractor must use reasonable efforts to correct Software Errors as follows:

"Severity 1":

within twenty-four (24) hours of notification by Canada;"

Severity 2":

within seventy-two (72) hours of notification by Canada;

"Severity 3":

within fourteen (14) days of notification by Canada;

"Severity 4":

within ninety (90) days of notification by Canada.

- iv. If Canada reports a Software Error to the Contractor, Canada must give the Contractor reasonable access to the computer system on which the Licensed Program resides, and must provide such information as the Contractor may reasonably request, including sample output and other diagnostic information, in order to permit the Contractor to expeditiously correct the Software Error.

7.6 Contractor Use of Canada's Data

- (a) The Contractor is provided access to use, for the term of the Contract, to Canada's Data for the sole and exclusive purpose of providing the **Solution** to Users, including a license to collect, process, store, generate, and display Canada Data only to the extent necessary in the providing of the Services.
- (b) The Contractor must:
 - (i) keep and maintain Canada's Data in strict confidence, using such degree of care as is appropriate and consistent with its obligations as further described in this Agreement and applicable law to avoid unauthorized access, use, disclosure, or loss;
 - (ii) use and disclose Canada's Data solely and exclusively for the purpose of providing the Services, such use and disclosure being in accordance with the Contract and applicable law; and,
 - (iii) not use, sell, rent, transfer, distribute, or otherwise disclose or make available Canada's Data for the Contractor's own purposes or for the benefit of anyone other than Canada without Canada's prior written consent.

The Contractor, its subcontractors, 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.

If requested by the Technical Authority, the 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 Contractor must not begin using a 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.

At the time it requests Personal Information from any individual, if the Contractor doubts that the individual has the capacity to provide consent to the disclosure and use of his or her Personal Information, the Contractor must ask the Technical Authority for instructions.

7.7 Services

- (a) **Solution Services**
 - (i) **Software as a Service.** The Contractor will provide all Services required for Canada to access and use the Solution as specified in Annex A – Statement of Work.
 - (ii) **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.

- (iii) **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.
- (iv) **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#>
- (v) **Included.** The Contractor represents and warrants that the Services include:
 - i. hosting and maintenance of the Solution,
 - ii. provision of all incidental and additional required information technology infrastructure services, in compliance with all required security standards,
 - iii. 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 unfettered access and use by the Client, regardless of the amount of data created, processed or stored by the Solution,
all of which is included in the price.
- (vi) **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:
 - i. distribute, license, loan, or sell the Solution;
 - ii. impair or circumvent the Solution's security mechanisms; or
 - iii. remove, alter, or obscure any copyright, trademark, or other proprietary rights notice on or in the Solution.
- (vii) **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 Contractor represents and warrants that any such modification will not result in less favorable terms, specifically including price, service levels and remedies, regardless of any notification to the contrary.

7.8 Documentation

- (a) **Solution Documentation.** The Contractor must provide or deliver access to the commercially available Solution Documentation to Canada upon Contract Award. The Contractor must update Solution Documentation on a commercially reasonable basis.
- (b) **Other Documentation.** The Contractor must provide or deliver access to any documentation required in performance of the Work.
- (c) **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.
- (d) **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.

- (e) **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.

7.9 Optional Professional and Training Services

- (a) **Professional Services.** The Contractor must perform and deliver such Professional Services (the "Work") to Canada on an as-and-when requested basis as detailed in a Task Authorization.
- (b) **Training Services.** The Contractor must perform and deliver such Training Services (the "Work") to Canada on an as-and-when requested basis as detailed in a Task Authorization.
- (c) **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.
- (d) **Time is of the Essence.** It is essential that the Work be delivered within or at the time stated in a Task Authorization.
- (e) **Authorized Personnel.** All the Work must be performed solely by Contractor's authorized personnel.
- (f) **Key Personnel.** If specific individuals are identified in the Contract to perform the Work, the Contractor must provide the services of those individuals. If the Contractor is unable to provide the services of any specific individual identified in the Contract, it must provide a replacement with equivalent qualifications and experience and provide written notice to Canada giving (i) the reason for the replacement, (ii) the name and qualifications of the replacement individual, and (iii) proof that the proposed replacement has the required security clearance from Canada.
- (g) **Request to Replace Key Personnel.** The Contracting Authority may order that a replacement stop performing the Work. In such a case, the Contractor must immediately comply with the order and secure a further replacement in accordance with terms of replacement of key personnel. The fact that the Contracting Authority does not order that a replacement stop performing the Work does not relieve the Contractor from its responsibility to meet the requirements of the Contract.
- (h) **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 Contractor 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. 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.
- (i) **Migration and 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 supplier and or migrate Client's Data to a new supplier environment, that there will be no charge for the services below other than those charges set out in the Basis of Payment.

7.10 Remedies

- (a) **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.
- (b) **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.
- (c) **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.

7.11 Subcontracts

- (a) **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 subcontractor is bound by the terms of this Contract, and (c) the Contractor remains liable to Canada for all the Work performed by the subcontractor.
- (b) **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 subcontractors at any tier to make purchases or subcontract as permitted in paragraphs (i) and (ii).

7.12 Excusable Delay

- (a) **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").
- (b) **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.

- (c) 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.
- (d) 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 subcontractors or agents as a result of an Excusable Delay.

7.13 Right to Terminate.

- (a) 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.

7.14 Inspection and Acceptance of the Work

- (a) 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.
- (b) Acceptance Procedures: Unless provided otherwise in the Contract, the acceptance procedures are as follows:
 - (c) when the Work is complete, the Contractor must notify the Technical Authority in writing, with a copy to the Contracting Authority, by referring to this provision of the Contract and requesting acceptance of the Work;
 - (d) Canada will have 30 days from receipt of the notice to perform its inspection (the "Acceptance Period").
 - (e) 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.
 - (f) 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.
 - (g) 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.

- (h) **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.
- (i) **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.

7.15 Kick-Off Meeting

- (a) The Contractor must schedule a kick off meeting with the presence of the Client and PSPC Contracting Authority within 5 business days of Contract award to discuss the overall requirement, the approach and methodology, contract, projects establishment, timeframe management and to clarify any issues. The meeting must occur prior starting any work and at a mutually agreed location or by teleconference. The Chairperson of the meeting shall be the Contracting Authority.
- (b) The Contractor must prepare and distribute the agenda of the meeting and submit it within a reasonable delay to the Contracting Authority for approval, prior to distribution to all Authorities.
- (c) The Contractor must provide the agenda and a presentation, if applicable, within 3 business days prior to the start date of the meeting.
- (d) The Contractor must prepare and provide minutes of the meeting within 10 business days to the Contracting Authority for approval, prior to distribution to all Authorities.

7.16 Progress Review Meeting

- (a) The Contracting Authority and the Contractor may, at any time, convene a meeting to discuss and review the progress of the Work against this Contract. Any such meeting must occur following notice to the other Party and must normally be held by teleconference. The Chairperson of the meeting shall be the Contracting Authority or the Party requesting the meeting;
- (b) The Contractor must prepare the agenda of the meeting and distribute it to all Authorities;
- (c) The Contractor must prepare the agenda of the meeting and submit it within a reasonable delay to the Contracting Authority for approval, prior to distributing them to all Authorities;
- (d) The Contractor will have to provide the completed presentation and items' agenda five (5) business days prior to the start date of the meeting;
- (e) The Contractor must prepare minutes of meeting and submit them within 15 working days to the Contracting Authority for approval, prior to distributing them to all Authorities.

7.17 Task Authorization

- (a) The Contractor's professional services performed under this Contract will be on an "as and when requested basis" using a Task Authorization.
- (b) **Form and Content of TA.** A TA will contain (a) Contract and TA number, (b) the details of the required activities and resources, (c) a description of the deliverables, (d) a schedule indicating completion dates for the major activities or submission dates for the deliverables, (e) security

requirements, and (f) costs. A TA will follow the format detailed in Annex F – Task Authorization Forms.

- (c) **Contractor's Response to TA.** The Contractor must provide to Canada, within the period specified in the TA, the proposed total price for performing the task and a breakdown of that cost, established in accordance with the fees. 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.
- (d) **TA Limit and Authorities for Validly Issuing TA.** A validly issued TA must be signed by the appropriate Canadian Authority as set forth in this Contract. Any work performed by the Contractor without receiving a validly issued TA is done at the Contractor's own risk.
- (e) **Periodic Usage Reports.** The Contractor must compile and maintain records on its provision of services to the federal government under the valid TA as issued under this Contract.
- (f) **Consolidation of TA for Administrative Purposes.** This Contract may be amended from time to time to reflect all validly issued TA to date, to document the Work performed under those TA for administrative purposes.

7.18 Security Requirement

Canada reserve the right to update the security requirement.

(a) Canadian Supplier

- (i) The Contractor/Offeror must, at all times during the performance of the Contract/Standing Offer, hold a valid Designated Organization Screening (DOS) with approved Document Safeguarding at the level of PROTECTED B, issued by the Canadian Industrial Security Directorate (CISD), **Public Works and Government Services Canada (PWGSC)**.
- (ii) The Contractor/Offeror personnel requiring access to PROTECTED information, assets or work site(s) must EACH hold a valid RELIABILITY STATUS, granted or approved by the CISD/PWGSC.
- (iii) The Contractor MUST NOT utilize its Information Technology systems to electronically process, produce or store PROTECTED information until the CISD/PWGSC has issued written approval. After approval has been granted or approved, these tasks may be performed at the level of PROTECTED B, including an IT Link at the level of PROTECTED B.
- (iv) Subcontracts which contain security requirements are NOT to be awarded without the prior written permission of CISD/PWGSC.
- (v) The Contractor/Offeror must comply with the provisions of the:
 - i. Security Requirements Check List and security guide (if applicable), attached at Annex C;
 - ii. Industrial Security Manual (Latest Edition)

(b) Foreign Supplier

The Canadian Designated Security Authority (Canadian DSA) for industrial security matters in Canada is the Industrial Security Sector (ISS), Public Works and Government Services Canada (PWGSC), administered by International Industrial Security Directorate (IISD), PWGSC. The Canadian DSA is the authority confirming foreign recipient **Contractor / Subcontractor** compliance with the security requirements for foreign suppliers. The following

security requirements apply to the foreign recipient **Contractor / Subcontractor** incorporated or authorized to do business in a jurisdiction other than Canada and delivering/performing the Solution, in addition to the Privacy and Security Requirements. These security requirements are in addition to those requirements identified below in Protection and Security of Data Stored in Databases.

- (i) The foreign recipient **Contractor / Subcontractor** must be from a Country within the North Atlantic Treaty Organization (NATO), the European Union (EU) or from a country with which Canada has an international bilateral security instrument. The Contract Security Program (CSP) has international bilateral security instruments with the countries listed on the following PWGSC website: <http://www.tpsgc-pwgsc.gc.ca/esc-src/international-eng.html>.
- (ii) The Foreign recipient **Contractor / Subcontractor** must at all times during the performance of the **contract/subcontract** be registered with the appropriate government administered supervisory authority responsible for Personal Information in the country(ies) in which it is incorporated or operating and authorized to do business. The Foreign recipient **Contractor / Subcontractor** must provide proof of its registration with the applicable supervisory authority to the Contracting Authority and the Canadian DSA, and identify the relevant national Privacy Authority. For European **Contractors / Subcontractors**, this will be the national Data Protection Authority (DPA).
- (iii) The foreign recipient **Contractor / Subcontractor** must, at all times during the performance of the **contract**, hold an equivalence to a valid Designated Organization Screening (DOS), issued by the Canadian DSA as follows:
 - i. The foreign recipient **Contractor / Subcontractor** must provide proof that they are incorporated or authorized to do business in their jurisdiction.
 - ii. The foreign recipient **Contractor / Subcontractor** must not begin the work, services or performance until the Canadian Designated Security Authority (DSA) is satisfied that all contract security requirement conditions have been met. Canadian DSA confirmation must be provided, in writing, to the foreign recipient **Contractor / Subcontractor** in an Attestation Form, to provide confirmation of compliance and authorization for services to be performed.
 - iii. The Foreign recipient **Contractor / Subcontractor** must identify an authorized Contract Security Officer (CSO) and an Alternate Contract Security Officer (ACSO) (if applicable) to be responsible for the overseeing of the security requirements, as defined in this **contract/subcontract**. This individual will be appointed by the proponent foreign recipient **Contractor's / Subcontractor's** Chief Executive officer or Designated Key Senior Official, defined as an owner, officer, director, executive, and or partner who occupy a position which would enable them to adversely affect the organization's policies or practices in the performance of the **contract/subcontract**.
 - iv. The foreign recipient **Contractor / Subcontractor** must not grant access to **CANADA PROTECTED B/Personal** information/assets, except to its personnel subject to the following conditions:
 - 1) Personnel have a need-to-know for the performance of the **contract/subcontract**;
 - 2) Personnel have been subject to a Criminal Record Check, with favorable results, from a recognized governmental agency or private sector

- organization in **their country** as well as a Background Verification, validated by the Canadian DSA;
- 3) The foreign recipient **Contractor / Subcontractor** must ensure that personnel provide consent to share results of the Criminal Record and Background Checks with the Canadian DSA and other Canadian Government Officials, if requested; and
 - 4) The Government of Canada reserves the right to deny access to **CANADA PROTECTED** information/assets to a foreign recipient **Contractor / Subcontractor** for cause.
- (iv) **CANADA PROTECTED/Personal** information/assets, provided to the foreign recipient **Contractor/Subcontractor** or produced by the Foreign recipient **Contractor/Subcontractor**, must:
- i. not be disclosed to another government, person or firm, or representative thereof not directly related to the performance of the **contract/subcontract**, without the prior written consent of Canada. Such consent must be sought from its national DPA, the Contracting Authority (in collaboration with the Canadian DSA); and
 - ii. not be used for any purpose other than for the performance of the **contract/subcontract** without the prior written approval Canada. This approval must be obtained by contacting its national DPA, the Contracting Authority (in collaboration with the Canadian DSA).
- (v) Until the Foreign recipient **Contractor / Subcontractor** has provided the Canadian DSA with the required written personnel security screening assurances, the Foreign recipient **Contractor / Subcontractor** personnel **MUST NOT HAVE ACCESS** to **CANADA PROTECTED A or B** information/assets, and **MUST NOT ENTER** "Government of Canada" or "Contractor" sites where such information/assets are kept, without an escort. An escort is defined as "a Government of Canada" or "Contractor" employee who holds the appropriate Personnel Security Clearance at the required level.
- (vi) The foreign recipient **Contractor / Subcontractor** must, at all times during the performance of the **contract/subcontract** hold an equivalence to an approved Document Safeguarding Capability (DSC) at the level of **CANADA PROTECTED B**. All **CANADA PROTECTED/Personal** information, furnished to the foreign recipient **Contractor / Subcontractor** or produced by the foreign recipient **Contractor / Subcontractor**, must also be safeguarded as follows:
- (vii) The foreign recipient **Contractor / Subcontractor** acknowledges and agrees that its obligations to safeguard, manage, and protect all Personal Information under the **contract / subcontract** are in addition to any obligations it has under national privacy legislation of the country(ies) in which it is incorporated or operates.
- (viii) The foreign recipient **Contractor / Subcontractor** **MUST NOT** remove **CANADA PROTECTED/Personal** information/assets from the identified work site(s), and the foreign recipient **Contractor / Subcontractor** must ensure that its personnel are made aware of and comply with this restriction.
- (ix) The foreign recipient **Contractor / Subcontractor** must not use the **CANADA PROTECTED/Personal** information/assets for any purpose other than for the

performance of the **contract** without the prior written approval of the Government of Canada. This approval must be obtained from the Canadian DSA.

- (x) The foreign recipient **Contractor / Subcontractor** must immediately report to the Canadian DSA all cases in which it is known or there is reason to suspect that **CANADA PROTECTED/Personal** information/ assets pursuant to this **contract** has been compromised.
- (xi) The foreign recipient **Contractor / Subcontractor** must immediately report to the Canadian DSA all cases in which it is known or there is reason to suspect that **CANADA PROTECTED/Personal** information/ assets accessed by the foreign recipient **Contractor / Subcontractor**, pursuant to this **contract**, have been lost or disclosed to unauthorized persons.
- (xii) The foreign recipient **Contractor / Subcontractor** must not disclose **CANADA PROTECTED/Personal** information/assets to a third party government, person, firm or representative thereof, without the prior written consent of the Government of Canada. Such consent must be sought through the Canadian DSA.
- (xiii) The foreign recipient **Contractor / Subcontractor** must provide the **CANADA PROTECTED/Personal** information/ assets a degree of safeguarding no less stringent than that provided by the Government of Canada in accordance with the National Policies, National Security legislation and regulations and as prescribed by the Canadian DSA.
- (xiv) Upon completion of the Work, the foreign recipient **Contractor / Subcontractor** must return to the Government of Canada, all **CANADA PROTECTED/Personal** information/assets furnished or produced pursuant to this **contract/subcontract**, including all **CANADA PROTECTED** information/ assets released to and/or produced by its subcontractors.
- (xv) The foreign recipient **Contractor / Subcontractor** requiring access to **CANADA PROTECTED/Personal** information/assets or Canadian restricted sites, under this contract, must submit a Request for Site Access to the Departmental Security Officer of Environment and Climate Change Canada.
- (xvi) The foreign recipient **Contractor / Subcontractor** MUST NOT utilize its Information Technology (IT) systems to electronically process, produce, or store on a computer system and transfer via an IT link any **CANADA PROTECTED B/Personal** information/assets until authorization to do so has been confirmed by the Canadian DSA.
- (xvii) The foreign recipient **Contractor / Subcontractor** must ensure that the appropriate security clauses, as determined by the Canadian DSA, are inserted in all subcontracts that involve access to **CANADA PROTECTED/Personal** information provided to or generated under this **contract/ subcontract** and must ensure that the conditions placed on a subcontractor are no less favorable to Canada than the conditions set out in these security requirements.
- (xviii) In the event that a foreign recipient **Contractor / Subcontractor** is chosen as a supplier for this **contract/subcontract**, subsequent country-specific foreign security requirement clauses must be generated and promulgated by the Canadian DSA, and provided to the Contracting Authority, to ensure compliance with the security provisions, as defined by the Canadian DSA, in relation to equivalencies.

-
- (xix) Subcontracts which contain security requirements are NOT to be awarded without the prior written permission of the Canadian DSA.
- (xx) The foreign recipient **Contractor / Subcontractor** must comply with the provisions of the Security Requirements Check List attached at Annex C.
- (xxi) Canada has the right to reject any request to electronically access, process, produce, transmit or store **CANADA PROTECTED/Personal** information/assets related to the Work in any other country if there is any reason to be concerned about the security, privacy, or integrity of the information.
- (c) **Protection and Security of Data Stored in Databases**
- (i) The foreign recipient **Contractor / Subcontractor** must ensure that all the databases used by organizations to provide the services described in the proposed Solution containing any **CANADA PROTECTED/Personal** information, related to the Work, are located in Canada.
- (ii) The foreign recipient **Contractor / Subcontractor** must control access to all databases on which any data relating to the **contract / subcontract** is stored so that only individuals with the appropriate security screening are able to access the database, either by using a password or other form of access control (such as biometric controls).
- (iii) The foreign recipient **Contractor / Subcontractor** must ensure that all databases on which any data relating to the **contract / subcontract** is stored are physically and logically independent (meaning there is no direct or indirect connection of any kind) from all other databases.
- (iv) The foreign recipient **Contractor / Subcontractor** must ensure that all data relating to the **contract/ subcontract** is processed only in Canada or in another country approved by the Contracting Authority under subsection 1.
- (v) The foreign recipient **Contractor / Subcontractor** must ensure that all domestic network traffic (meaning traffic or transmissions initiated in one part of Canada to a destination or individual located in another part of Canada) is routed exclusively through Canada, unless the Contracting Authority has first consented in writing to an alternate route. The Contracting Authority will only consider requests to route domestic traffic through another country that meets the requirements of subsection 1.
- (vi) Despite any section of the General Conditions relating to subcontracting, the foreign recipient **Contractor / Subcontractor** must not subcontract (including to an affiliate) any function that involves providing a subcontractor with access to any data relating to the contract unless the Contracting Authority (in collaboration with the Canadian DSA) first consents in writing.
- (d) **Personal Information**
- (i) **Interpretation**
- i. In the **contract / subcontract**, unless the context otherwise requires,
“General Conditions” means the general conditions that form part of the **contract / subcontract**;
“Personal Information” means information about an individual, including the types of information specifically described in the *Privacy Act*, R.S. 1985, c. P-21;

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

- ii. Words and expressions defined in the General Conditions and used in these supplemental general conditions have the meanings given to them in the General Conditions.
- iii. If there is any inconsistency between the General Conditions and these supplemental general conditions, the applicable provisions of these supplemental general conditions prevail.⁷

(e) Ownership of Personal Information and Record

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

(f) Use of Personal Information

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

(g) Collection of Personal Information

- (i) If the foreign recipient **Contractor / Subcontractor** must collect Personal Information from a third party to perform the Work, the foreign recipient **Contractor / Subcontractor** must only collect Personal Information that is required to perform the Work. The foreign recipient **Contractor / Subcontractor** must collect the Personal Information from the individual to whom it relates and the foreign recipient **Contractor / Subcontractor** must inform that individual (at or before the time when it collects the Personal Information) of the following:
 - i. that the Personal Information is being collected on behalf of, and will be provided to, Canada;
 - ii. the ways the Personal Information will be used;
 - iii. that the disclosure of the Personal Information is voluntary or, if there is a legal requirement to disclose the Personal Information, the basis of that legal requirement;
 - iv. the consequences, if any, of refusing to provide the information;
 - v. that the individual has a right to access and correct his or her own Personal Information; and
 - vi. that the Personal Information will form part of a specific personal information bank (within the meaning of the *Privacy Act*), and also provide the individual with information about which government institution controls that personal information bank, if the Contracting Authority has provided this information to the foreign recipient **Contractor / Subcontractor**.

-
- (ii) The foreign recipient Contractor, its subcontractors, 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.
 - (iii) If requested by the Contracting Authority, the foreign recipient **Contractor / Subcontractor** must develop a request for consent form to be used when collecting Personal Information, or a script for collecting the Personal Information by telephone. The foreign recipient **Contractor / Subcontractor** must not begin using the form or script unless the Contracting Authority first approves it in writing. The Contractor must also obtain the Contracting Authority's approval before making any changes to a form or script.
 - (iv) At the time it requests Personal Information from any individual, if the foreign recipient **Contractor / Subcontractor** doubts that the individual has the capacity to provide consent to the disclosure and use of his or her Personal Information, the foreign recipient **Contractor / Subcontractor** must ask the Contracting Security Authority for instructions.
- (h) **Maintaining the Accuracy, Privacy and Integrity of Personal Information**
- The foreign recipient **Contractor / Subcontractor** must ensure that the Personal Information is as accurate, complete, and up to date as possible. The foreign recipient **Contractor / Subcontractor** must protect the privacy of the Personal Information. To do so, at a minimum, the foreign recipient **Contractor / Subcontractor** must:
- (i) not use any personal identifiers (e.g. social insurance number) to link multiple databases containing Personal Information;
 - (ii) segregate all Records from the foreign recipient **Contractor's/Subcontractor's** own information and records;
 - (iii) 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);
 - (iv) provide training to anyone to whom the foreign recipient **Contractor / Subcontractor** will provide access to the Personal Information regarding the obligation to keep it confidential and use it only to perform the Work. The foreign recipient **Contractor / Subcontractor** must provide this training before giving an individual access to any Personal Information and the foreign recipient **Contractor / Subcontractor** must keep a record of the training and make it available to the Contracting Authority if requested;
 - (v) if requested by the Contracting Authority, before providing anyone with access to the Personal Information, require anyone to whom the foreign recipient **Contractor / Subcontractor** provides access to the Personal Information to acknowledge in writing (in a form approved by the Contracting Authority) their responsibilities to maintain the privacy of the Personal Information;
 - (vi) 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);
 - (vii) include a notation on any Record(s) that an individual has requested be corrected if the foreign recipient **Contractor / Subcontractor** has decided not to make the correction for any reason. Whenever this occurs, the foreign recipient **Contractor / Subcontractor** must immediately advise the Contracting Authority of the details of the requested correction and the reasons for the foreign recipient **Contractor's/Subcontractor's**

decision not to make it. If directed by the Contracting Authority to make the correction, the Contractor must do so;

- (viii) keep a record of the date and source of the last update to each Record;
- (ix) maintain an audit log that electronically records all instances of and attempts to access Records stored electronically. The audit log must be in a format that can be reviewed by the foreign recipient **Contractor / Subcontractor** and Canada at any time; and
- (x) secure and control access to any hard copy Records.

(i) **Safeguarding Personal Information**

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

- (i) 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;
- (ii) ensure that passwords or other access controls are provided only to individuals who require access to the Personal Information to perform the Work;
- (iii) not outsource the electronic storage of Personal Information to a third party (including an affiliate) unless the Canadian DSA has first consented in writing;
- (iv) 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;
- (v) maintain a secure back-up copy of all Records, updated at least weekly;
- (vi) implement any reasonable security or protection measures requested by Canada from time to time; and
- (vii) notify the Contracting Authority and the Canadian DSA immediately of any security breaches; for example, any time an unauthorized individual accesses any Personal Information.

(j) **Appointment of Privacy Officer**

The foreign recipient **Contractor / Subcontractor** must appoint someone to be its privacy officer and to act as its representative for all matters related to the Personal Information and the Records. The foreign recipient **Contractor / Subcontractor** must provide that person's name to the Contracting Authority and the Canadian DSA within ten (10) days of the award of the **Contract / subcontract**.

(k) **Quarterly Reporting Obligations**

Within 30 calendar days of the end of each quarter (January-March; April-June; July-September; October-December), the foreign recipient **Contractor / Subcontractor** must submit the following to the Contracting Authority:

- (i) a description of any new measures taken by the foreign recipient **Contractor / Subcontractor** to protect the Personal Information (for example, new software or access controls being used by the foreign recipient **Contractor / Subcontractor**);

- (ii) a list of any corrections made to Personal Information at the request of an individual (including the name of the individual, the date of the request, and the correction made);
- (iii) details of any complaints received from individuals about the way in which their Personal Information is being collected or handled by the **Contractor / Subcontractor**; and
- (iv) a complete copy (in an electronic format agreed to by the Contracting Authority and the foreign recipient **Contractor / Subcontractor**) of all the Personal Information stored electronically by the **contract / subcontract**.

(l) **Threat and Risk Assessment**

Within ninety (90) calendar days of the award of the **contract / subcontract** and, if the **contract/ subcontract** lasts longer than one year, within thirty (30) calendar days of each anniversary date of the **contract / subcontract**, the foreign recipient **Contractor / Subcontractor** must submit to the Contracting Authority and the Canadian DSA a threat and risk assessment, which must include:

- (i) a copy of the current version of any request for consent form or script being used by the foreign recipient **Contractor / Subcontractor** to collect Personal Information;
- (ii) a list of the types of Personal Information used by the foreign recipient **Contractor / Subcontractor** in connection with the Work;
- (iii) a list of all locations where hard copies of Personal Information are stored;
- (iv) a list of all locations where Personal Information in machine-readable format is stored (for example, the location where any server housing a database including any Personal Information is located), including back-ups;
- (v) a list of every person to whom the foreign recipient **Contractor / Subcontractor** has granted access to the Personal Information or the Records;
- (vi) a list of all measures being taken by the foreign recipient **Contractor / Subcontractor** to protect the Personal Information and the Records;
- (vii) a detailed explanation of any potential or actual threats to the Personal Information or any Record, together with an assessment of the risks created by these threats and the adequacy of existing safeguards to prevent these risks; and
- (viii) an explanation of any new measures the foreign recipient **Contractor / Subcontractor** intends to implement to safeguard the Personal Information and the Records.

(m) **Audit**

Canada may audit the foreign recipient **Contractor's/Subcontractor's** compliance with these supplemental general conditions at any time. If requested by the Contracting Authority, the foreign recipient **Contractor / Subcontractor** must provide Canada (or Canada's authorized representative) with access to its premises and to the Personal Information and Records at all reasonable times. If Canada identifies any deficiencies during an audit, the foreign recipient **Contractor / Subcontractor** must immediately correct the deficiencies at its own expense.

(n) **Statutory Obligations**

- (i) The foreign recipient **Contractor / Subcontractor** acknowledges that Canada is required to handle the Personal Information and the Records in accordance with the provisions of Canada's *Privacy Act*, *Access to Information Act*, R.S. 1985, c. A-1, and *Library and Archives of Canada Act*, S.C. 2004, c. 11. The foreign recipient **Contractor / Subcontractor** agrees to comply with any requirement established by the Contracting

Authority that is reasonably required to ensure that Canada meets its obligations under these acts and any other legislation in effect from time to time.

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

(o) **Disposing of Records and Returning Records to Canada**

The foreign recipient **Contractor / Subcontractor** must not dispose of any Record, except as instructed by the Contracting Authority. On request by the Contracting Authority, or once the Work involving the Personal Information is complete, the **contract / subcontract** is complete, or the **contract / subcontract** is terminated, whichever of these comes first, the foreign recipient **Contractor / Subcontractor** must return all Records (including all copies) to the Contracting Authority.

(p) **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 / Subcontractor** must immediately notify the Contracting Authority, in order to provide the Contracting Authority with an opportunity to participate in any relevant proceedings.

(q) **Complaints**

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

(r) **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 subcontractors, agents, or representatives, or any of their employees.

7.19 Contractor's Sites or Premises Requiring Safeguarding Measures

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

Street Number / Street Name, Unit / Suite / Apartment Number

City, Province, Territory / State

Postal Code / Zip Code

Country

The Company Security Officer must ensure through the [Contract Security Program](#) that the Contractor and individuals hold a valid security clearance at the required level of document safeguarding capability.

7.20 Basis of Payment

- (a) **Phase 1 – Prototype Solution:** For the Work described in article 2. Phase 1 – Prototype Solution of Annex A – Statement of Work. In consideration of the Contractor satisfactorily completing its obligations under the Contract, the Contractor will be paid a firm lot price(s) in accordance with Annex B – Basis of Payment, in Canadian funds, customs duty included, Goods and Services Tax or Harmonized Sales Tax is extra, if applicable.
- (b) **Optional Phase 2 – Solution:** At Canada's sole discretion, Canada may exercise the irrevocable option to deliver the production-ready Solution in accordance with article 3. Phase 2 - Solution of Annex A – Statement of Work. If Canada exercises this irrevocable option, and in consideration of the Contractor satisfactorily completing its obligations under the Contract, the Contractor will be paid a firm lot price(s) in accordance with Annex B – Basis of Payment, in Canadian funds, customs duty included, Goods and Services Tax or Harmonized Sales Tax is extra, if applicable.
- (c) **Optional Annual Software as a Service Subscription Solution Authorized User Access:** At Canada's sole discretion, Canada may exercise the irrevocable option to deliver Annual Software as a Service Subscription Solution Access. If Canada exercises this irrevocable option, and in consideration of the Contractor satisfactorily completing its obligations under the Contract, the Contractor will be paid a firm lot price(s) in accordance with Annex B – Basis of Payment, in Canadian funds, customs duty included, Goods and Services Tax or Harmonized Sales Tax is extra, if applicable.
- (d) **Optional Professional Services provided under a Task Authorization with a Firm Price:** For professional services requested by Canada, in accordance with a validly issued Task Authorization, Canada will pay the Contractor, in arrears, the firm price per Deliverable (travel and living expenses excluded), as set out in the Task Authorization, applicable Taxes extra and any resulting deliverables in accordance with the firm per diem rates set out in Annex B, Basis of Payment. Partial days will be prorated based on actual hours worked based on a 7.5-hour workday.
- (e) **Optional Training Services provided under a Task Authorization with a Firm Price:** For training services requested by Canada, in accordance with a validly issued Task Authorization, Canada will pay the Contractor, in arrears, the firm price per Deliverable (travel and living expenses excluded), as set out in the Task Authorization, Applicable Taxes extra and any resulting deliverables in accordance with the firm per diem rates set out in Annex B, Basis of Payment. Partial days will be prorated based on actual hours worked based on a 7.5-hour workday.
- (f) **Travel and Living Expenses – National Joint Council Travel Directive:** The Contractor will be reimbursed its authorized travel and living expenses reasonably and properly incurred in the performance of the Work, at cost, without any allowance for profit and/or administrative overhead, in accordance with the meal, and private vehicle allowances specified in Appendices B, C and D of the [National Joint Council Travel Directive](#), and with the other provisions of the directive referring to "travellers", rather than those referring to "employees". Canada will not pay the Contractor any incidental expense allowance for authorized travel.
 - (i) All travel must have the prior authorization of the Technical Authority.
 - (ii) All payments are subject to government audit.

- (g) **Limitation of Price.** 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.
- (h) **Limitation of Expenditure – Professional Services provided under a Task Authorization**
- (i) Canada's total liability to the Contractor under the Contract for all authorized Task Authorizations (Task), inclusive of any revisions, must not exceed the sum of \$ _____ *(to be inserted at contract award)*. Customs duties are included and Applicable Taxes are extra.
- (ii) No increase in the total liability of Canada will be authorized or paid to the Contractor unless an increase has been approved, in writing, by the Contracting Authority.
- (iii) The Contractor must notify the Contracting Authority in writing as to the adequacy of this sum:
- (1) when it is 75 percent committed, or
 - (2) four (4) months before the contract expiry date, or
 - (3) as soon as the Contractor considers that the sum is inadequate for the completion of the Work required in all authorized Task, inclusive of any revisions, whichever comes first.
- (iv) If the notification is for inadequate contract funds, the Contractor must provide to the Contracting Authority, a written estimate for the additional funds required. Provision of such information by the Contractor does not increase Canada's liability.
- (i) **Limitation of Expenditure – Training provided under a Task Authorization**
- (i) Canada's total liability to the Contractor under the Contract for all authorized Task Authorizations (Task), inclusive of any revisions, must not exceed the sum of \$ _____ *(to be inserted at contract award)*. Customs duties are included and Applicable Taxes are extra.
- (ii) No increase in the total liability of Canada will be authorized or paid to the Contractor unless an increase has been approved, in writing, by the Contracting Authority.
- (iii) The Contractor must notify the Contracting Authority in writing as to the adequacy of this sum:
- i. when it is 75 percent committed, or
 - ii. four (4) months before the contract expiry date, or
 - iii. as soon as the Contractor considers that the sum is inadequate for the completion of the Work required in all authorized Task, inclusive of any revisions, whichever comes first.
- (iv) If the notification is for inadequate contract funds, the Contractor must provide to the Contracting Authority, a written estimate for the additional funds required. Provision of such information by the Contractor does not increase Canada's liability.

7.21 Method of Payment

(a) **Single Payment – Phase 1 – Prototype Solution**

Canada will pay the Contractor upon completion and delivery of the Work in accordance with the payment provisions of the Contract if:

- (i) an accurate and complete invoice and any other documents required by the Contract have been submitted in accordance with the invoicing instructions provided in the Contract;
- (ii) all such documents have been verified by Canada;
- (iii) the Work delivered has been accepted by Canada.

(b) Monthly Payment – Optional Phase 2 - Solution

At Canada's sole discretion, Canada may exercise the irrevocable option for the Contractor to perform Work in accordance with article 3. Phase 2 - Solution of Annex A – Statement of Work. If Canada exercises this irrevocable option, Canada will pay the Contractor on a monthly basis for work performed during the month covered by the invoice in accordance with the payment provisions of the Contract if:

- (i) an accurate and complete invoice and any other documents required by the Contract have been submitted in accordance with the invoicing instructions provided in the Contract;
- (ii) all such documents have been verified by Canada; and
- (iii) the Work performed has been accepted by Canada.

(c) Monthly Payment – Optional Annual Software as a Service Subscription Solution Authorized User Access

At Canada's sole discretion, Canada may exercise the irrevocable option to deliver Authorized User Access to the Solution. If Canada exercises this irrevocable option, Canada will pay the Contractor on a monthly basis for work performed during the month covered by the invoice in accordance with the payment provisions of the Contract if:

- (i) an accurate and complete invoice and any other documents required by the Contract have been submitted in accordance with the invoicing instructions provided in the Contract;
- (ii) all such documents have been verified by Canada; and
- (iii) the Work performed has been accepted by Canada.

(d) Monthly Payment – Task Authorized Optional Professional Services with a Firm Price

Canada will pay the Contractor on a monthly basis for work performed during the month covered by the invoice in accordance with the payment provisions of the Contract if:

- (i) an accurate and complete invoice and any other documents required by the Contract have been submitted in accordance with the invoicing instructions provided in the Contract;
- (ii) all such documents have been verified by Canada; and
- (iii) the Work performed has been accepted by Canada.

(e) Monthly Payment – Task Authorized Optional Training Services with a Firm Price

Canada will pay the Contractor on a monthly basis for work performed during the month covered by the invoice in accordance with the payment provisions of the Contract if:

- (i) an accurate and complete invoice and any other documents required by the Contract have been submitted in accordance with the invoicing instructions provided in the Contract;
- (ii) all such documents have been verified by Canada; and
- (iii) the Work performed has been accepted by Canada.

7.22 Invoicing

- (a) **Invoice Submission.** The Contractor must submit invoices for the Services and delivery of any Work, as applicable.

- (b) **Invoice Requirements.** Invoices must be submitted in the Contractor's name and contain:
- (i) the date, the name and address of the client department, item or reference numbers, deliverable/description of the Work, contract number, Client Reference Number (CRN), Procurement Business Number (PBN), and financial code(s);
 - (ii) 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;

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

7.23 Taxes

- (a) **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.
- (b) **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.
- (c) **Foreign-based Contractor.** Unless specified otherwise in the Contract, the price includes no amount for any federal excise tax, state or local sales or use tax, or any other tax of a similar nature, or any Canadian tax whatsoever. The price, however, includes all other taxes. If the Work is normally subject to federal excise tax, Canada will, upon request, provide the Contractor a certificate of exemption from such federal excise tax in the form prescribed by the federal regulations.
- (d) Canada will provide the Contractor evidence of export that may be requested by the tax authorities. If, as a result of Canada's failure to do so, the Contractor has to pay federal excise tax, Canada will reimburse the Contractor if the Contractor takes such steps as Canada may require to recover any payment made by the Contractor. The Contractor must refund to Canada any amount so recovered.
- (e) **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.
- (f) **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.
- (g) **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.
- (h) **Electronic Payment of Invoices – Contract**

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

- (i) Visa Acquisition Card;
- (ii) MasterCard Acquisition Card;
- (iii) Direct Deposit (Domestic and International);
- (iv) Electronic Data Interchange (EDI);
- (v) Wire Transfer (International Only);
- (vi) Large Value Transfer System (LVTS) (Over \$25M)

7.24 Certifications and Additional Information

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

7.25 Federal Contractors Program for Employment Equity – Default by 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.

7.26 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.

7.27 Limitation of Liability

Except as expressly provided in paragraph (b), the Contractor is liable to Canada for all direct damages it causes in performing or failing to perform the Contract in relation to:

- (a) The Contractor's acts or omissions under the Contract affecting real or tangible personal property owned, possessed or occupied by Canada;
- (b) The Contractor's breach of confidentiality obligations under the Contract, but such limitation does not apply to the disclosure by Contractor of the trade secrets of Canada or a third party related to information technology;
- (c) Liens or encumbrances relating to any portion of the Work under the Contract, not including claims or encumbrances relating to intellectual property rights; and
- (d) Contractors breach of warranty obligations;

However, the Contractor is not liable to Canada for indirect, special or consequential damages caused by items (a) to (d) above.

With respect to direct damages related to the Contractor's breach of warranty obligations, the Contractor's maximum liability to Canada is the total estimated cost of the Contract (meaning the dollar amount shown on the first page of the Contract in the block titled "**Total Estimated Cost**"). All direct damages not listed above that do not relate to breach of warranty are subject to a maximum of .25 times the Total Estimated Cost or \$1M, whichever is greater.

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

None of the above limitations apply to damages based on loss of life or injury or claims based on infringement of intellectual property.

7.28 General Provisions

- (a) **Applicable Laws.** This Contract will be interpreted and governed by the laws of Ontario.
- (b) **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.
- (c) **Severability.** If any provision of this Contract is declared unenforceable by an authoritative court, the remainder of this Contract will remain in force.
- (d) **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.
- (e) **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.
- (f) **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).
- (g) **International Sanctions.**
 - (i) 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](#).
 - (ii) The Contractor must not supply to the Government of Canada any goods or services which are subject to economic sanctions.

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.
- (h) **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 Services and Procurement Canada's website at [Ineligibility and Suspension Policy](#).

- (i) **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.
- (j) **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.

7.29 Authorities

(a) Contracting Authority

The Contracting Authority for the Contract is:

Name: **Wesley Fenwick**
Title: A/Supply Specialist
Organization: Public Services and Procurement Canada, Acquisitions Branch
Directorate: Software Procurement Directorate
Address: 10 Rue Wellington, Gatineau, QC K1A 0S5
Telephone: 613-720-7743
E-mail address: wesley.fenwick@tpsgc-pwgsc.gc.ca

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

(b) Technical Authority – Canada School of Public Service

Will be added at Contract Award.

Name: _____
Title: _____
Organization: _____
Address: _____
Telephone: _____
Facsimile: _____
E-mail address: _____

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.

7.30 Proactive Disclosure of Contracts with Former Public Servants

By providing information on its status, with respect to being a former public servant in receipt of a Public Service Superannuation Act (PSSA) pension, the Contractor has agreed that this information will be reported on departmental web sites as part of the published proactive disclosure reports, in accordance with Contracting Policy Notice: 2012-2 of the Treasury Board Secretariat of Canada.

7.31 Priority of Documents

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

- (a) these Articles of Agreement, including any individual SACC Manual clauses incorporated by reference in these Articles of Agreement;
- (b) the general conditions 2035 (2018-06-21) General Conditions – Higher Complexity – Services
- (c) the supplemental general conditions, in the following order:
 - (i) 4008, (2008-12-12) Personal Information
- (d) Annex A – Statement of Work
- (e) Annex B – Basis of Payment
- (f) Annex C – Security Requirement Check List
- (g) Annex D – Definitions and Interpretations
- (h) Annex E – Privacy Obligations
- (i) Annex F – Task Authorization Forms
- (j) Annex G – Bid Evaluation Criteria
- (k) Annex H – Bidder Forms
- (l) Annex I – Security Control Profile
- (m) the signed Task Authorizations and any Certifications as required;
- (n) the Contractor's bid dated _____ (*insert date of bid*) not including any software publisher license terms and conditions that may be included in the bid, not including any provisions in the bid with respect to limitations on liability, and not including any terms and conditions incorporated by reference (including by way of a web link) in the bid.

7.32 Joint Venture Contractor

- (a) The Contractor confirms that the name of the joint venture is _____ and that it is comprised of the following members:
- (b) With respect to the relationship among the members of the joint venture Contractor, each member agrees, represents and warrants (as applicable) that:
 - (i) _____ has been appointed as the “representative member” of the joint venture Contractor and has full authority to act as agent for each member regarding all matters relating to the Contract;

-
- (ii) by giving notice to the representative member, Canada will be considered to have given notice to all the members of the joint venture Contractor; and
 - (iii) all payments made by Canada to the representative member will act as a release by all the members.
 - (c) All the members agree that Canada may terminate the Contract in its discretion if there is a dispute among the members that, in Canada's opinion, affects the performance of the Work in any way.
 - (d) All the members are jointly and severally or solidarily liable for the performance of the entire Contract.
 - (e) The Contractor acknowledges that any change in the membership of the joint venture (i.e., a change in the number of members or the substitution of another legal entity for an existing member) constitutes an assignment and is subject to the assignment provisions of the General Conditions.
 - (f) The Contractor acknowledges that all security and controlled goods requirements in the Contract, if any, apply to each member of the joint venture Contractor.

Note to Bidders: *This Article will be deleted if the Bidder awarded the contract is not a joint venture. If the contractor is a joint venture, this clause will be completed with information provided in its bid.*

ANNEX A

STATEMENT OF WORK

1. INTRODUCTION

1.1 TITLE

- a) Next Generation Digital Learning Environment (NGDLE) Solution, referred to hereafter as the "Solution."

1.2 BACKGROUND

- a) The Canada School of Public Service's (hereafter, "the School") mandate is to provide a broad range of learning activities to build individual, professional, and organizational capacity, and management excellence across the federal public service. The School is responsible for learning that is common across all federal departments. This includes supporting a public-service-wide culture of learning that is relevant, responsive, accessible, and supportive of broader government objectives. Also included are core and common learning, such as public service orientation, learning shared by professional communities, such as HR and Finance specialists, and learning linked to job functions, such as supervisors, managers and executives.
- b) The School's client base covers an estimated 260,000 individual public servants who must be served in both official languages (English and French) across Canada. These public servants belong to separate departments, agencies and crown corporations.
- c) In December 2014, the School launched GCcampus, as a public service-wide learning portal to enhance the learner experience, integrating its existing learning management system with a web content management system, distance learning platform, and video/media platform accessed through a single sign-on.
- d) The portal provides public servants with access to formal and informal learning such as:
 - i) self-paced e-learning;
 - ii) cohort-based distance learning;
 - iii) live and recorded event webcasts;
 - iv) videos;
 - v) blogs;
 - vi) podcasts;
 - vii) micro-learning;
 - viii) virtual classroom deliveries;
 - ix) classroom and event catalogues;
 - x) online registration;
 - xi) a wide range of 3rd party-sourced content; and
 - xii) an environment for learning coordinators to schedule and register learners and courses.

1.3 SCOPE OF WORK

- a) The Canada School of Public Service (School) is seeking a Next Generation Digital Learning Environment (NGDLE) Solution to succeed its current Learning Management System.
- b) The School desires a Solution that has the flexibility and capability to meet current and future business functions and integrates those functions into a single web-based digital environment.

- c) The Solution will host digital learning content and information about virtual and in-person workshops, courses and events in a variety of subject areas that may come from multiple sources, including the School, other government departments, and third-party vendors. The primary users of the Solution will include over 260,000 public service employees across Canada and worldwide.
- d) **Out of Scope.** Learning content is outside the scope of this solicitation. For the School, learning content is currently sourced from 3rd-party suppliers, other government departments, or developed in-house by the School. However, there is still a requirement to connect to 3rd-party content providers.

1.4 OBJECTIVES

- a) The School is seeking a cloud-based Software as a Service (SaaS) Next Generation Digital Learning Environment (NGDLE) Solution that enables the School to fulfil its mandate, carry out core business operations related to the design and delivery of learning products, and provide public servants with interactive and open online resources, videos, in-person and virtual courses, seminars and events to support the School's approach to learning, accessible any time and from anywhere.
- b) Through the NGDLE, the School is looking to make improvements in usability, functional, technical and services attributes, as well as to reduce overall operating costs of managing the current multi-platform learning ecosystem.
- c) Specifically, the School requires an innovative and modern Solution that must:
 - i) Provide learners with modern, user-friendly learning experiences, minimal logins, access to integrated catalogues, and comprehensive, federated search of content.
 - ii) Provide the School faculty, course designers and various stakeholders with modern, rapid learning self-service authoring tools, with role-based function that enables editing and publishing of content.
 - iii) Maintain secure learner data records that provide evidence of learning progress, completions, and certifications that uses API to interoperate with other central agency systems as well departmental learning management systems.
 - iv) Provide integrated tools to manage learning delivery resources (such as facilities, rooms, instructors and course materials) associated with online, in-person and blended/hybrid offerings.
 - v) Enable system integrations with other tools in the School learning ecosystem, as well as external platforms. (ex: third party commercial off the shelf content)
 - vi) Provide, real time, readily available analytics related to learners, operations, business metrics, audit management and system metrics.
 - vii) Provide personalized, automated, immediate feedback, recommendations and content to learners in order to rapidly match learners with content that is relevant to learner interests and their professional development needs.
- d) The School also has identified an as-and when requested need for the following services:
 - i) Professional Services for implementation, and data migration, as well as others on an as-and-when requested basis
 - ii) Training Services for end-users and administrators on an as-and-when requested basis.

1.5 CURRENT SCHOOL LEARNING ECOSYSTEM

a) GCcampus, the existing School core business learning ecosystem and platform, has been architected in-house using a suite of software and hardware technology infrastructure. It has a Service-Oriented Architecture (SOA) implemented with an Enterprise Service Bus (ESB) which enables the integration of all its components (COTS, Open source, custom code).

b) Specifically, it is currently configured for:

- **Users:**
 - To support a **300,000** user base infrastructure capacity scalable to 500,000;
 - **2,203** (active) non-learner accounts (admins, RTC, teacher...)
 - **112,396** Terminated accounts (kept for record keeping policy)
 - **138,108** People have completed at least 1 activity within the last year (including face to face and online learning products)
 - An average of **4,000** user sessions per day with peaks at **4,500** user sessions per day.
 - An average of **5,000** unique active users (consuming online learning activities) per month with peaks up to **10,000**.

- **Learning objects:**
 - Online self-paced: mostly SCORM (Shareable Content Object Reference Model) packages.
 - Number: 4,600
 - Size: 98 GB
 - Videos
 - Number: 727
 - Size: 1.2 TB (each video is stored in many resolutions)
 - Distance Learnings
 - Number: 3 increasing to 98 by the end of 2019;
 - Size : 21 GB (12 GB of files and 9 GB portal data)
 - Microlearning
 - Number: 7,600 media files (SCORM, doc, pdf, jpg, png...)
 - Size : 95 GB (84 GB of files and 11 GB of portal data)

c) Below is a summary of the current utilization of the existing learning ecosystem at the School from April 2018 to March 2019.

Delivery Mode	Enrollments	Access	Volume of Data on System
Classroom (in-person and virtual)	31,693	n/a	n/a
Event (in person and virtual)	51,406	n/a	n/a
Videos	n/a	36,195	1.2 TB
Self-Paced E-Learning	420,988	n/a	96 GB
Distance Learning	895	12,196 (July 2018 to June 2019)	< 21 GB
Micro-learning (blog, case studies, job aids)	n/a	28,408	17 MB
Overall User Portal	n/a	1,444,365	n/a

- d) The current GCcampus infrastructure includes:
- The SABA application version 7.3, a Commercial Off the Shelf (COTS) learning management system (LMS) that houses all SCORM content and all learner records;
 - Moodle version 3.5, an open-source software learning management / course management system is used as the course Management System and for social/distance course delivery;
 - Drupal, version 7, an open source content management system which is the web portal and front end interface to the learning portal; and
 - Kaltura Community Edition version 9.18.0 which houses and streams all video content; and

- other products along with internally developed custom software.

e) The School's production environment has a wide variety of servers and supported technologies.

The following system software is part of the School's production environment:

- Windows Server 2008 R2
- Microsoft IIS 7.5
- SQL Server 2008r2

For the Saba Learning Management System (LMS):

- RedHat Linux 6.4
- Apache 2.4
- JBOSS CE 6
- Oracle 11G

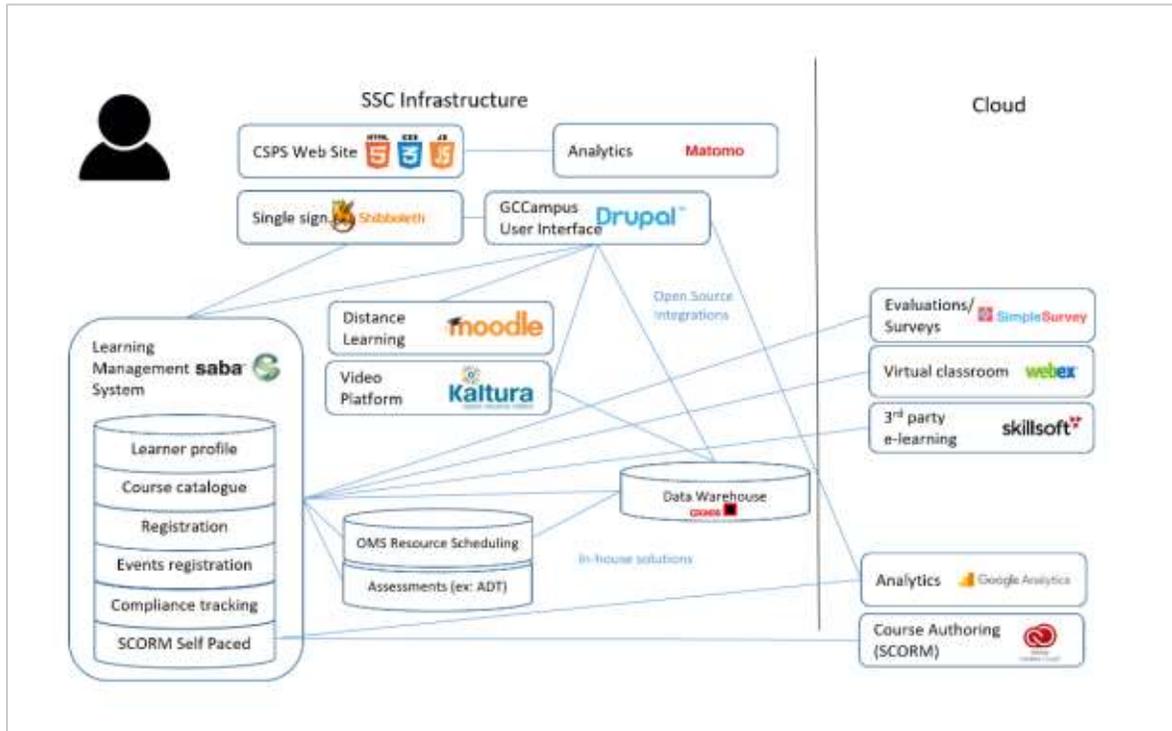
Others:

- Apache 2.4.6
- MySQL 5.1
- PHP 5.5.1.4
- Shibboleth Service Provider 2.5
- Tomcat 7

These systems are largely on-premise installations hosted on Shared Services Canada servers. Shared Services Canada provides high speed access to the internet.

- f) In addition, the School uses a range of SaaS cloud-based learning technologies/platforms, including:
- Webex Training Centre and Events Centre for virtual classroom sessions;
 - Simple Survey for course and event evaluations;
 - Skillsoft and other third-party content suppliers for commercial, off the shelf e-learning courses and other learning products.
 - Matomo Web Analytics.
 - A range of third-party authoring tools to develop SCORM self-paced e-learning content.

Current School Learning Ecosystem Architecture



1.6 ESTIMATED SOLUTION VOLUME

The School projects the following usage estimates over the lifespan of the resulting Contract.

- a) Estimated Authorized User access
 - i) CSPA estimates a requirement of 150,000 Authorized Users to access the Solution in the initial period, with an estimated growth of up to 500,000 Authorized Users.
- b) Estimated Concurrent Authorized User access
 - i) CSPA estimates a requirement of an average of 5,000 concurrent Authorized Users per month, with peaks of up to 10,000 concurrent Authorized Users per month.
- c) Role-based Authorized Users
 - i) CSPA estimates a requirement of 2,500 Role-based Authorized User access (ie. CSPA Solution administrators, instructors, content creators, etc.) to the Solution.
- d) Estimated Web Sessions
 - i) CSPA estimates a total traffic volume on public-facing web pages of 1.5 million Web Sessions per year, with an estimated growth of up to 3 million Web Sessions per year.
- e) Estimated Data Storage
 - i) CSPA estimates Solution data storage to be 1.4 Terabytes (TB), with an estimated growth of up to 32 TB of data.
- f) CSPA estimates there may be additional public-facing web page and content catalogue access traffic to the Solution

2. PHASE 1 – PROTOTYPE SOLUTION

2.1 SCOPE OF WORK

- a) Planning, design, and delivery of a fully featured, hosted, cloud-based, SaaS Solution Prototype supporting up to 200 users, in accordance with the required technical, functional, official languages, usability and accessibility requirements. This also includes a detailed Solution Comprehensive Product Plan and a detailed Solution Technical Infrastructure Design and Implementation Plan.

2.2 REQUIREMENTS

The Prototype Solution must include the following functionalities:

- a) Flexibility across access points for learning, whether in formally structured face-to-face, hybrid and flipped, or fully online learning, and whether for certification-seeking learners, self-directed learners, community-based social learning, or open educational resources.
- b) Compatibility with external 3rd party e-learning content suppliers via single sign-on.
- c) Cloud-based Software-as-a-Service (SaaS) hosted entirely on servers residing on Canadian soil.
- d) Hosting, registration, tracking and reporting of online learning content of various modalities (synchronous and asynchronous)
- e) Registration, tracking and reporting of face-to-face events and classroom sessions;
- f) Allow limitation of course and content availability by member entities/tenants in an extended enterprise with multiple business lines/ tenants.
- g) User interfaces, documentation and support available in both of Canada's official languages (English and French).
- h) A modern user interface with easy and intuitive navigation, including:
 - Tools for learners to browse, search and find content, contribute content, view personal learning, training requirements, progress towards completion, personalized learning plans/recommendations, view and print their own training transcript and certificates (includes completion date, exam scores, certification credits, etc.) in real time.
 - Tools for immediate supervisors and their managers to evaluate skills, manage roles, and assign specific learning content to people that have skill gaps; view dashboards of all team members and drill down to view skills, profile information, transcripts, certifications, training requirements and progress towards completion, and other individual user information and learning activities of their team members, create and run reports of team's member status of required learning, view, approve, and assign required or recommended trainings to their team members individually or as a group.
 - Tools for asynchronous online course designers to design and build effective, engaging digital learning experiences, including tools for multimedia content (video, audio);
 - Tools for faculty/instructors in synchronous courses to design and build effective, engaging digital in-person learning experiences (web conferencing, screen sharing, discussion forums);
 - Tools for School administrators to:
 - (i) create, find, view, or update user information, and unified password management;
 - (ii) enter and update course properties, perform classroom management, track and view completion/test results for learning events, and manually mark completion for all learners;
 - (iii) create repeatable sessions based on a standard course template and the ability to assign multiple courses to multiple users and groups simultaneously is required;
 - (iv) perform user, manager, and instructor management tasks for tenant domains.
- i) A mobile-friendly, responsive design that supports all major functions of the Solution across all common mobile platforms.
- j) Personalized learning experiences for learners such as: automated learning recommendations; and allow for user-generated rankings and ratings of learning content.
- k) Provide modern learning experiences to learners, including gamification, video content, micro-

learning, user generated/co-created and curated content based on learner attributes/preferences.

- l) Support badges and leaderboards for course, skill, and competency completion and display badges in a user-friendly format.
- m) Support the following common learning technology standards: Learning Tools Interoperability (LTI) 1.0 and 1.1, Shareable Content Object Reference Model (SCORM) 1.2 and 2004.
- n) Must incorporate a Learner Record Store (LRS) implementing xAPI/Tin Can.
- o) Available and accessible to individuals with disabilities, compliant with WCAG 2.0 A accessibility standards.

2.3 DELIVERABLES

The Contractor must deliver the following items to the Client Technical Authority:

- a) 1 Prototype Solution, which must include:
 - (1) Access for 200 Authorized Users, which all Solution usage rights grants, Software Documentation, Warranty, Hosting and Maintenance and Support (excluding Training), waivers, non-disclosure agreements, or other releases to Canada
 - (2) Support documentation or help files for each Use Case (scenario)
- b) 1 Comprehensive Project Plan, which must include:
 - (1) 1 Project Implementation Plan: Detailed listing of Stages, tasks and subtasks for the entire Project that including: start and completion dates, responsibility, and predecessors. Tasks to include all implementation activity, deadlines, milestones, draft deliverables, review periods, final deliverables and sign offs.
 - (a) 1 Communication Plan
 - (b) 1 Risk Management/Mitigation Plan
 - (c) 1 Transition Plan
 - (d) 1 Change Management Plan
 - (e) 1 On-going Communication, Coordination, and Project Status Reports
- c) 1 Technical Infrastructure Design and Implementation Plan, which must include:
 - (1) Design for hosted environments proposed by the Contractor, containing at a minimum detailed information on:
 - (2) Methodology, tools, procedures, activities, and services
 - (3) Security infrastructure and services (identify, protective, monitoring/detective, and responsive/recovery)
 - (4) Network and connectivity
 - (5) Performance characteristics
 - (6) Availability and flexibility requirements.

Table 1 – Phase 1 Deliverable Schedule

Deliverable	Description of Deliverable	Delivery Date
1	1 Prototype Solution (including access for up to 200 Active Users)	6 Weeks after date of Contract Award
2	1 Comprehensive Project Plan, digital copy delivered to Client Technical Authority	6 Weeks after date of Contract Award
3	1 Technical Infrastructure Design and Implementation Plan, digital copy delivered to Client Technical Authority	6 Weeks after date of Contract Award

2.4 CAPABILITY AND USABILITY ASSESSMENT (CUA)

- a) A Capability and Usability Assessment will be conducted on the Prototype Solution in accordance with Appendix A – Capability and Usability Assessment.

2.5 LOCATION/TRAVEL

- a) Location of work is at the Contractor's facility. No travel is anticipated.

3. PHASE 2 – SOLUTION

All Work listed under article 3. Phase 2 – Solution is subject to and contingent upon, at Canada's sole discretion, Canada's decision to exercise the irrevocable option under article 7.1 c) i) in the Contract to authorize the Contractor to perform all or a portion of the Work as described under article 3. Phase 2 Solution of Annex A – Statement of Work.

3.1 SCOPE OF WORK

- a) To fully implement a fully functional, hosted, cloud-based SaaS Solution with the ability to support digital learning and development, including planning design, delivery, training materials, help desk strategies and personnel, professional training services, and operation on on-going technical support of Phase 2 will include the planning, design, delivery and operation on on-going technical support of a fully functional, hosted, cloud-based SaaS platform with the ability to support digital learning and development for 260,000 full-time employees, and an average of 5,000 monthly active users at all levels nationwide and across 93 federal departments and agencies, as well as external "guest" users accessing openly available learning content.

3.2 REQUIREMENTS

- a) The Solution must include the functional requirements listed in Section 2.2 Requirements of the Statement of Work, and must also include the following additional functionality:
- i. A cloud-based solution that is the platform and device-agnostic, accessible by all users, including system administrators, without the need for any additional software installation.
 - ii. Compatible and capable of integrating with internal School learning ecosystem systems or providing equivalent functionality, including Kaltura, Moodle, WebEx, and SimpleSurvey.
 - iii. All upgrades, including regulatory updates, at no additional cost.
 - iv. The Solution service must scale to at least 260,000 Authorized Users and allow for scalability of up to 500,000 Authorized Users over the lifespan of the Contract.
 - v. The Solution must be able to scale to 500,000 Authorized Users and must address variable numbers of concurrent users.
 - vi. Single sign-on integration support via SAML/OpenID Connect.
 - vii. Multiple SaaS environments (Pre-production, Testing, Production, training) hosted in a secure data centre environment in Canada;
 - viii. Multi-tenancy configurations with granular access, individual branding and security.
 - ix. Must allow the School to configure and maintain a mixed catalogue of open by default and closed/private learning content including:
 - x. Solution Content visible on the internet based on public or restricted profiles.
 - xi. Must allow the School to offer and manage learning products, learning programs and curricula for internal (federal public servants) and external audiences that are dispersed

- geographically across multiple time zones; and
- xii. All data processed, stored and maintained in the Solution, including all online storage as well as data backups and archived data, must reside in Canada.

3.3 DELIVERABLES

- a) The School is aware of the level of effort required for a successful Solution implementation. The School also understands the importance of a disciplined implementation that includes services for project management, system design configurations, deployment, documentation, testing, training and end-user support. The School also desires a Solution where the Contractor must configure and provide of on-going support for the fully-functional Solution, including:
- i. Providing in-depth as-and-when requested consultation regarding best practices and process efficiencies, ensuring a successful integration with the School's processes, procedures and technology environment;
 - ii. Providing as-and-when requested training and training materials for end users and administrators
 - iii. Providing support to ensure the School maximizes both the use and cost effectiveness of the Solution.
- b) To ensure the success of the implementation of the Solution, the project will include, at minimum, the following implementation deliverables. The creation of each deliverable is the responsibility of the Contractor and must be formally presented to the School for review and acceptance. For milestones with multiple stages, each stage is expected to contain each deliverable (unless noted otherwise).

The Contractor must provide the following deliverables:

- i) 1 fully-functional, hosted, cloud-based SaaS NGDLE Solution with the ability to support digital learning and development for 260,000 full-time employees, and an average of 5,000 monthly active users at all levels nationwide and across 93 federal departments and agencies, as well as external "guest" users accessing openly available learning content, including Solution access for up to 260,000 initial Authorized Users which includes all Solution usage rights grants, Software Documentation, Warranty, Hosting and Maintenance and Support (excluding Training), waivers, non-disclosure agreements, or other releases to Canada.
- ii) Comprehensive Project Plan, including:
 - (1) Project Implementation Plan: Detailed listing of Stages, tasks and subtasks for the entire Project that including: start and completion dates, responsibility, and predecessors. Tasks to include all implementation activity, deadlines, milestones, draft deliverables, review periods, final deliverables and sign offs.
- iii) Communication Plan
- iv) Risk Management/Mitigation Plan
- v) Transition Plan
- vi) Change Management Plan
- vii) On-Going Communication, Coordination, and Project Status Reports
 - (1) Reports to be created and delivered on an as-and-when requested basis
- viii) Technical Infrastructure Design and Implementation Plan

- (1) Design for hosted environments proposed by the Contractor, containing at a minimum detailed information on:
 - (A) Methodology, tools, procedures, activities, and services
 - (B) Security infrastructure and services (identify, protective, monitoring/detective, and responsive/recovery)
 - (C) Network and connectivity
 - (D) Performance characteristics
 - (E) Availability and flexibility requirements.
- ix) System Design Documents
 - (1) Requirements Validation Document: Work product that validates the desired future state business processes and required functionality.
 - (2) System Design Document: Work product that identifies both business process decisions as well as system configuration decisions for each in scoped business process and system feature.
- x) System Configuration, Migration and Integration
 - (1) Custom Configuration
 - (2) Legacy Data Migration (as required)
 - (3) Report Implementation and Development (as required)
 - (4) Application Integration
- xi) Testing
 - (1) Test Plans and Scripts (as required)
 - (2) User Acceptance Testing
 - (3) Pre-production security testing.
- xii) Training
 - (1) User training for end-users who will be accessing and administering the Solution.
 - (2) System Administration documentation and training: complete system manual for how to use the configured system (Manuals, training video, etc.)
- xiii) Support Plan
 - (1) A support plan for ongoing maintenance support for the duration of the Contract.
- xiv) Transition Plan
 - (1) A transition strategy and plan for maintaining two systems in parallel until all data and content is fully transitioned to the Solution.
- xv) Cutover Plan
 - (1) Complete set of activities required for Go-Live, including Go-Live and Post Go-Live Support.

Table 2 – Phase 2 Deliverable Schedule

#	Milestone	Deliverable	Delivery Date
1	Project Kick-Off	Comprehensive Project Plan; Communication Plan;	<u>7</u> days from award date of Contract Amendment to Exercise Phase 2 Work Option
2	Planning & Design	Technical Infrastructure Design and Implementation Plan; Training Plan; Requirements Validation Document; System Design Document	<u>15</u> days from award date of Contract Amendment to Exercise Phase 2 Work Option

3	Data and content migration	Testing Plan(s); Risk Management/ Mitigation plan	60 days from award date of Contract Amendment to Exercise Phase 2 Work Option
4	Deployment of various environments	Deployment Plan	90 days from award date of Contract Amendment to Exercise Phase 2 Work Option
5	Quality Assurance, Testing and Training	QA and Testing Reports; Complete System Manual	120 days from award date of Contract Amendment to Exercise Phase 2 Work Option
7	Implementation & Support	Transition Plan; Support Plan	150 days from award date of Contract Amendment to Exercise Phase 2 Work Option
8	Solution	NDGLE Solution	150 days from award date of Contract Amendment to Exercise Phase 2 Work Option
9	Acceptance and Close-out & ongoing support	Project Closeout Plan; Cutover Plan; Change Management Plan;	180 days from award date of Contract Amendment to Exercise Phase 2 Work Option

3.4 LOCATION/TRAVEL

- a) Location of Work is at the Contractor's facility. No travel is anticipated.

4.0 ADDITIONAL OPTIONAL REQUIREMENTS

All Additional Optional Requirements listed under article 4. of Annex A – Statement of Work are subject to and contingent upon, at Canada's sole discretion, Canada's decision to exercise the respective irrevocable options under articles 7.1 c) ii) Professional Services and 7.1 c) iii) Training Services in the Contract.

4.1 ANNUAL SOFTWARE AS A SERVICE SUBSCRIPTION SOLUTION AUTHORIZED USER ACCESS:

The Contractor must provide Annual Software as a Service (SaaS) Subscription Solution Authorized User Access in accordance with article 1.6- Estimated Solution Usage under Annex A-Statement of Work and Annex B- Basis of Payment. The Annual SaaS subscription Solution Authorized User access must include all Solution usage rights grants, Software Documentation, Warranty, Hosting and Maintenance and Support (excluding Training), waivers, non-disclosure agreements, or other releases to Canada.

4.2 PROFESSIONAL SERVICES

- a) The Contractor must provide Professional Services, on an as-and-when-requested basis, in accordance with Article 3 a) of Annex B – Basis of Payment. Professional Services must follow the Task Authorization process in accordance with Article 7.9 of the Contract.

- b) All Task Authorized Work must be within the scope of the Contract. Work considered to be in accordance with the scope of the Contract may include, but is not limited to, Work associated to updating the accepted Solution as a result of changes to the Government of Canada Web Accessibility Standard, adding new functionalities to the accepted solution and adapting to changes in the solution's IT environment.

4.3 TRAINING SERVICES

- a) The Contractor must provide additional Training Services on an as-and-when-requested basis in accordance with Article 3 b) of Annex B – Basis of Payment. Training Services must follow the Task Authorization process in accordance with Article 7.9 of the Contract.
- b) All Task Authorized Training Services must be within the scope of the Contract. Training Services considered to be in accordance with the scope of the Contract may include, but is not limited to, Solution-relevant training for administrators, and other identified users accessing the Solution.

5.0 REFERENCE DOCUMENTS

- [Accessible Canada Act](#)
- [Web Experience Toolkit \(WET\);](#)
- [WCAG 2.0 A Accessibility Standards;](#)
- [Official Languages Act;](#)
- [Access to Information Act;](#) and
- [Privacy Act;](#)

APPENDIX A TO ANNEX A – CAPABILITY AND USABILITY ASSESSMENT

GENERAL

Purpose.

This document outlines the Capability and Usability Assessment process.

Instructions

Upon the award of up to 3 Contracts, Contractors must develop and submit a cloud-based CUA Prototype Solution for the School's assessment.

The CUA Prototype Solution must support access to the Prototype Solution, including all Solution usage rights grants, Software Documentation, Warranty, Hosting and Maintenance and Support (excluding Training), waivers, non-disclosure agreements, or other releases to Canada for purposes of conducting the CUA assessment, for up to 200 Authorized Users to use the Prototype Solution for Capability and Usability Assessment purposes during the initial contract period. These designated hands-on capability/usability assessment testers may include faculty, staff, administrators, course designers, data analysts, individuals with disabilities, technology professionals, and learners from various public service departments and agencies. Their structured feedback will be included in the Capability and Usability Assessment score.

Contractor must provide access, which includes all usage rights grants, Software Documentation, Warranty, Hosting and Maintenance and Support (excluding Training), waivers, non-disclosure agreements, or other releases to Canada, to the CUA Prototype Solution to use for Capability and Usability Assessment purposes during the initial contract period:

SELECTION OF CONTRACTOR'S PROTOTYPE SOLUTION

Following award of a Contract, a Capability and Usability Assessment (CUA) will be conducted by Canada. The Capability and Usability Assessment (CUA) Prototype Solution deliverables provided under the Contract will be assessed by Canada against the criteria detailed at Appendix A to Annex A – Statement of Work.

The sum of the scores for each individual category will be calculated in accordance with the assessment criteria and maximum points listed in each category of Appendix A to Annex A – Statement of Work.

The top ranked CUA Prototype Solution will be determined based on the highest responsive combined rating of technical merit, price and CUA. 30% weighting will be given to the Technical Evaluation Score from Evaluation. 20% weighting will be given to the Financial Evaluation Score. 50% weighting will be given to the CUA Score, as per the following table:

Assessment	Weightage
Technical Evaluation Score	30%
Financial Evaluation Score	20%

Capability and Usability Assessment Score	50%
---	-----

In the event of a tie, the CUA Score will be used to rank the Contractors from highest to lowest score. If there are further ties, the lowest Financial Score will be used to rank the Contractor.

Canada will, at its discretion, exercise its irrevocable option to select a Contractor to perform all or a portion of the Work under article 3. Phase 2 - Solution of Annex A – Statement of Work. Canada may also, at its discretion, exercise its irrevocable option with other Contractors who participated in the CUA for all or a portion of the Work if it is determined that this would best meet the needs of Canada

Capability and Usability Assessment Criteria and Test Scenarios

Canada will post the Capability and Usability Assessment Criteria and Test Scenarios at a later date through an amendment to the Solicitation.

ANNEX B

BASIS OF PAYMENT

1. Financial Response

All prices must be provided in Canadian dollars exclusive of any applicable taxes.

The detailed financial proposal consists of the following all-inclusive price components:

1. A firm fixed price for Work under Phase 1 of Annex A - Statement of Work to Develop and Deliver a Prototype Solution. The price for this Work is set at: \$30,000.00 CAD, applicable taxes extra.
2. A firm fixed price for the optional Work under Phase 2 of Annex A - Statement of Work to Develop and Deliver the Full Solution.
3. A firm fixed price for optional services under Phase 2 of Annex A - Statement of Work for Annual Software as a Service Subscription Solution Access
4. A firm fixed per diem rate for optional services under Phase 2 for Task Authorized Professional Service
5. A firm fixed per diem rate for optional services under Phase 2 for Task Authorized Training Services

2. Work

(a) Phase 1 - Work to develop and deliver a CUA Solution Prototype

Table 1 - Firm All-Inclusive Price (applicable taxes extra) for the Work described in article 2. Phase 1 Prototype Solution of the Statement of Work in Annex A, including granting Solution access which includes all Solution usage rights grants, Software Documentation, Warranty, Hosting and Maintenance and Support (excluding Training), waivers, non-disclosure agreements, or other releases to Canada for purposes of conducting the CUA assessment, for up to 200 Authorized Users to use the Prototype Solution for Capability and Usability Assessment purposes during the initial contract period:

Item # (A)	Description (B)	Firm All-Inclusive Price (C)
1	All deliverables associated with Article 2. Phase 1 – Prototype Solution in Annex A – Statement of Work.	\$30,000.00 CAD (excluding any applicable taxes)

3. Optional Goods and Services

(a) Phase 2 – Delivery of the Solution

- (i) At Canada's sole discretion, Canada may exercise the irrevocable option to deliver the production-ready Solution in accordance with article 3. Phase 2 - Solution of Annex A – Statement of Work.

Table 2 - Firm All-Inclusive Price (applicable taxes extra) for the Work described in article 3. Phase 2 - Solution of Annex A – Statement of Work. including access which includes all Solution usage rights grants, Software Documentation, Warranty, Hosting and Maintenance and Support (excluding Training), waivers, non-disclosure agreements, or other releases to Canada for up to 260,000 Authorized Users :

Item # (A)	Description (B)	Firm All-Inclusive Price (C)
1	All deliverables associated with Article 3. Phase 2 – Solution of the Statement of Work in Annex A	\$

(b) **Authorized User Access to Solution**

Table 3 - Firm all-inclusive price for optional Annual Subscription Authorized User Access to the Solution, which includes all Solution usage rights grants, Software Documentation, Warranty, Hosting and Maintenance and Support (excluding Training), waivers, non-disclosure agreements, or other releases to Canada:

Item #	Description	Option Period 1	Option Period 2	Option Period 3	Option Period 4	Option Period 5	Option Period 6	Option Period 7	Option Period 8	Option Period 9
		Firm All-Inclusive Price (D)	Firm All-Inclusive Price (E)	Firm All-Inclusive Price (F)	Firm All-Inclusive Price (G)	Firm All-Inclusive Price (H)	Firm All-Inclusive Price (I)	Firm All-Inclusive Price (J)	Firm All-Inclusive Price (K)	Firm All-Inclusive Price (L)
1	Annual Software as a Service Subscription Access for 0 to 260,000 Authorized Users	\$	\$	\$	\$	\$	\$	\$	\$	\$
2	Annual Software as a Service Subscription Access for 260,001 to 360,000 Authorized Users	\$	\$	\$	\$	\$	\$	\$	\$	\$
3	Annual Software as a Service Subscription Access for 360,001 to 460,000 Authorized Users	\$	\$	\$	\$	\$	\$	\$	\$	\$
4	Annual Software as a Service Subscription Access for 460,001 and above Authorized Users	\$	\$	\$	\$	\$	\$	\$	\$	\$

(c) **Optional Professional Services**

Table 4 - Firm all-inclusive per diem rates for Optional Professional Services to be provided on an as-and-when requested basis as described in Annex A – Statement of Work and in accordance with the Task Authorization process:

Item #	Resource Category	Initial Period	Option Period 1	Option Period 2	Option Period 3	Option Period 4	Option Period 5	Option Period 6	Option Period 7	Option Period 8	Option Period 9
(A)	(B)	(C)	(D)	(E)	(F)	(G)	(H)	(I)	(J)	(K)	(L)
		Firm All-Inclusive Per Diem Rate									
1		\$	\$	\$	\$	\$	\$	\$	\$	\$	\$
2		\$	\$	\$	\$	\$	\$	\$	\$	\$	\$
3		\$	\$	\$	\$	\$	\$	\$	\$	\$	\$
4		\$	\$	\$	\$	\$	\$	\$	\$	\$	\$

(d) **Optional Training Services**

Table 5 - Firm all-inclusive per diem rate for Training Services on an as-and-when requested basis, as detailed in Annex A – Statement of Work and in accordance with the Task Authorization process:

Item #	Description	Initial Period	Option Period 1	Option Period 2	Option Period 3	Option Period 4	Option Period 5	Option Period 6	Option Period 7	Option Period 8	Option Period 9
		Firm All-Inclusive Per Diem Rate (C)	Firm All-Inclusive Per Diem Rate (D)	Firm All-Inclusive Per Diem Rate (E)	Firm All-Inclusive Per Diem Rate (F)	Firm All-Inclusive Per Diem Rate (G)	Firm All-Inclusive Per Diem Rate (H)	Firm All-Inclusive Per Diem Rate (I)	Firm All-Inclusive Per Diem Rate (J)	Firm All-Inclusive Per Diem Rate (K)	Firm All-Inclusive Per Diem Rate (L)
(A)	(B)										
1	Training Services	\$	\$	\$	\$	\$	\$	\$	\$	\$	\$

Solicitation No. - N° de l'invitation
0X001-190594/A
Client Ref. No. - N° de réf. du client
0X001-190594

Amd. No. - N° de la modif.
-
File No. - N° du dossier
108xl0X001-190594

Buyer ID - Id de l'acheteur
108 XL
CCC No./N° CCC - FMS No./N° VME

ANNEX C

SECURITY REQUIREMENT CHECK LIST



Government of Canada
 Gouvernement du Canada

Contract Number / Numéro du contrat OX001-190594
Security Classification / Classification de sécurité

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

PART A - CONTRACT INFORMATION / PARTIE A - INFORMATION CONTRACTUELLE		
1. Originating Government Department or Organization / Ministère ou organisme gouvernemental d'origine CSPS	2. Branch or Directorate / Direction générale ou Direction User Experience Directorate - LPB	
3. a) Subcontract Number / Numéro du contrat de sous-traitance	3. b) Name and Address of Subcontractor / Nom et adresse du sous-traitant	
4. Brief Description of Work / Brève description du travail Software as a service (Saas) Cloud-Based Learning Management System		
5. a) Will the supplier require access to Controlled Goods? Le fournisseur aura-t-il accès à des marchandises contrôlées? <input checked="" type="checkbox"/> No <input type="checkbox"/> Yes Non Oui		
5. b) Will the supplier require access to unclassified military technical data subject to the provisions of the Technical Data Control Regulations? Le fournisseur aura-t-il accès à des données techniques militaires non classifiées qui sont assujetties aux dispositions du Règlement sur le contrôle des données techniques? <input checked="" type="checkbox"/> No <input type="checkbox"/> Yes Non Oui		
6. Indicate the type of access required / Indiquer le type d'accès requis		
6. a) Will the supplier and its employees require access to PROTECTED and/or CLASSIFIED information or assets? Le fournisseur ainsi que les employés auront-ils accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS? (Specify the level of access using the chart in Question 7. c) (Préciser le niveau d'accès en utilisant le tableau qui se trouve à la question 7. c) <input type="checkbox"/> No <input checked="" type="checkbox"/> Yes Non Oui		
6. b) Will the supplier and its employees (e.g. cleaners, maintenance personnel) require access to restricted access areas? No access to PROTECTED and/or CLASSIFIED information or assets is permitted. Le fournisseur et ses employés (p. ex. nettoyeurs, personnel d'entretien) auront-ils accès à des zones d'accès restreintes? L'accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS n'est pas autorisé. <input checked="" type="checkbox"/> No <input type="checkbox"/> Yes Non Oui		
6. c) Is this a commercial courier or delivery requirement with no overnight storage? S'agit-il d'un contrat de messagerie ou de livraison commerciale sans entreposage de nuit? <input checked="" type="checkbox"/> No <input type="checkbox"/> Yes Non Oui		
7. a) Indicate the type of information that the supplier will be required to access / Indiquer le type d'information auquel le fournisseur devra avoir accès		
Canada <input checked="" type="checkbox"/>	NATO / OTAN <input type="checkbox"/>	
	Foreign / Étranger <input type="checkbox"/>	
7. b) Release restrictions / Restrictions relatives à la diffusion		
No release restrictions Aucune restriction relative à la diffusion <input checked="" type="checkbox"/>	All NATO countries Tous les pays de l'OTAN <input type="checkbox"/>	
Not releasable À ne pas diffuser <input type="checkbox"/>		
Restricted to: / Limité à: <input type="checkbox"/> Specify country(ies): / Préciser le(s) pays:	Restricted to: / Limité à: <input type="checkbox"/> Specify country(ies): / Préciser le(s) pays:	
	No release restrictions Aucune restriction relative à la diffusion <input type="checkbox"/>	
	Restricted to: / Limité à: <input type="checkbox"/> Specify country(ies): / Préciser le(s) pays:	
7. c) Level of Information / Niveau d'information		
PROTECTED A PROTÉGÉ A <input checked="" type="checkbox"/>	NATO UNCLASSIFIED NATO NON CLASSIFIÉ <input type="checkbox"/>	PROTECTED A PROTÉGÉ A <input type="checkbox"/>
PROTECTED B PROTÉGÉ B <input checked="" type="checkbox"/>	NATO RESTRICTED NATO DIFFUSION RESTREINTE <input type="checkbox"/>	PROTECTED B PROTÉGÉ B <input type="checkbox"/>
PROTECTED C PROTÉGÉ C <input type="checkbox"/>	NATO CONFIDENTIAL NATO CONFIDENTIEL <input type="checkbox"/>	PROTECTED C PROTÉGÉ C <input type="checkbox"/>
CONFIDENTIAL CONFIDENTIEL <input type="checkbox"/>	NATO SECRET NATO SECRET <input type="checkbox"/>	CONFIDENTIAL CONFIDENTIEL <input type="checkbox"/>
SECRET SECRET <input type="checkbox"/>	COSMIC TOP SECRET COSMIC TRÈS SECRET <input type="checkbox"/>	SECRET SECRET <input type="checkbox"/>
TOP SECRET TRÈS SECRET <input type="checkbox"/>		TOP SECRET TRÈS SECRET <input type="checkbox"/>
TOP SECRET (SIGINT) TRÈS SECRET (SIGINT) <input type="checkbox"/>		TOP SECRET (SIGINT) TRÈS SECRET (SIGINT) <input type="checkbox"/>

Solicitation No. - N° de l'invitation
 OX001-190594/A
 Client Ref. No. - N° de réf. du client
 OX001-190594

Amd. No. - N° de la modif.
 -
 File No. - N° du dossier
 108x10X001-190594

Buyer ID - Id de l'acheteur
 108 XL
 CCC No./N° CCC - FMS No./N° VME



Government of Canada
 Gouvernement du Canada

Contract Number / Numéro du contrat OX001-190594
Security Classification / Classification de sécurité

PART A (continued) / PARTIE A (suite)

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

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

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

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

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

<input checked="" type="checkbox"/> RELIABILITY STATUS COTE DE FIABILITÉ	<input type="checkbox"/> CONFIDENTIAL CONFIDENTIEL	<input type="checkbox"/> SECRET SECRET	<input type="checkbox"/> TOP SECRET TRÈS SECRET
<input type="checkbox"/> TOP SECRET- SIGINT TRÈS SECRET - SIGINT	<input type="checkbox"/> NATO CONFIDENTIAL NATO CONFIDENTIEL	<input type="checkbox"/> NATO SECRET NATO SECRET	<input type="checkbox"/> COSMIC TOP SECRET COSMIC TRÈS SECRET
<input type="checkbox"/> SITE ACCESS ACCÈS AUX EMPLACEMENTS			

Special comments: **Should the contractor or its employee(s) not hold a valid security clearance, he/she must be escorted**
 Commentaires spéciaux : **at all times by a CSPS employee while working on CSPS premises.**

NOTE: If multiple levels of screening are identified, a Security Classification Guide must be provided.
 REMARQUE : Si plusieurs niveaux de contrôle de sécurité sont requis, un guide de classification de la sécurité doit être fourni.

10. b) May unscreened personnel be used for portions of the work?
 Du personnel sans autorisation sécuritaire peut-il se voir confier des parties du travail? No / Non Yes / Oui
 If Yes, will unscreened personnel be escorted?
 Dans l'affirmative, le personnel en question sera-t-il escorté? No / Non Yes / Oui

PART C - SAFEGUARDS (SUPPLIER) / PARTIE C - MESURES DE PROTECTION (FOURNISSEUR)

INFORMATION / ASSETS / RENSEIGNEMENTS / BIENS

11. a) Will the supplier be required to receive and store PROTECTED and/or CLASSIFIED information or assets on its site or premises?
 Le fournisseur sera-t-il tenu de recevoir et d'entreposer sur place des renseignements ou des biens PROTÉGÉS et/ou CLASSIFIÉS? No / Non Yes / Oui

11. b) Will the supplier be required to safeguard COMSEC information or assets?
 Le fournisseur sera-t-il tenu de protéger des renseignements ou des biens COMSEC? No / Non Yes / Oui

PRODUCTION

11. c) Will the production (manufacture, and/or repair and/or modification) of PROTECTED and/or CLASSIFIED material or equipment occur at the supplier's site or premises?
 Les installations du fournisseur serviront-elles à la production (fabrication et/ou réparation et/ou modification) de matériel PROTÉGÉ et/ou CLASSIFIÉ? No / Non Yes / Oui

INFORMATION TECHNOLOGY (IT) MEDIA / SUPPORT RELATIF À LA TECHNOLOGIE DE L'INFORMATION (TI)

11. d) Will the supplier be required to use its IT systems to electronically process, produce or store PROTECTED and/or CLASSIFIED information or data?
 Le fournisseur sera-t-il tenu d'utiliser ses propres systèmes informatiques pour traiter, produire ou stocker électroniquement des renseignements ou des données PROTÉGÉS et/ou CLASSIFIÉS? No / Non Yes / Oui

11. e) Will there be an electronic link between the supplier's IT systems and the government department or agency?
 Disposera-t-on d'un lien électronique entre le système informatique du fournisseur et celui du ministère ou de l'agence gouvernementale? No / Non Yes / Oui

TBS/SCT 350-103(2004/12)

Security Classification / Classification de sécurité
--



Solicitation No. - N° de l'invitation
 0X001-190594/A
 Client Ref. No. - N° de réf. du client
 0X001-190594

Amd. No. - N° de la modif.
 -
 File No. - N° du dossier
 108x10X001-190594

Buyer ID - Id de l'acheteur
 108 XL
 CCC No./N° CCC - FMS No./N° VME



Government of Canada
 Gouvernement du Canada

Contract Number / Numéro du contrat 0X001-190594
Security Classification / Classification de sécurité

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

For users completing the form manually use the summary chart below to indicate the category(ies) and level(s) of safeguarding required at the supplier's site(s) or premises.

Les utilisateurs qui remplissent le formulaire manuellement doivent utiliser le tableau récapitulatif ci-dessous pour indiquer, pour chaque catégorie, les niveaux de sauvegarde requis aux installations du fournisseur.

For users completing the form online (via the Internet), the summary chart is automatically populated by your responses to previous questions.

Dans le cas des utilisateurs qui remplissent le formulaire en ligne (par Internet), les réponses aux questions précédentes sont automatiquement saisies dans le tableau récapitulatif.

SUMMARY CHART / TABLEAU RÉCAPITULATIF

Category Catégorie	PROTECTED PROTÉGÉ			CLASSIFIED CLASSIFIÉ			NATO				COMSEC					
	A	B	C	CONFIDENTIAL CONFIDENTIEL	SECRET	TOP SECRET TRÈS SECRET	NATO RESTRICTED NATO DIFFUSION RESTREINTE	NATO CONFIDENTIAL NATO CONFIDENTIEL	NATO SECRET	COSMIC TOP SECRET COSMIC TRÈS SECRET	PROTECTED PROTÉGÉ			CONFIDENTIAL CONFIDENTIEL	SECRET	TOP SECRET TRÈS SECRET
											A	B	C			
Information / Assets Renseignements / Biens Production																
IT Media / Support TI																
IT Link / Lien électronique																

12. a) Is the description of the work contained within this SRCL PROTECTED and/or CLASSIFIED?
 La description du travail visé par la présente LVERS est-elle de nature PROTÉGÉE et/ou CLASSIFIÉE? No / Non Yes / Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification".
 Dans l'affirmative, classifiez le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire.

12. b) Will the documentation attached to this SRCL be PROTECTED and/or CLASSIFIED?
 La documentation associée à la présente LVERS sera-t-elle PROTÉGÉE et/ou CLASSIFIÉE? No / Non Yes / Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification" and indicate with attachments (e.g. SECRET with Attachments).
 Dans l'affirmative, classifiez le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire et indiquez qu'il y a des pièces jointes (p. ex. SECRET avec des pièces jointes).

Solicitation No. - N° de l'invitation
OX001-190594/A
Client Ref. No. - N° de réf. du client
OX001-190594

Amd. No. - N° de la modif.
-
File No. - N° du dossier
108x10X001-190594

Buyer ID - Id de l'acheteur
108 XL
CCC No./N° CCC - FMS No./N° VME



Government of Canada
Gouvernement du Canada

Contract Number / Numéro du contrat

OX001-190594

Security Classification / Classification de sécurité

PART D - AUTHORIZATION / PARTIE D - AUTORISATION

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

Name (print) - Nom (en lettres moulées) Nowosielski, Leszek		Title - Titre Executive Director	Signature
Telephone No. - N° de téléphone 819-953-5764	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel leszek.nowosielski@canada.ca	Date August 12, 2019

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

Name (print) - Nom (en lettres moulées) Leduc, Pierre		Title - Titre Director Security	Signature Leduc, Pierre <small>Digitally signed by Leduc, Pierre Date: 2019.08.15 08:30:53 -04'00'</small>
Telephone No. - N° de téléphone 819-934-8318	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel pierre.leduc2@canada.ca	Date

15. Are there additional instructions (e.g. Security Guide, Security Classification Guide) attached?
Des instructions supplémentaires (p. ex. Guide de sécurité, Guide de classification de la sécurité) sont-elles jointes?

<input checked="" type="checkbox"/> No Non	<input type="checkbox"/> Yes Oui
---	-------------------------------------

16. Procurement Officer / Agent d'approvisionnement

Name (print) - Nom (en lettres moulées) Fenwick, Wesley		Title - Titre A/Supply Specialist	Signature
Telephone No. - N° de téléphone 6136-720-7743	Facsimile No. - N° de télécopieur N/A	E-mail address - Adresse courriel wesley.fenwick@tpsgc-pwgsc.gc.ca	Date

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

Name (print) - Nom (en lettres moulées)		Title - Titre	Signature
Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date

**APPENDIX A TO ANNEX C –
 SECURITY CLASSIFICATION GUIDE**

The following table outlines the personnel and facility security clearance requirements based on the expected roles and access to GC data.

Table A-1 Security Classification Guide for Commercial Cloud Services

#	Role/Function	Expected Type of Data Accessed	Data Access Location (Canada / Foreign / Both)	Screening Required	Responsibility	Details
1.	Any Contractor personnel with physical access to the Contractor data centers	<ul style="list-style-type: none"> Physical hardware Data Center facilities Data as stored on the Contractor's local Backup Media 	Canada	Reliability	Contractor	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 logical access to the Contractor services	<ul style="list-style-type: none"> 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	Contractor	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.
3.	Any Contractor personnel with privileged roles and unrestricted logical access to GC assets within the Contractor services	<ul style="list-style-type: none"> 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	Contractor	This is for any Contractor personnel that has elevated privileges with unrestricted logical access to the GC assets hosted in the Contractor data centers and 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	Responsibility	Details
4.	Any Contractor personnel or Reseller who has access to the GC Master Account information and/or credentials	<ul style="list-style-type: none"> GC Master Account Information/Credentials 	Both	Reliability	Contractor and/or Reseller	This is for any Contractor or Reseller personnel that has access to the GC master account or root credentials for the cloud service account setup.
5.	Prime Contractor*	Media	Both	Reliability	Contractor	Information that is sent from Prime Contractor to Subcontractor - needs to be encrypted.
6.	Operations Manager/Personnel *	Name, addresses, email, phone numbers and data centers	Both	Reliability	Contractor	Information that is sent from Prime Contractor to Subcontractor - needs to be encrypted.
7.	General duties	Public and reception zones	Both	N/A	Contractor	
8.	General duties*	Sensitive sites (such as operational zones where data is stored)	Both	Reliability Status	Contractor	<p>*Information within site may be of sensitive nature. Individuals who are not screened must be escorted at all times.</p> <p>General duties include personnel providing maintenance services, security guards in the Operational Zone, etc.</p>

*The Contractor must contact PSPC CISD to ensure that the appropriate sub-SRCL is established for Sub-Contractors.

APPENDIX B TO ANNEX C –

SECURITY OBLIGATIONS

Security Obligations

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

1. Change Management.

- (a) The Contractor must, throughout the Contract, take all steps required to update and maintain the Security Obligations as needed to comply with the security practices of industry standards.
- (b) 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.

2. Acknowledgements.

The parties acknowledge that:

- (a) All Assets and Information Assets are subject to these Security Obligations.
- (b) Notwithstanding any other provision of the Contract, the parties have shared responsibility for developing and maintaining policies, procedures and security controls relating to Assets and Information Assets.

3. Data Transfer and Retrieval.

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, source code hosted in a Canada code repository, and network configurations such that the Client 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>).

4. Data Disposition and Returning Records to Canada.

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

- (b) The Contractor must, upon request by Canada, 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.

5. Continuous Monitoring.

- (a) The Contractor must continually manage, monitor, and maintain the security posture of all Assets, Contractor Infrastructure and Service Locations throughout the period of the Contract, and ensure that the Public Cloud Services provided to Canada are in a manner that complies with these Security Obligations. As part of this obligation, the Contractor must:
 - (i) Actively and continuously monitor threats and vulnerabilities to its Assets, Contractor Infrastructure, Service Locations, or Information Assets;
 - (ii) Undertake best efforts to prevent attacks through security measures such as denial of service protections;
 - (iii) Undertake best efforts to detect attacks, Security Incidents, and other abnormal events;
 - (iv) Identify unauthorized use and access of any Public Cloud Services, data and components relevant to Canada's IaaS, PaaS or SaaS Solution;
 - (v) Manage and apply security-related patches and updates in a timely and systematic manner to mitigate vulnerabilities and remedy any publicly reported issues in the Public Cloud Services or libraries that the Solution make use of, and provide advance notices of patches in accordance with agreed-upon service level commitments;
 - (vi) Respond, contain, and recover from threats and attacks against the Contractor Services; and
 - (vii) Where required, take proactive countermeasures, including taking both pre-emptive and responsive actions, to mitigate threats.
- (b) The Contractor's Public Cloud Services must allow for GC application data (for IaaS, PaaS and SaaS) and GC network traffic (for IaaS and PaaS) of cloud hosted GC services to be copied and forwarded to a predetermined location (in the cloud or on GC premises).
- (c) The Contractor's Public Cloud Services must allow Canada to deploy and operate security software to perform advanced monitoring and mitigations of cyber threats for Canada's Solution at the Canada managed host and network layer, for Canada managed components only.

6. Notifications.

- (a) The Contractor must provide:
 - (i) Timely notification of any interruption that is expected to impact service availability and performance (as agreed to by the parties and included in the SOW and/or SLA);
 - (ii) Regular updates on the status of returning the Solution to an operating state according to the agreed upon SLAs and system availability requirements, both as advance alerts and post-implementation alerts; and

- (iii) Information system security alerts, advisories, and directives via email for vulnerabilities that pose a threat to the Solution

7. Security Incident Response

- (a) 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 Client Data or Personal Information 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.
- (b) The Contractor must alert and promptly notify the Client (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.
- (c) 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:
 - (i) Allowing only designated representatives of Canada to have the ability to:
 - i. request and receive information associated with the Security Incident and any compromised Information Assets (including user data, system/security event logs, network or host packet captures, logs from security components such as IDS/IPS/Firewalls, etc.), in an unencrypted fashion, for the purposes of conducting investigations;
 - ii. track the status of a reported information security event or Security Incident.
 - (ii) Supporting Canada's investigative efforts in the case of any compromise of the users or data in the Solution that is identified.
- (d) The Contractor must:
 - (i) Maintain a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data or the service; and
 - (ii) Track, or enable Canada to track, disclosures of Assets and Information Assets, including what data has been disclosed, to whom, and at what time.

8. E-Discovery and Legal Holds

The Contractor must (and must, to the extent applicable given the nature of the subcontracted Public Cloud Services provided by each Contractor Sub-processor, require Contractor Sub-processors to) take reasonable measures to ensure the Solution 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.

9. Security Assessment Testing

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 Solution components within the Contractor environment.

10. Sub-processors

- (a) The Contractor must provide a list of Sub-processors that could be used to perform any part of the Public Cloud Services in providing Canada with the Solution. The list must include the following information (i) the name of the Sub-processor; (ii) the identification of the Public Cloud Services that would be performed by the Sub-processor; and (iii) the location(s) where the Sub-processor would perform the Public Cloud Services.
- (b) 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 Client Data or Personal Information. The Contractor must assist Canada with verification of sub-processors within 10 working days.

11. Supply Chain Risk Management

Within 30 days of contract award, the Contractor must provide an up-to-date Supply Chain Risk Management (SCRM) Plan that has been independently assessed and validated by an independent third party certified under AICPA or CPA Canada, and/or ISO certification regime. The SRCM Plan must be provided to Canada on an annual basis, or upon request, or promptly following any material Change to the SRCM Plan.

APPENDIX C TO ANNEX C –

ADDITIONAL SECURITY INFORMATION FOR FOREIGN CONTRACTOR OR SUBCONTRACTOR

The Foreign Recipient **Contractor / Subcontractor** must perform a security screening of all its personnel who will need access to **CANADA PROTECTED** information:

- a) Identity check
 - i. Copies of two of valid original pieces of government issued identity documentation, one of which must include a photo
 - ii. Surname (last name)
 - iii. Full given names (first name) – underline or circle usual name used
 - iv. Family name at birth
 - v. All other names used (aliases)
 - vi. Name changes
 1. Must include the name they changed from and the name they changed to, the place of change and the institution changed through
 - vii. Sex
 - viii. Date of birth
 - ix. Place of birth (city, province/state/region, and country)
 - x. Citizenship(s)
 - xi. Marital status/common-law partnership
 1. Current Status (married, common-law, separated, widowed, divorced, single)
 2. All current spouses (if applicable)
 - a. Surname (last name)
 - b. Full given names (first name) – underline or circle usual name used
 - c. Date and duration of marriage/common-law partnership
 - d. Date of birth
 - e. Family name at birth
 - f. Place of birth (city, province/state/region, and country)
 - g. Citizenship
- b) Residency check
 - i. The last five (5) years of residency history starting from most recent with no gaps in time.
 1. Apartment number, street number, street name, city, province or state, postal code or zip code, country, from-to dates
- c) Educational check
 - i. The educational establishments attended and the corresponding dates.
- d) Employment history check
 - i. The last five (5) years of employment history starting from most recent with no gaps in time.
 - ii. Three (3) employment reference checks from the last five (5) years.
- e) Criminal records check:
 - i. report(s) containing all criminal convictions for the last five (5) years in and outside of the candidate's country of residence.

ANNEX D

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 Contractor Subcontractor’s data centre, networking, storage, servers, virtualization platforms, operating systems, middleware, and applications).

“API (Application Programming Interface)” mean an interface that allows developers to interact with programs and applications, including learning management systems.

“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.

“Asynchronous learning” means a student-centred teaching method that allows learners to train individually, enabling them to complete courses at a time, place and pace that suits them.

“Authoring Tool” means a software often paired with an LMS that is used to develop content for online learning and training programs. An eLearning content authoring tool is a software package which content developers use to create and package eLearning course content using SCORM or xAPI standards.

“Authorized User” means any user that holds a valid Solution access log-in profile.

“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.

“Blended Learning” means a style of education in which students learn via electronic and online media as well as traditional face-to-face teaching.

“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 Contractor Subcontractors by or on behalf of the Canada or End Users; (ii) to which the Contractor or any Contractor Subcontractors 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 Contractor Subcontractor 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.

“**Certification**” means the action or process of providing someone or something with an official document attesting to a status or level of achievement. Some certifications are mandatory and condition to employment.

“**Classroom Course**” means a course taught by a teacher where the students attend and participate to the course in real time. The offering can be live on-site, virtual or both at the same time.

“**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 SaaS 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.

“**Concurrent User**” means more than one Authorized User utilizing the Solution at the same time.

“**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.

“**Contractor**” means 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.

“**Course**” means a collection of learning materials, activities and assessment that pursue a set of specific learning objectives.

“Course Catalogue” means a collection of courses made available to learners so they can self-select the training they want to complete.

“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.

“CRUD” means Create, Read, Update and Delete (CRUD) operations.

“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.

“Distance Learning” means a method of studying in which lectures are broadcast or lessons are conducted by correspondence, without the student needing to attend a School or college.

“eLearning (Electronic Learning)” means the delivery of learning and training through digital resources. Although eLearning is based on formalized learning, it's provided through electronic devices such as computers, tablets and even cellular phones that are connected to the internet.

“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.

“Gamification” means an approach to motivate students to learn by using game design and game elements in learning environments.

“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).

“Interoperability” means the extent to which hardware and software elements work together. eLearning standards like SCORM, xAPI (Tin Can) and AICC were developed to enhance the interoperability of online learning content and technologies.

“Learning Activity” means an activity with a learning product.

“Learning Objectives” means the learning intention (or objective) related to a learning product which describes clearly what the teacher wants the students to learn (i.e. know / understand / be able to do) as a result of the learning or teaching activities.

“Learning outcomes” means statements that describe significant and essential understanding or skills that learners can reliably demonstrate upon successful completion of a course or program.

“Learning Path” means structured learning programs that guide learners through a series of courses. They allow admins to control the timeframe in which courses are made available to learners and the order in which they're completed.

“Learning Product” means a generic expression referring to any content that supports some pedagogical objectives. e.g.: video, blog, course (online, distance, classroom), event, graphics, case studies, etc.

“Learning Product Offering” an instance of a limited learning resource delivery. It binds a learning product, participants, facilitators, assets and facilities to a timeframe.

“Learning Program” means a learning path leading to a certification.

“Limited Learning Product” means a generic expression referring to any learning products that have physical constraints such as classroom courses, events, distance learnings, etc.

“LRS (Learning Record Store)” means a system that works with xAPI (Tin Can) to collect, store and retrieve statements that track learning experiences. Data stored by an LRS can be presented in a way that's accessible and easy to interpret.

“Maintenance Releases” means all commercially available enhancements, extensions, improvements, upgrades, updates, releases, versions, renames, rewrites, cross-grades, components and back grades or other modifications to the Solution developed or published by the Contractor or its licensor.

“Manage” means, in the context of an information system, actions such as the creation, the access, the modification, and the deletion for information or record(s).

“Micro-learning” means a way to deliver training content to learners in bite-sized, focused bursts. Each unit or module focuses on an individual learning objective.

“MOOC” means a Massive Open Online Course is an online course aimed at unlimited participation and open access via the web. In addition to traditional course materials such as filmed lectures, readings, and problem sets, many MOOCs provide interactive user forums to support community interactions among students, professors, and teaching assistants (TAs).

“Offering” means an instance of a learning resource delivery. It binds a learning product, participants, facilitators, assets and facilities to a timeframe.

“Online Assessment” means an online assessment evaluates what the learner has learned. This can come in the form of quizzes, surveys, questionnaires, etc.

“Online Self-Paced Course” means an online asynchronous course taken at the learner's own time and pace, and does not involve any interactions with teachers or other learners.

“On-site Offering” means an offering where participants are physically attending the learning delivery.

“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.

“Podcast” means digital audio files streamed over the internet, used by millions of listeners to learn about a huge range of subjects.

“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.

“Quick Start” Services means a defined package of services possibly including essential training on best practices, Architecture, Deployment, Operational Design Integration, scalability, or use of the Solution. Also sometimes referred to as a Jump Start Package or Quick Start Guide.

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

“Role-based Authorized User” means an Authorized User with specific, role-based Solution access privileges, such as an administrator, teacher, content creator, etc.

“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 Subcontractor’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 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 Solution access and usage rights;
- ii) providing Solution Documentation;
- iii) maintaining, upgrading, and updating the Solution;
- 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.

“Single Sign-On (SSO)” means a set of credentials that allows users to access multiple applications in your organization while only needing to log in once.

“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.

“the School” means the Canada School of Public Service.

“Software Error” means any software 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.

“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 A – Statement of Work, including the procedures for determining whether the requirements have been met.

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

“Synchronous learning” means learning involving real-time interactions between participants and/or facilitator.

“TBS” means Treasury Board of Canada Secretariat.

“UI (User Interface)” means the means by which the user and a computer system interact.

“UX (User Experience)” means an individual's reaction to the use of a particular product, system or service. It generally describes the emotional reaction to the use of the system mainly in light of its ease of use or the satisfaction it provides.

“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, a SaaS, or a CSP who is also an SaaS.

“Virtual Classroom” means a digital environment where teacher(s) and students assigned to a given offering can exchange (group discussion, private chat, documents, etc.) and collaborate (documents, activities, exercises) either synchronously or asynchronously.

“Virtual Offering” means an offering where participants are remotely attending the learning delivery, typically through some teleconferencing or virtual meeting services.

“Web Session” means a group of user interactions with the Solution that takes place within a given time frame. For example, a single session can contain multiple page views, events, interactions, and transactions.

“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 E

PRIVACY OBLIGATIONS

1. Auditing Compliance

- (a) In the event Canada needs to conduct security audits, inspections and/or review any additional information (e.g., documentation, data protection description, data architecture and security descriptions) pursuant to Section 12.1, both Parties agree to negotiate a solution in good faith and consider both the rationale for Canada's request and the Contractor's processes and protocols.
- (b) Within 30 days of request from the Contracting Authority, 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 Client data as defined by the Contractor and does not specifically have Personal Information in Support Data (collected in logs (e.g., telemetry data such as email message headers and content)).

2. Data Ownership and Privacy Requests

- (a) Client Data including all Personal Information (PI) will be used or otherwise processed only to provide the Services, including purposes compatible with providing the Services. The Contractor must not use or otherwise process Canada Data or derive information from it for any advertising or similar commercial purposes. As between the parties, the Client retains all right, title and interest in and to Client Data. The Contractor acquires no rights in Canada Data, other than the rights Client grants to the Contractor to provide the Solution to the Customer.
- (b) All data the Contractor 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 five Federal Government Working Days (or seven Federal Government Working Days if it must be retrieved from offsite backup/replication) in a Word or Excel document.

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

- (a) Upon request of the Technical Authority, the Contractor must support Canada in creating a privacy impact assessment in accordance with the Treasury Board Directive on Privacy Impact Assessment (<https://www.statcan.gc.ca/eng/about/pia/dcpia>) 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 ten working days of a request or within a mutually agreed upon timeframe depending on the complexity of the request by the Canada.

4. Privacy Breach

- (a) 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 Contractor 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).
- (b) 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 Client Data or Personal Information 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.
- (c) The Contractor must:
 - (i) Maintain a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data; and
 - (ii) Tracks, or enables Canada to track, disclosures of Canada Data, including what data has been disclosed, to whom, and at what time.

ANNEX F

TASK AUTHORIZATION FORM

TASK AUTHORIZATION (TA) FORM				
Contractor:		Contract Number:		
Commitment: #		Financial Coding:		
Task Number (Amendment):		Issue Date:	Response Require By:	
1. Statement of Work (Work Activities, Certifications and Deliverables)				
See attached for Statement of Work and Certifications required.				
2. Period of Service:	From (Date)		To (Date)	
3. Work Location:				
4. Travel Requirements:				
5. Language Requirement:				
6. Other Conditions/Constraints:				
7. Level of Security Clearance required for the Contractor Personnel:				
8. Contractor's Response:				
Category and Name of Proposed Resource	PSPC Security File Number	Per Diem Rate	Estimated # of Days	Total Cost
Estimated Cost				
Applicable Taxes				
Total Labour Cost				
Total Travel & Living Cost				

TASK AUTHORIZATION (TA) FORM	
Firm Price or Maximum TA Price	
Contractor's Signature	
Name, Title and Signature of Individual Authorized to sign on behalf of the Contractor (type or print) _____ _____	Signature: _____ Date: _____
Approval – Signing Authority	
Signatures (Client) Name, Title and Signature of Individual Authorized to sign: Technical Authority: _____ Date: _____	Signatures (PSPC) Contracting Authority ¹ : _____ Date: _____
¹ Signature required for TA valued at (<i>AMOUNT TO BE UPDATED AT CONTRACT AWARD</i>) or more, Applicable Taxes included.	
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 in any attached sheets at the price set out thereof.	

APPENDIX A TO ANNEX F

CERTIFICATIONS AT THE TASK AUTHORIZATION STAGE

The following Certifications are to be used, as applicable. If they apply, they must be signed and attached to the Contractor's quotation when it is submitted to Canada.

1. CERTIFICATION OF EDUCATION AND EXPERIENCE

The Contractor certifies that all the information provided in the résumés and supporting material proposed for completing the subject work, particularly the information pertaining to education, achievements, experience and work history, has been verified by the Contractor to be true and accurate. Furthermore, the Contractor warrants that every individual proposed by the Contractor for the requirement is capable of performing the Work described in the Task Authorization.

Print name of authorized individual & sign above

Date

2. CERTIFICATION OF AVAILABILITY OF PERSONNEL

The Contractor certifies that, should it be authorized to provide services under this Task Authorization, the persons proposed in the quotation will be available to commence performance of the work within a reasonable time from the date of issuance of the valid Task Authorization, or within the time specified in the TA Form, and will remain available to perform the work in relation to the fulfillment of the requirement.

Print name of authorized individual & sign above

Date

3. CERTIFICATION OF STATUS OF PERSONNEL

If the Contractor has proposed any individual who is not an employee of the Contractor, the Contractor certifies that it has permission from that individual to propose his/her services in relation to the Work to be performed under this TA and to submit his/her résumé to Canada. At any time during the Contract the Contractor must, upon request from the Contracting Authority, provide the written confirmation, signed by the individual, of the permission that was given to the Contractor of his/her availability. Failure to comply with the request may result in a default under the Contract in accordance with the General Conditions.

Print name of authorized individual & sign above

Date

Solicitation No. - N° de l'invitation
0X001-190594/A
Client Ref. No. - N° de réf. du client
0X001-190594

Amd. No. - N° de la modif.
-
File No. - N° du dossier
108xl0X001-190594

Buyer ID - Id de l'acheteur
108 XL
CCC No./N° CCC - FMS No./N° VME

4.CERTIFICATION OF LANGUAGE

The Contractor certifies that the proposed resource(s) in response to this draft Task Authorization is/are fluent in English. The individual(s) proposed must be able to communicate orally and in writing in English without any assistance and with minimal errors.

Print name of authorized individual & sign above

Date

ANNEX G

BID EVALUATION CRITERIA

GENERAL

Purpose

This document outlines the bid evaluation process of the *Next Generation Digital Learning Experience Solution*.

Instructions

Bidders must be assessed in accordance with the following instructions and criteria as detailed within this document. The following instructions shall apply to the bidder evaluation:

Mandatory requirements are identified by the word "must". All mandatory requirements must be met in order to meet compliance with the requirements;

Bid submissions must address all criteria identified in Appendix H with complete supporting detail. Insufficient information to substantiate compliance or a nil response may result in the rejection of a response and may result in the bid submission rated as non-compliant. Bidders must provide a complete technical and functional specification proposal which must describe in detail how they meet the following mandatory criteria. The Bidders must identify where this information can be found in their proposal.

References to other websites are not acceptable to meet this requirement. Canada will evaluate only the documentation provided with a Bidder's bid. Canada will not evaluate information such as references to websites where additional information can be found, or technical manuals or brochures not submitted with the bid. Relevant website references may be printed and included in proposal to support technical compliance.

Bid submissions should provide documentation, such as any videos, brochures, pamphlets, and or test results, with full explanation and background testing certification, if applicable, in order to show that every aspect of the proposed solution is compliant.

1.0 STAGE 1: EVALUATION OF BIDDER'S PROPOSAL

1.1 Mandatory Criteria

The bid must meet all the mandatory criteria specified below. Bids that fail to meet all the mandatory technical criteria will be declared non-responsive. Each mandatory technical criterion should be addressed separately.

For Requirements MC-11 to MC-23, demonstrate the following functionality mentioned below via a video demonstration to be submitted as part of the bid.

MC No.	Requirement Description	Compliant		Reference:
		Yes	No	
Background/qualifications requirements				
MC-1	<p>Experience</p> <p>The Bidder must provide a description of their company's experience in the implementation of Learning Management Solutions. The Bidder must demonstrate this experience by describing 3 projects similar in size and scope to Appendix A – Statement of Work, including:</p> <ul style="list-style-type: none"> • client name; • project name; • project timeline (start and end dates); • project manager; • the breadth of the solution implemented; and • whether the project was completed on schedule and/or within the budget. 			
MC-2	<p>Multilingual Interface and Support</p> <p>The solution must be 100% bilingual (Canadian French and English) on all platforms offered. This means users selecting French as their language will not see anything in English in the solution's GUI, including but not limited to help files, tutorials, error</p>			

MC No.	Requirement Description	Compliant		Reference:
		Yes	No	
	<p>messages and legal information. (User-generated content is excluded). If your solution is not 100% bilingual as described above, provide a detailed roadmap indicating the delays required by your company to produce and deliver – at no additional cost to the CSPS – a completely bilingual solution.</p> <p>The Bidder must also demonstrate how it regularly provides on-going support and maintenance services, as well as help desk support in English and French.</p>			
Planning				
MC-3	<p>Project Plan and Methodology</p> <p>The Bidder must submit an overall Project Implementation Plan that will ensure the successful deployment of their proposed Solution.</p> <p>The Project Implementation Plan must contain:</p> <ul style="list-style-type: none"> • a description of the Bidder's implementation approach; • an implementation methodology; including project phases; • implementation best practices; • roles and responsibilities on each task for the Bidder and School; and • Change Control, tools or models to be used by the Bidder for best practice implementations. 			
Technical requirements				
MC-4	<p>Reporting and Analytics</p> <p>The Bidder's proposed Solution must demonstrate the ability to provide real-time analytics, and produce ad hoc and customized reports.</p>			

MC No.	Requirement Description	Compliant		Reference:
		Yes	No	
MC-5	<p>Multi-Tenancy</p> <p>The Bidder's proposed Solution must support multi-tenancy, including a hierarchy of separate department/agencies, organizational units within a department, and faculties/business lines. The solution must support segmenting and sharing of users and content across these partitions along with individual branding of partitions.</p>			
Application integration requirements				
MC-6	<p>Application Programming Interface</p> <p>The Bidder's proposed Solution must implement a RESTful Application Programming Interface (API) and provide evidence of such integrations.</p>			
MC-7	<p>Learning Record Store</p> <p>The Bidder's proposed Solution must support xAPI to enable tracking of learning progress outside the platform and a learning record store in order to maintain records of learning activities.</p>			
MC-8	<p>Integration with Webex</p> <p>The Bidder's proposed Solution must have turnkey integration with Webex Meeting, Training and Events Centre.</p>			
MC-9	<p>Single Sign-On/Single Log-Out (SSO/SLO)</p>			

MC No.	Requirement Description	Compliant		Reference:
		Yes	No	
Accessibility requirements				
MC-10	<p>WCAG 2.0 A Conformance Statement</p> <p>The Bidder must describe how it documents the conformance of its system to the World Wide Web Consortium (WC) WCAG 2.0 guidelines Success Criteria Level A or higher, including:</p> <ul style="list-style-type: none"> the Bidder's accessibility statement; and the Bidder's methodology used to ascertain conformance. 			
functional REQUIREMENTS -				
<i>For Requirements MC-11 to MC-23, demonstrate the following functionality mentioned below via a video demonstration</i>				
Catalogue Management				
MC-11	<p>The Bidder's proposed Solution must support the management of a comprehensive enterprise-wide learning product catalogue, including a configurable internal catalogue visible to users once they've logged in and configurable external one visible on web for users not logged into the platform, including:</p> <ul style="list-style-type: none"> events in-class courses online self-paced e-learning, distance learning synchronous virtual classroom standalone media (such as videos, podcasts, images, documents). 			
Resource Management				

MC No.	Requirement Description	Compliant		Reference:
		Yes	No	
MC-12	The solution must integrate tools to manage instructors, rooms and associated resources used in training activities, including management and scheduling of instructors, rooms and other resources required to deliver courses and events.			
Offering and Registration Management				
MC-13	The Bidder's proposed Solution must support the scheduling and management of learning product offerings across multiple time zones, including the management of the related registration and waiting list business rules.			
Learning Planning				
MC-14	The Bidder's proposed Solution must: <ul style="list-style-type: none"> manage a catalogue of competencies and allow for the mapping of learning content to competencies; allow individual learners to self-assess against published competencies; enable multi-rater assessments of individual learner competencies by peers or managers; support automated push of learning content and system-generated recommendations to bridge identified learning gaps; and provide analytics and reporting at the organizational or enterprise level to identify work unit, organizational or enterprise wide learning gaps. 			
Notification Management				
MC-15	The Bidder's proposed Solution must support the management of detailed and timely notifications to all users, including the following:			

MC No.	Requirement Description	Compliant		Reference:
		Yes	No	
User Management				
MC-16	<p>The Bidder's proposed Solution must support configurable user accounts, including:</p> <ul style="list-style-type: none"> learners; instructors; training coordinators; and system administrators. 			
Learning Management				
MC-17	<p>The Bidder's proposed Solution must allow:</p> <ul style="list-style-type: none"> administrators to assign training to groups of targeted learners and report on learners' progress; and managers to assign learning content to employees within their work unit, view progress, view summaries of learner progress towards course or certification completion. 			
Profile Management				
MC-18	<p>The Bidder's proposed Solution must be able to allow users to freely update some of their profile information depending on their department, classification and level, including the following:</p> <ul style="list-style-type: none"> name; password; 			

MC No.	Requirement Description	Compliant		Reference:
		Yes	No	
Audit Management				
MC-19	The Bidder's proposed Solution must be able to manage audit records concerning access and changes to both the Solution configuration and data.			
Learner Experience				
MC-20	The Bidder must demonstrate how its proposed Solution supports and engages learners in their learning journey and must include: <ul style="list-style-type: none"> comprehensive search and filter capabilities; competency-based discovery of content by learners; learning paths; personal dashboards; and usage based recommendations. 			
Online Course Authoring Tools				
MC-21	The Bidder must demonstrate how its proposed Solution supports self-service course authoring for instructors, including tools to: <ul style="list-style-type: none"> enable collaboration between learners; enable instructors to share and reuse learning objects; preview and test course content; and publish online course content for learners. 			

MC No.	Requirement Description	Compliant		Reference:
		Yes	No	
Tools for Instructors				
MC-22	<p>Content Editor (WYSIWYG)</p> <p>The Bidder's proposed Solution must include a WYSIWYG* content editor that allows the manipulation of the following for the purpose of authoring and editing content pages, including:</p> <ul style="list-style-type: none"> • text; • images; • hyperlinks; and • a video and audio player. <p>*WYSIWYG = What you see is what you get.</p>			
MC-23	<p>The Bidder's proposed Solution must allow content to be viewable on, without requiring any additional plug-ins, any browser across all common operating systems, including the following:</p> <ul style="list-style-type: none"> • mobile device; • tablet; and • desktop. 			

1.2 Point Rated Technical Criteria

Bids will be evaluated and scored as specified in the table inserted below. Each point rated technical criterion should be addressed separately.

Bids which fail to obtain the overall minimum required score specified below will be declared non-responsive, and will be given no further consideration in the evaluation process.

For the following 23 Point Rated Criteria, Bidders should provide a "sandbox" Solution with access for five evaluation committee members for up to two months to assess the following requirements.

PRC No.	Requirement Description	Point Rated Grid	Reference	Score
PRC-1	<p>Application Integration Requirements</p> <p>Interoperability with technologies through the Learning Tools Interoperability (LTI) standard.</p> <p>The Bidder's proposed Solution should demonstrate how it can integrate with the School's existing open source learning platforms via Learning Tools Integration and define which level of LTI is supported for integration with:</p> <ul style="list-style-type: none"> Moodle 3.5+; and Kaltura Community Edition. 	<p>Maximum 10 points</p> <p>Maximum 5 points for the ability to integrate with each of the Schools learning technology ecosystem application.</p> <p>For each application listed;</p> <p>0 pts = None - no integration supported</p> <p>3 pts = Support for LTI 1.1</p> <p>5 pts = Support for LTI 1.3</p>		
PRC-2	<p>3rd Party Off the Shelf Learning Content Integrations</p> <p>The Bidder's proposed Solution should provide turnkey real-time integration with cloud-based, 3rd party learning content providers.</p>	<p>Maximum 5 points</p> <p>0 pts = None - no integration supported</p> <p>3 pts = Partial/ Limited integration supported</p>		

PRC-3	<p>Integration with Web Analytics</p> <p>The Bidder's proposed Solution should provide real-time integration with the following web analytics platforms:</p> <ul style="list-style-type: none"> • Google Analytics; and • Matomo Web Analytics. 	<p>5 pts = Full turnkey integration supported.</p> <p>Maximum 10 points</p> <p>For each application listed;</p> <p>0 pts = None - no integration supported/documented</p> <p>3 pts = Partial/ Limited integration supported/documented or only one of Google/Matomo</p> <p>5 pts = Full turnkey integration supported/documented with either Google or Matomo</p> <p>10 pts = Full turnkey integration supported/documented with both Google and Matomo</p>	
Project Management Deliverable Requirements			
PRC-4	<p>Work Plan, Assumptions & Deliverables</p> <p>The Bidder should provide a Project Management Plan containing information on the following:</p> <ol style="list-style-type: none"> 1. Work Plan: A detailed work plan reflecting a logical, best practice method. The work plan should reflect a detailed Work Breakdown Structure (WBS) illustrating project phases, tasks, sub-tasks, deliverables and assumptions. 2. Project Organization Chart: Identification of the Bidder's proposed key resources and their respective roles and responsibilities. 	<p>Maximum 25 points</p> <p>0 pts = Poor – Project management plan missing core aspects.</p> <p>15 pts = Adequate – Project management plan sufficiently outlines a plan, but lacks key details on processes, mechanisms to fully meet the requirement.</p> <p>25 pts = Excellent – Project management plan fully details processes, mechanisms and plans to fully meet the requirement.</p>	

	<p>3. Risks: The Bidder's description of risks and mitigation strategies.</p>		
<p>PRC-5</p>	<p>Training Plan</p> <p>The Bidder should describe the Training Plan and support strategy associated with its proposed Solution, including:</p> <ul style="list-style-type: none"> • an overview of proposed training plan/strategy; and • details on how and when training is to be delivered for both on-site and off-site training, web training services for the core project team, end users, and technology personnel (if required). 	<p>Maximum 20 points</p> <p>0 pts = Poor – Training Plan was not provided</p> <p>14 pts = Adequate – Training Plan sufficiently outlines a plan, but lacks key details on processes, mechanisms to fully meet the requirement.</p> <p>20 pts = Excellent – Training Plan fully details processes, mechanisms and plans to engage users and fully meet the requirement.</p>	
Accessibility Requirements			
<p>PRC-6</p>	<p>Accessibility Criteria</p> <p>The Bidder should demonstrate how and at what level their Solution conforms to the World Wide Web Consortium (WC) WCAG 2.X guidelines Success Criteria for:</p> <ul style="list-style-type: none"> • Learner functionality; • Internal (i.e. administrative) functionality; and • Bidder's product release cycle. <p>The Bidder should describe in detail how accessibility is built into their proposed solution from the standpoint of their release cycle.</p>	<p>Maximum 10 points</p> <p>For each item listed;</p> <p>0 pts = The Solutions does not meet WCAG 2.0 A minimum.</p> <p>4 pts = The Solutions meets WCAG 2.0 AA or 2.1 A.</p> <p>7 pts = The Solutions meets WCAG 2.0 AA or 2.1 A with an actionable plan or product release cycle to move to WCAG 2.1 AA or higher.</p> <p>10 pts = The Solution meets WCAG 2.1 AA or higher.</p>	
Multi-Language Toggle			
<p>PRC-7</p>	<p>The Bidder should demonstrate how its proposed Solution allows users to toggle the</p>	<p>Maximum 5 points</p>	

	user interface between French and English languages from anywhere in the solution without losing the page context.	<p>0 pts = No demonstration provided/ no information provided</p> <p>3 points = partially demonstrated to meet the requirement</p> <p>5 points = Fully demonstrated to meet the requirement</p>	
User Interface/Usability			
PRC-8	<p>Offline Access</p> <p>The Bidder should demonstrate how its proposed Solution allows for working offline and synchronization for all users/roles in the following roles:</p> <ul style="list-style-type: none"> • Learners; and • Instructors. 	<p>Maximum 5 points</p> <p>0 pts = No demonstration provided / no information provided</p> <p>3 points = partially demonstrated to meet the requirement</p> <p>5 points = Fully demonstrated to meet the requirement</p>	
PRC-9	<p>Mobile Access/Responsive Design</p> <p>The Bidders should demonstrate how its proposed Solution supports mobile friendly user interfaces for those using mobile and tablet devices via responsive web design.</p>	<p>Maximum 5 points</p> <p>0 pts = No demonstration provided/ no information provided</p> <p>3 points = partially demonstrated to meet the requirement</p> <p>5 points = Fully demonstrated to meet the requirement.</p>	
Authentication/User Accounts			
PRC-10	<p>Self-Service Account Creation</p> <p>The Bidder should demonstrate how its proposed Solution allows users to self-register a learner account and/or link to using an existing authentication solution.</p>	<p>Maximum 5 points</p> <p>0 pts = No demonstration provided/ no information provided</p> <p>3 points = partially demonstrated to meet the requirement</p>	

		5 points = Fully demonstrated to meet the requirement	
Integrated/Federated Course Catalog			
PRC-11	<p>Learning Paths and Certifications</p> <p>The Bidder should demonstrate how its proposed Solution allows for the creation of learning paths and certifications, including</p> <ul style="list-style-type: none"> • Allowing administrators to create, manage and publish personal learning paths; and • Allowing administrators to create certifications enabling learners to earn certification by completing designated courses, learning plan or external training activities. 	<p>Maximum 5 points</p> <p>0 pts = No demonstration provided/ no information provided</p> <p>3 points = partially demonstrated to meet the requirement</p> <p>5 points = Fully demonstrated to meet the requirement</p>	
PRC-12	<p>Learning Offerings</p> <p>The Bidder should demonstrate how its proposed Solution will allow the School to manage and publish a single federated catalogue and determine, through configuration, which (content), where (platform, i.e. NGDLE or Internet) and when content is visible, and to whom (authenticated users, sub groups of users/system tenants and non-authenticated users) all or part of the catalogue is visible, using various interactive formats including:</p> <ul style="list-style-type: none"> • list; • map; • printable format; and • calendar. 	<p>Maximum 10 points</p> <p>0 pts = No demonstration provided/ no information provided</p> <p>5 points = partially demonstrated to meet the requirement</p> <p>10 points = Fully demonstrated to meet the requirement</p>	
PRC-13	<p>Sharing/User Recommendations</p> <p>The Bidder should demonstrate how its proposed Solution allows users (to share</p>	<p>Maximum 5 points</p> <p>0 pts = No demonstration provided/ no information provided</p>	

	<p>learning products in the learning catalogue with colleagues and friends both</p> <ul style="list-style-type: none"> • within the platform with authenticated users; and • outside the platform via common social media (ex: Twitter, LinkedIn etc.) 	<p>3 points = partially demonstrated to meet the requirement 5 points = Fully demonstrated to meet the requirement</p>	
Tools for Online Learners			
PRC-14	<p>Course Collaboration Tools</p> <p>The Bidder's proposed Solution should include the following tools in digital learning spaces/courses:</p> <ol style="list-style-type: none"> 1. Discussion posts, threads, and forums, and ability to search post content; 2. Peer assessment tool within courses; 3. Assignment submission tool; 4. Audio, video, and written feedback on assignments; 5. Calendar links to assignments and activity due dates; 6. Ability to subscribe to the calendar and integrate it with their personal calendars through CalDAV, or some equivalent calendar standard protocol; 7. Audio/video recording ability, allowing instructors and learners to contribute audio/video content to courses activities; 8. Internal messaging platform for students and instructors to communicate with each other; and 9. Web conferencing features. 	<p>Maximum 18 points 2 points per item</p>	

<p>PRC-15</p>	<p>Gamification</p> <p>The Bidder should demonstrate how its proposed Solution would allow the School to apply gaming concepts to its digital learning offerings, including:</p> <ul style="list-style-type: none"> • Points; • Leaderboards; • Badges; • Levels; and • Rewards. 	<p>Maximum of 10 points.</p> <p>2 points per demonstrated gamification function</p>		
<p>PRC-16</p>	<p>User and System Personalization and Recommendations</p> <p>The Bidder should demonstrate how its proposed Solution:</p> <ul style="list-style-type: none"> • Recommends learning based on their data, preferences, interests, similar people with similar interests, content ratings, position requirements, departmental requirements & government requirements; • Displays relevant learner-determined and/or manager or organizationally determined learning content first; • Asks learners a series of questions to identify personalization criteria upon first log in; • Allows learners to update their own personalization criteria at any time; • Tags learning content to multiple criteria such as competency, topics, 	<p>Maximum 20 points</p> <p>2 points per demonstrated personalization function</p>		

	<p>role, level, delivery type, content ratings, etc.;</p> <ul style="list-style-type: none"> Allows learners to rate content and instructors; Allows learners to bookmark, add to wish list and favorite learning content for later use; Recommends related follow-up content to learners after content completion; Improves the marketing of content such as new, retiring, low registration, geographically-related or seasonal learning recommendations; and Allows learners to see their progression through courses. 			
Tools for Online Instructors				
PRC-17	<p>Course Templates</p> <p>The Bidder should demonstrate how its proposed Solution provides the ability to create courses based templates, such as departmental or School-specific templates.</p>	<p>Maximum 5 points</p> <p>0 pts = No demonstration provided/ no information provided</p> <p>3 points = partially demonstrated to meet the requirement</p> <p>5 points = Fully demonstrated to meet the requirement</p>		
PRC-18	<p>Course/Learner Analytics for Instructors</p> <p>The Bidder should demonstrate how its proposed Solution provides instructors with easy to use, real-time analytics and reporting related to the following:</p> <ul style="list-style-type: none"> learner course access; time spent in content; and enrolment data. 	<p>Maximum 5 points</p> <p>0 pts = No demonstration provided/ no information provided</p> <p>3 points = partially demonstrated to meet the requirement</p> <p>5 points = Fully demonstrated to meet the requirement</p>		

<p>PRC-19</p>	<p>Selective Release of Course Materials/Content based on Conditions</p> <p>The Bidder should demonstrate how its proposed Solution allows restrictions on releasing content, modules, lessons, or elements of a course by Instructors in the following:</p> <ul style="list-style-type: none"> • Requiring completion of one topic in a course before second topic is made available; • Automated trigger to send a reminder email to learners who have not yet started a course, completed a required quiz or submitted a required assignment within the course; • Requiring viewing course content such as a video or file before gaining access to a quiz; and • Requiring posting to a discussion topic before a learner can see a content module. 	<p>Maximum of 8 points.</p> <p>2 points per demonstrated function</p>	
Notifications			
<p>PRC-20</p>	<p>Opt-Out of Notifications</p> <p>The Bidder should demonstrate how its proposed Solution allows users to opt-out of messages at the following levels:</p> <ul style="list-style-type: none"> • Granular level; • Site-wide; and • Course-wide. 	<p>Maximum 5 points</p> <p>0 pts = None of the elements demonstrated</p> <p>3 points = 1 of 3 elements demonstrated in the proposed Solution</p> <p>5 points = 2 or more of the elements demonstrated in the proposed Solution</p>	

Resource and Offering Management		Maximum 10 points total
PRC-21	<p>The Bidder should demonstrate how its proposed Solution manages learning product offerings and schedules including:</p> <ul style="list-style-type: none"> • Availability: <ul style="list-style-type: none"> ○ to groups of users, instructors, resources; and ○ for periods of time. • Registration: <ul style="list-style-type: none"> ○ limits; ○ waiting list; ○ cancellation ○ open/closed; ○ self-registration vs. by invitation; • Assigning courses; • Attendance/Completion; and • Expiration. 	<p>Max 1 point for each of the elements covered under availability and registration as follows:</p> <p>0 pts = Not covered or demonstrated</p> <p>1 point = Fully covered and demonstrated.</p>
PRC-22	<p>The Bidder should demonstrate how its proposed Solution supports simultaneous offerings of the same learning product in multiple formats and modes, including:</p> <ul style="list-style-type: none"> • Virtual; • on-site; and • self-paced online. 	<p>Maximum 5 points</p> <p>0 pts = No demonstration provided/ no information provided</p> <p>3 points = partially demonstrated to meet the requirement</p> <p>5 points = Fully demonstrated to meet the requirement</p>
Flexible Analytics, Learning Assessment and Evaluation		Maximum 25 points
PRC-23	<p>The Bidder should demonstrate how its proposed Solution provides detailed, real-time analytics and insights on the usage, effectiveness and efficiency of learning content at an individual, team, organizational or enterprise level, including:</p>	<p>5 points per demonstrated analytics component</p>

	<ul style="list-style-type: none"> • Number and duration of views of learning content; • Registration, attendance and completion rates of formal learning; • Learner performance and progress within courses or across content linked to competencies; • Learner satisfaction and approval of learning content; and • Business metrics with respect to training demand and operations, waitlist management, instructor and resource utilization. 			
			<p>Maximum points: 231</p> <p>Minimum pass mark: 162</p>	<p>Total score</p>

ANNEX H

BIDDER FORMS

FORM 1 – BIDDER'S FORMS

BID SUBMISSION FORM													
<p>Bidder's full legal name</p> <p><i>[Note to Bidders: Bidders who are part of a corporate group should take care to identify the correct corporation as the Bidder.]</i></p>													
<p>Authorized Representative of Bidder for evaluation purposes (e.g., clarifications)</p>	<table border="1" style="width: 100%;"> <tr> <td style="width: 30%;">Name:</td> <td></td> </tr> <tr> <td>Title:</td> <td></td> </tr> <tr> <td>Address:</td> <td></td> </tr> <tr> <td>Telephone #:</td> <td></td> </tr> <tr> <td>Fax #:</td> <td></td> </tr> <tr> <td>Email:</td> <td></td> </tr> </table>	Name:		Title:		Address:		Telephone #:		Fax #:		Email:	
Name:													
Title:													
Address:													
Telephone #:													
Fax #:													
Email:													
<p>Bidder's Procurement Business Number (PBN)</p> <p><i>[see the Standard Instructions 2003]</i></p> <p><i>[Note to Bidders: Please ensure that the PBN you provide matches the legal name under which you have submitted your bid. If it does not, the Bidder will be determined based on the legal name provided, not based on the PBN, and the Bidder will be required to submit the PBN that matches the legal name of the Bidder.]</i></p>													
<p>Jurisdiction of Contract:</p> <p>Province or Territory in Canada the Bidder wishes to be the legal jurisdiction applicable to any resulting contract (if other than as specified in solicitation)</p>													
<p>Former Public Servants</p> <p>See the Article in Part 2 of the bid solicitation entitled "Former Public Servant" for a definition of "Former Public Servant".</p>	<p>Is the Bidder a FPS in receipt of a pension as defined in the bid solicitation?</p> <p>Yes ____ No ____</p> <p>If yes, provide the information required by the Article in Part 2 entitled "Former Public Servant "</p>												

BID SUBMISSION FORM									
	<p>Is the Bidder a FPS who received a lump sum payment under the terms of the terms of the Work Force Adjustment Directive?</p> <p>Yes _____ No _____</p> <p>If yes, provide the information required by the Article in Part 2 entitled "Former Public Servant "</p>								
<p>Canadian Content Certification</p> <p>As described in the solicitation, bids with at least 80% Canadian content are being given a preference.</p> <p><i>[For the definition of Canadian goods and services, consult the PWGSC SACC clause A3050T]</i></p>	<p>On behalf of the Bidder, by signing below, I confirm that <i>[check the box that applies]</i>:</p>								
	<table border="1" style="width: 100%;"> <tr> <td style="width: 80%;">At least 80 percent of the bid price consists of Canadian goods and services (as defined in the solicitation)</td> <td style="width: 20%;"></td> </tr> <tr> <td>Less than 80 percent of the bid price consists of Canadian goods and services (as defined in the solicitation)</td> <td></td> </tr> </table>	At least 80 percent of the bid price consists of Canadian goods and services (as defined in the solicitation)		Less than 80 percent of the bid price consists of Canadian goods and services (as defined in the solicitation)					
	At least 80 percent of the bid price consists of Canadian goods and services (as defined in the solicitation)								
Less than 80 percent of the bid price consists of Canadian goods and services (as defined in the solicitation)									
<p>Hardware:</p> <p><i>(Contracting Authority should only insert when Supplemental General Conditions 4001 have been inserted in Part 7).</i></p>	<table border="1" style="width: 100%;"> <tr> <td style="width: 70%;">Toll-Free Telephone Number for maintenance services:</td> <td></td> </tr> <tr> <td>Website for maintenance services:</td> <td></td> </tr> </table>	Toll-Free Telephone Number for maintenance services:		Website for maintenance services:					
	Toll-Free Telephone Number for maintenance services:								
Website for maintenance services:									
<p>Licensed Software Maintenance and Support:</p> <p><i>(Contracting Authority should only insert when supplemental General Conditions 4004 has been inserted in Part 7).</i></p>	<table border="1" style="width: 100%;"> <tr> <td style="width: 70%;">Toll-free Telephone Access:</td> <td></td> </tr> <tr> <td>Toll-Free Fax Access:</td> <td></td> </tr> <tr> <td>E-Mail Access:</td> <td></td> </tr> <tr> <td>Website address for web support:</td> <td></td> </tr> </table>	Toll-free Telephone Access:		Toll-Free Fax Access:		E-Mail Access:		Website address for web support:	
	Toll-free Telephone Access:								
	Toll-Free Fax Access:								
	E-Mail Access:								
Website address for web support:									
<p>Security Clearance Level of Bidder</p> <p>[include both the level and the date it was granted]</p> <p>[Note to Bidders: Please ensure that the security clearance matches the legal name of the Bidder. If it does not, the security clearance is not valid for the Bidder.]</p>									
<p>On behalf of the Bidder, by signing below, I confirm that I have read the entire bid solicitation including the documents incorporated by reference into the bid solicitation and I certify that:</p> <ol style="list-style-type: none"> 1. The Bidder considers itself and its products able to meet all the mandatory requirements described in the bid solicitation; 2. This bid is valid for the period requested in the bid solicitation; 3. All the information provided in the bid is complete, true and accurate; and 4. If the Bidder is awarded a contract, it will accept all the terms and conditions set out in the resulting contract clauses included in the bid solicitation. 									

Solicitation No. - N° de l'invitation
0X001-190594/A
Client Ref. No. - N° de réf. du client
0X001-190594

Amd. No. - N° de la modif.
-
File No. - N° du dossier
108xl0X001-190594

Buyer ID - Id de l'acheteur
108 XL
CCC No./N° CCC - FMS No./N° VME

BID SUBMISSION FORM	
Signature of Authorized Representative of Bidder	<hr/>

FORM 2 - CLOUD SERVICE PROVIDER LETTER OF ATTESTATION

Name of Respondent _____

This authorization applies to the following proposed Commercially Available Public Cloud Service (Name of the Propose solution):

The Respondent declares that is underlying infrastructure and platforms is hosted on a Commercially Available Public Cloud Services:

The definition of "Cloud Service Provider" for the purposes of this certification can be found in Annex D – Definitions and Interpretations of the Request for Proposal.

Cloud Service Provider _____

Cloud Service Provider Data Center Location _____

Signature of authorized signatory of CSP _____

Print Name of authorized signatory of CSP _____

Print Title of authorized signatory of CSP _____

Address for authorized signatory of CSP _____

Telephone no. for authorized signatory of CSP _____

Fax no. for authorized signatory of CSP _____

Date signed _____

FORM 3 – SOFTWARE PUBLISHER CERTIFICATION FORM

Form 3
Software Publisher Certification Form
(to be used where the Bidder itself is the Software Publisher)

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

[Bidders should add or remove lines as needed]

FORM 4 – SOFTWARE PUBLISHER AUTHORIZATION FORM

Form 4
Software Publisher Authorization Form
(to be used where the Bidder is not the Software Publisher)

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

This authorization applies to the following software products:

[Bidders should add or remove lines as needed]

Name of Software Publisher (SP) _____

Signature of authorized signatory of SP _____

Print Name of authorized signatory of SP _____

Print Title of authorized signatory of SP _____

Address for authorized signatory of SP _____

Telephone no. for authorized signatory of SP _____

Fax no. for authorized signatory of SP _____

Date signed _____

Solicitation Number _____

Name of Bidder _____

	Yes	No	Comments
52: False or misleading representation 53: deceptive notice of winning a prize			
Corruption of Foreign Public Officials Act 3: Bribing a foreign public official 4: Accounting 5: Offence committed outside Canada	<input type="checkbox"/>	<input type="checkbox"/>	
Controlled Drugs and Substance Act 5: Trafficking in substance 6: Importing and exporting 7: Production of substance	<input type="checkbox"/>	<input type="checkbox"/>	
Other Acts 239: False or deceptive statements of the Income Tax Act 327: False or deceptive statements of the Excise Tax Act	<input type="checkbox"/>	<input type="checkbox"/>	

Additional Comment

- I, (name) _____, (position) _____, of (company name bidder) _____ authorise PWGSC to collect and use the information provided, in addition to any other information that may be required to make a determination of ineligibility and to publicly disseminate the results.
- I, (name) _____, (position) _____, of (company name bidder) _____ certify that the information provided in this form is, to the best of my knowledge, true and complete. Moreover, I am aware that any erroneous or missing information could result in the cancellation of my bid as well as a determination of ineligibility/suspension.

We appreciate your interest in doing business with The Government of Canada and your understanding on the additional steps that we need to take to protect the integrity of PWGSC's procurement process.

FORM 6 - LIST OF NAMES FORM

In accordance with Part 5, Article 5.3, – Integrity Provision – List of Names, please complete the Form below.

Complete Legal Name of Company	
Company's address	
Company's Procurement Business Number (PBN)	
Solicitation number	
Board of Directors (Use Format – first name last name) Or put the list as an attachment	
1. Director	
2. Director	
3. Director	
4. Director	
5. Director	
6. Director	
7. Director	
8. Director	
9. Director	
10. Director	
Other members	
Comments	

FORM 7 - LIST OF NAMES FORM

Form 7 to Part 5 – Bid Solicitation (*insert if applicable*) FEDERAL CONTRACTORS PROGRAM FOR EMPLOYMENT EQUITY – CERTIFICATION

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

I, the Bidder, by submitting the present information to the Contracting Authority, certify that the information provided is true as of the date indicated below. The certifications provided to Canada are subject to verification at all times. I understand that Canada will declare a bid non-responsive, or will declare a contractor in default, if a certification is found to be untrue, whether during the bid evaluation period or during the contract period. Canada will have the right to ask for additional information to verify the Bidder's certifications. Failure to comply with 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 and Social Development Canada \(ESDC\)](#) - Labours' website.

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

Complete both A and B.

A. Check only one of the following:

- A1. The Bidder certifies having no work force in Canada.
- A2. The Bidder certifies being a public sector employer.
- A3. The Bidder certifies being a [federally regulated employer](#) being subject to the *Employment Equity Act*.
- A4. The Bidder certifies having a combined work force in Canada of less than 100 employees (combined work force includes: permanent full-time, permanent part-time and temporary employees [temporary employees only includes those who have worked 12 weeks or more during a calendar year and who are not full-time students]).
- A5. The Bidder has a combined workforce in Canada of 100 or more employees; and
 - A5.1 The Bidder certifies already having a valid and current [Agreement to Implement Employment Equity](#) (AIEE) in place with 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 Federal Contractors Program for Employment Equity - Certification. (Refer to the Joint Venture section of the Standard Instructions).

FORM 8 - ELECTRONIC PAYMENT INSTRUMENTS

As indicated in Part 3, clause 3.1.2, the Bidder must identify which electronic payment instruments they are willing to accept for payment of invoices.

The Bidder accepts any of the following Electronic Payment Instrument(s):

- VISA Acquisition Card;
- MasterCard Acquisition Card;
- Direct Deposit (Domestic and International);
- Electronic Data Interchange (EDI);
- Wire Transfer (International Only);
- Large Value Transfer System (LVTS) (Over \$25M)

FORM 9 - FINANCIAL BID PRESENTATION SHEET

1. Work

(a) Phase 1 - Work to develop and deliver a CUA Solution Prototype

Table 1 - Firm All-Inclusive Price (applicable taxes extra) for the Work described in article 2. Phase 1 Prototype Solution of the Statement of Work in Annex A, including granting Solution access which includes all Solution usage rights grants, Software Documentation, Warranty, Hosting and Maintenance and Support (excluding Training), waivers, non-disclosure agreements, or other releases to Canada for purposes of conducting the CUA assessment; for up to 200 Authorized Users to use the Prototype Solution for Capability and Usability Assessment purposes during the initial contract period:

Item # (A)	Description (B)	Firm All-Inclusive Price (C1)
1	All deliverables associated with Article 2. Phase 1 – Prototype Solution in Annex A – Statement of Work.	\$30,000.00 CAD (excluding any applicable taxes)
Total Evaluated Bid Price = C1		\$30,000.00 CAD (excluding any applicable taxes)

2. Optional Goods and Services

(a) Phase 2 – Delivery of the Solution

- (i) At Canada's sole discretion, Canada may exercise the irrevocable option to deliver the production-ready Solution in accordance with article 3. Phase 2 - Solution of Annex A – Statement of Work.

Table 2 - Firm All-Inclusive Price (applicable taxes extra) for the Work described in article 3. Phase 2 - Solution of Annex A – Statement of Work. including access which includes all Solution usage rights grants, Software Documentation, Warranty, Hosting and Maintenance and Support (excluding Training), waivers, non-disclosure agreements, or other releases to Canada for up to 260,000 Authorized Users :

Item # (A)	Description (B)	Firm All-Inclusive Price – (C2)
1	All deliverables associated with Article 3. Phase 2 – Solution of the Statement of Work in Annex A	\$
Total Evaluated Bid Price = C2		\$

(b) Authorized User Access to Solution

Table 3 - Firm all-inclusive price for optional additional Annual Subscription Authorized User Access to the Solution, which includes all Solution usage rights grants, Software Documentation, Warranty, Hosting and Maintenance and Support (excluding Training), waivers, non-disclosure agreements, or other releases to Canada:

Item #	Description	Initial Period	Option Period 1	Option Period 2	Option Period 3	Option Period 4	Option Period 5	Option Period 6	Option Period 7	Option Period 8	Option Period 9
(A)	(B)	(C)	(D)	(E)	(F)	(G)	(H)	(I)	(J)	(K)	(L)
1	Annual Software as a Service Subscription Access for 0 to 150,000 Authorized Users	\$	\$	\$	\$	\$	\$	\$	\$	\$	\$
2	Annual Software as a Service Subscription Access for 150,001 to 250,000 Authorized Users	\$	\$	\$	\$	\$	\$	\$	\$	\$	\$
3	Annual Software as a Service Subscription Access for 250,001 to 350,000 Authorized Users	\$	\$	\$	\$	\$	\$	\$	\$	\$	\$
4	Annual Software as a Service Subscription Access for 350,001 and above Authorized Users	\$	\$	\$	\$	\$	\$	\$	\$	\$	\$
Total Evaluated Bid Price = Sum of each of the AVG of columns C to K = C3											

Note 1: AVG of each column is calculated by adding all of the figures under a given column/ 4

(c) Optional Professional Services

- (i) The Bidder must identify any potential Professional Services resource categories and associated per diem rates, as applicable. The following table is for the Bidder to input their per-diem rates for each resource as per article 5. Statement of Work. The Bidder may add additional categories as necessary.
- (ii) The Bidder must provide a description of each Professional Services Resource Category listed in Table 5 by completing article 1 Table 2. Task Authorized Optional Professional Services Resource Category Descriptions of Appendix A – Optional Task Authorized Professional and Training Services Resource Categories.
- (iii) For purposes of evaluation, the average of all per diem rates submitted by a Bidder will be calculated by the sum of all per diems divided by the total number of proposed professional service resources.

Table 4 - Firm all-inclusive per diem rates for Optional Professional Services to be provided on an as-and-when requested basis as described in Annex A – Statement of Work and in accordance with the Task Authorization process:

Item #	Resource Category	Initial Period	Option Period 1	Option Period 2	Option Period 3	Option Period 4	Option Period 5	Option Period 6	Option Period 7	Option Period 8	Option Period 9	Average Per Diem Rate
(A)	(B)	Firm All-Inclusive Per Diem Rate (C)	Firm All-Inclusive Per Diem Rate (D)	Firm All-Inclusive Per Diem Rate (E)	Firm All-Inclusive Per Diem Rate (F)	Firm All-Inclusive Per Diem Rate (G)	Firm All-Inclusive Per Diem Rate (H)	Firm All-Inclusive Per Diem Rate (I)	Firm All-Inclusive Per Diem Rate (J)	Firm All-Inclusive Per Diem Rate (K)	Firm All-Inclusive Per Diem Rate (L)	Sum of Columns C to L divided by 10 (M)
1		\$	\$	\$	\$	\$	\$	\$	\$	\$	\$	\$
2		\$	\$	\$	\$	\$	\$	\$	\$	\$	\$	\$

Solicitation No. - N° de l'invitation
 OX001-190594/A
 Client Ref. No. - N° de réf. du client
 OX001-190594

Amd. No. - N° de la modif.
 108 XL
 File No. - N° du dossier
 108X/OX001-190594

Buyer ID - Id de l'acheteur
 108 XL
 CCC No./N° CCC - FMS No./N° VME

3	\$	\$	\$	\$	\$	\$	\$	\$	\$	\$	\$	\$	\$	\$
4	\$	\$	\$	\$	\$	\$	\$	\$	\$	\$	\$	\$	\$	\$
Total Evaluated Bid Price = (Sum of Column M divided by total number of Resources) * 100 = C4 (Applicable Taxes Excluded):														
Note 1: Bidders to enter per diem rate for each category and period.														
Note 2: For evaluation purposes, 100 represents the estimated Level of Effort.														

(d) **Optional Training Services**

- (i) The Bidder must identify as-and-when requested Training Services per diem rates below. This following table is for the Bidder to input their per-diem rates for each resource as per article 5. Statement of Work.
- (ii) The Bidder must provide a description of the Training Services listed in Table 6 by completing article 2 Table 2. Task Authorized Optional Training Services Resource Category Descriptions of Appendix A – Optional Task Authorized Professional and Training Services Resource Categories.

Table 5 - Firm all-inclusive per diem rate for Training Services on an as-and-when requested basis, as detailed in Annex A – Statement of Work and in accordance with the Task Authorization process:

Item #	Description	Initial Period	Option Period 1	Option Period 2	Option Period 3	Option Period 4	Option Period 5	Option Period 6	Option Period 7	Option Period 8	Option Period 9
(A)	(B)	Firm All-Inclusive Per Diem Rate (C)	Firm All-Inclusive Per Diem Rate (D)	Firm All-Inclusive Per Diem Rate (E)	Firm All-Inclusive Per Diem Rate (F)	Firm All-Inclusive Per Diem Rate (G)	Firm All-Inclusive Per Diem Rate (H)	Firm All-Inclusive Per Diem Rate (I)	Firm All-Inclusive Per Diem Rate (J)	Firm All-Inclusive Per Diem Rate (K)	Firm All-Inclusive Per Diem Rate (L)
1	Training Services	\$	\$	\$	\$	\$	\$	\$	\$	\$	\$
Total Evaluated Bid Price = Sum of Columns C to L= C5											\$

3. Overall Total Evaluated Bid Price

Table	Description	Total Evaluated Bid Price per Table (C)
(A)	(B)	(C)
1	Total Evaluated Bid Price for Phase 1 – Work to Develop and Deliver Prototype Solution	C-1: \$30,000.00
2	Total Evaluated Bid Price for Phase 2 – Optional Delivery of the Solution	C-2:
3	Total Evaluated Bid Price for Phase 2 – Optional Annual Software as a Service Subscription Solution Access	C-3:
4	Total Evaluated Bid Price for Phase 2 – Optional Task Authorized Professional Services	C-4:
5	Total Evaluated Bid Price for Phase 2 – Optional Task Authorized Training Services	C-5:
Overall Total Evaluated Bid Price =SUM(C1:C5)		\$

4. Additional Financial Submission Information

The Bidder must provide the following information in the table below:

SaaS Solution's Name:	
SaaS Publisher's Name	
Cloud Service Provider's Name:	

Appendix A to Form 9 – Optional Task Authorized Professional and Training Services Resource Categories

1. Optional Task Authorized Professional Services as identified in Table 5 – Annex B – Basis of Payment

Table 1. Optional Task Authorized Professional Services Resource Category (PSRC) Descriptions	
PSRC #	RESOURCE CATEGORY DESCRIPTION
	Responsibilities could include but are not limited to:
	Responsibilities could include but are not limited to:
	Responsibilities could include but are not limited to:
	Responsibilities could include but are not limited to:

2. Optional Task Authorized Training Services as identified in Table 6 – Annex B – Basis of Payment

Table 2. Optional Task Authorized Training Services Resource Category (TSRC) Descriptions	
TSRC #	RESOURCE CATEGORY DESCRIPTION
1	Training Services Responsibilities could include but are not limited to:

ANNEX I

SECURITY CONTROL PROFILE

The table also shows the allocation of security controls to the GC and CSPs.

The following values are included in the table:

- X indicates that the control was selected or is applicable
- Not selected indicates that the control was not selected for inclusion in the profile
- Not allocated indicates that the control is selected, but not the responsibility for either the GC or the CSP to implement

Not applicable indicates that the control is not included in the standard/profile (e.g. PM control family not included in ITSG-33 Annex 3 Controls Catalog)

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture						Cross-Reference to Standards				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile ULL	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as aService (IaaS)	Platform as aService (PaaS)	Software as aService (SaaS)	Fed RAMP	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
			176													
A C-1	Access Control Policy and Procedures	(A) Personnel or roles = To be defined as part of the tailoring process (B)(a) Frequency = [at least every 3 years] (B)(b) Frequency = [at least annually]	X	X	X	X	X						X	AIS-04 AAC-03 DSI-04 GR M-06 GR M-08 GR M-09 GR M-11 IAM-02 IAM-05 IAM-07 IAM-12 IVS-12	CC3.2	A.5.1.1 A.5.1.2 A.6.1.1 A.9.1.1 A.12.1 .1 A.18.1 .1 A.18.2 .2

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture							Cross-Reference to Standards			
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile ULL	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as aService (IaaS)	Platform as aService (PaaS)	Software as aService (SaaS)	Fed RAMP	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
A C-2	Account Management	(A) Information system account types = To be defined as part of the tailoring process (E) Personnel or roles = To be defined as part of the tailoring process (F) Procedures or conditions = To be defined as part of the tailoring process (J) Frequency = [at least annually]	X	X	X	X	X						X	IAM-05 IAM-10 IAM-11 IAM-12	CC5.2 CC6.1	A.9.2.1 A.9.2.2 A.9.2.3 A.9.2.5 A.9.2.6
A C-3	Access Enforcement	Not applicable	X	X	X				X	X	X	X	X	IAM-09 IAM-12	CC5.1	A.6.2.2 A.9.1.2 A.9.4.1 A.9.4.4 A.9.4.5 A.13.1.1 A.14.1.2 A.14.1.3 A.18.1.3
A C-4	Information Flow Enforcement	(A) Information flow control policies = To be defined as part of the tailoring process	X	X	X				X	X	X		Not Selected	AIS-04 DSI-01 IVS-09	CC5.1	A.13.1.3 A.13.2.1 A.14.1.2 A.14.1.3
A C-5	Separation of Duties	(A)(a) Duties = To be defined as part of the tailoring process	X	X	X	X	X						Not Selected	IAM-05 IAM-09	CC5.1	A.6.1.2
A C-6	Least Privilege	Not applicable	X	X	X	X	X						Not Selected	IAM-05 IAM-09 IAM-13	CC5.4	A.6.1.2

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture							Cross-Reference to Standards			
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile ULL	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as aService (IaaS)	Platform as aService (PaaS)	Software as aService (SaaS)	Fed RAMP	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
A C-7	Unsuccessful Login Attempts	(A) Number = [not more than three] (A) Time period = [15 minutes] (B) Selection: locks the account/node for an [Assignment: organization-defined time period]; locks the account/node until released by an administrator; delays next logon prompt according to [Assignment: organization-defined delay algorithm] = [locks the account/node for a [Assignment: organization-defined time period]] (B) Time period (if selected) = 30 minutes (B) Delay algorithm (if selected) = Not selected	X	X	X				X	X	X	X	X	IAM-02	CC5.3	A.6.1.2
A C-8	System Use Notification	(A) Message or banner = To be defined as part of the tailoring process (C)(a) Conditions = To be defined as part of the tailoring process and approved by the GC	X	X	X				X	X	X	X	X	HRS-08	CC2.3	A.6.1.2
A C-11	Session Lock	(A) Time period = [15 minutes]	X	X	X				X	X	X	X	Not Selected	HRS-11 IAM-12	CC5.3	A.11.2.8 A.11.2.9
A C-14	Permitted Actions Without Identification or Authentication	(A) User actions = To be defined as part of the tailoring process	X	X	X	X	X						X	IAM-02	CC5.1	None

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture							Cross-Reference to Standards			
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile ULL	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as aService (IaaS)	Platform as aService (PaaS)	Software as aService (SaaS)	Fed RAMP	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
A C-17	Remote Access	Not applicable	X	X	X	X	X						X	DCS-04 HRS-05	CC5.6	A.6.2.1 A.6.2.2 A.13.1.1 A.13.2.1 A.14.1.2
A C-18	Wireless Access	Not applicable	X	X	X	X							X	EKM-03 HRS-05 IVS-12	CC5.6	A.6.2.1 A.13.1.1 A.13.2.1
A C-18 (1)	Wireless Access	Selection (one or more); users; devices = To be defined as part of the tailoring process	X	X	X			X					Not Selected	EKM-03 HRS-05 IVS-12	CC5.6	
A C-19	Access Control for Mobile Devices	Not applicable	X	X	X	X	X						X	HRS-05	CC5.6	A.6.2.1 A.11.2.6 A.13.2.1
A C-20	Use of External Information Systems	Not applicable	X	X	X	X	X						X	HRS-08	CC2.3	A.11.2.6 A.13.1.1 A.13.2.1
A C-22	Publicly Accessible Content	(D) Frequency = [at least quarterly]	X	X	X	X	X						X	DSI-03	CC5.4	None
A T-1	Security Awareness and Training Policy and Procedures	(A) Personnel or roles = To be defined as part of the tailoring process (B)(a) Frequency = [at least every 3 years] (B)(b) Frequency = [at least annually]	X	X	X	X	X						X	AAC-03 GRM-06 GRM-08 GRM-09 GRM-11 HRS-09 IAM-07	CC3.2	A.5.1.1 A.5.1.2 A.6.1.1 A.12.1.1 A.18.1.1 A.18.2.2

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture							Cross-Reference to Standards			
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile ULL	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as aService (IaaS)	Platform as aService (PaaS)	Software as aService (SaaS)	Fed RAMP	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
A T-2	Security Awareness	(A)(c) Frequency = [at least annually]	X	X	X	X	X						X	GR M-03 HRS -09 HRS -10	CC2.3	A.7.2.2.2 A.12.2.1
A T-3	Role Based Security Training	(A)(c) Frequency = [at least annually]	X	X	X	X	X						X	GR M-03 HRS -09 HRS -10	CC2.3	A.7.2.2*
A T-4	Security Training Records	(B) Time period = [at least one year]	X	X	X	X	X						X	GR M-03 HRS -09 HRS -10	CC2.3	None
A U-1	Audit and Account ability Policy and Procedures	(A) Personnel or roles = To be defined as part of the tailoring process (B)(a) Frequency = [at least every 3 years] (B)(b) Frequency = [at least annually]	X	X	X	X	X						X	AAC -03 GR M-06 GR M-08 GR M-09 GR M-11 IAM-05 IAM-07 IVS-01 IVS-03	CC3.2	A.5.1.1 A.5.1.2 A.6.1.1 A.12.1.1 A.18.1.1 A.18.2.2

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture							Cross-Reference to Standards			
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile ULL	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as aService (IaaS)	Platform as aService (PaaS)	Software as aService (SaaS)	Fed RAMP	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
AU-2	Auditable Events	(A) Auditable events = [Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes] (D) Auditable events (or subset thereof) with frequency of or situation for auditing = [organization-defined subset of the auditable events defined in AU-2 a to be audited continually for each identified event]	X	X	X	X	X						X	IAM-05 IAM-12 IVS-01	CC6.1	None
AU-2(3)	Auditable Events	Frequency = [annually or whenever there is a change in the threat environment]	X	X	X	X	X						Not Selected	IAM-12 IVS-01	CC6.1	
AU-3	Content of Audit Records	Not applicable	X	X	X				X	X	X	X	X	IVS-01	CC6.1	A.12.4.1*
AU-4	Audit Storage Capacity	(A) Storage requirements = To be defined as part of the tailoring process	X	X	X	X	X						X	IVS-01	CC6.1	A.12.1.3

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture						Cross-Reference to Standards				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile ULL	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as aService (IaaS)	Platform as aService (PaaS)	Software as aService (SaaS)	Fed RAMP	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
AU-5	Response To Audit Processing Failures	(A) Personnel or roles = To be defined as part of the tailoring process (B) Additional actions = [overwrite oldest audit records]	X	X	X				X	X	X	X	X	IVS-01	CC6.1	None
AU-6	Audit Review, Analysis, and Reporting	(A) Frequency = [at least weekly] (A) Inappropriate or unusual activity = To be defined as part of the tailoring process (B) Personnel or roles = To be defined as part of the tailoring process	X	X	X	X	X						X	IAM-05 IAM-10 IVS-01 SEF-04	CC6.1	A.12.4.1 A.16.1.2 A.16.1.4
AU-8	Time Stamps	(B) Granularity = To be defined as part of the tailoring process	X	X	X				X	X	X	X	X	IVS-03	CC6.1	A.12.4.4
AU-9	Protection of Audit Information	Not applicable	X	X	X				X	X	X	X	X	IAM-01 IVS-01 SEF-04	CC6.1	A.12.4.2 A.12.4.3 A.18.1.3
AU-11	Audit Record Retention	CSP: (A) Time period = [at least 90 days] GC: (A) Time period = [events and logs at least 3 months online and at least 6 months in storage; events and logs associated with a security incident for at least 2 years]	X	X	X	X	X						X	IAM-12 IVS-01 SEF-04	CC6.1	A.12.4.1 A.16.1.7

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture						Cross-Reference to Standards				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile ULL	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as aService (IaaS)	Platform as aService (PaaS)	Software as aService (SaaS)	Fed RAMP	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
AU-12	Audit Generation	(A) Components = [all information system and network components where audit capability is deployed/available] (B) Personnel or roles = To be defined as part of the tailoring process	X	X	X				X	X	X	X	X	IVS-01	CC6.1	A.12.4.1 A.12.4.3
CA-1	Security Assessment and Authorization Policies and Procedures	(A) Personnel or roles = To be defined as part of the tailoring process (B)(a) Frequency = [at least every 3 years] (B)(b) Frequency = [at least annually]	X	X	X	X	X						X	AIS-02 AAC-02 AAC-03 CCC-01 CCC-05 GRM-03 GRM-06 GRM-08 GRM-09 GRM-11 IAM-07	CC3.2	A.5.1.1 A.5.1.2 A.6.1.1 A.12.1.1 A.18.1.1 A.18.2.2
CA-2	Security Assessments	(B) Frequency = [at least annually] (D) Individuals or roles = To be defined as part of the tailoring process but to include [GC governance body]	X	X	X	X	X						X	AIS-02 AAC-01 AAC-02 DSI-06	CC4.1	A.14.2.8 A.18.2.2 A.18.2.3
CA-2(1)	Security Assessments	Level of independence = [an external independent organization]	X	Not allocated	X	X							X	AIS-02 AAC-01 AAC-02 DSI-06	CC4.1	

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture						Cross-Reference to Standards				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile ULL	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as aService (IaaS)	Platform as aService (PaaS)	Software as aService (SaaS)	Fed RAMP	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
C A-3	Information System Connections	(C) Frequency = [annually]	X	X	X	X	X						X	GR M-02 STA-03 STA-05 STA-09	CC7.1	A.13.1 .2 A.13.2 .1 A.13.2 .2
C A-3(3)	Information System Connections		X	X	X	X	X						Not Selected		CC7.1	
C A-5	Plan of Action and Milestones	(B) Frequency = [at least monthly]	X	X	X	X	X						X	AIS-02 GR M-03	CC4.1	None
C A-6	Security Authorization	(C) Frequency = [at least every three years or when a significant change occurs]	X	X	X	X	X						X	AIS-02 AAC-02 CCC-05 GR M-03 GR M-11	CC7.4	None

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture						Cross-Reference to Standards				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile ULL	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as aService (IaaS)	Platform as aService (PaaS)	Software as aService (SaaS)	Fed RAMP	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
C A-7	Continuous Monitoring	(A) Metrics = To be defined as part of the tailoring process but to include [GC-approved metrics] (B) Frequencies for monitoring = To be defined as part of the tailoring process but to include [GC-approved frequencies] (B) Frequencies for assessments = To be defined as part of the tailoring process but to include [GC-approved frequencies] (G) Personnel or roles = To be defined as part of the tailoring process but to include [GC governance body] (G) Frequency = To be defined as part of the tailoring process but to include [GC-approved frequencies]	X	X	X	X	X						X	AAC-01 CCC-05 GRM-03 GRM-11	CC4.1	None
C A-9	Internal System Connections	(A) Components or classes of components = To be defined as part of the tailoring process	X	X	X	X	X						X		CC7.1	None

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture						Cross-Reference to Standards				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile ULL	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as aService (IaaS)	Platform as aService (PaaS)	Software as aService (SaaS)	Fed RAMP	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
C M-1	Configuration Management Policy and Procedures	(A) Personnel or roles = To be defined as part of the tailoring process (B)(a) Frequency = [at least every 3 years] (B)(b) Frequency = [at least annually]	X	X	X	X	X						X	AAC-03 CCC-01 CCC-03 CCC-04 GRM-05 GRM-06 GRM-08 GRM-09 GRM-11 IAM-07	CC3.2	A.5.1.1 A.5.1.2 A.6.1.1 A.12.1.1 A.18.1.1 A.18.2.2
C M-2	Baseline Configuration	Not applicable	X	X	X	X	X						X	BCR-10 CCC-03 CCC-04 CCC-05 GRM-01	CC7.4	None
C M-2(1)	Baseline Configuration	(a) Frequency = [at least annually] (b) Circumstances = To be defined as part of the tailoring process but to include [when directed by the GC governance body]	X	X	X	X	X						Not Selected	BCR-10 CCC-03 CCC-04 CCC-05 GRM-01	CC7.2 CC7.3 CC7.4	

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture						Cross-Reference to Standards				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile ULL	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as aService (IaaS)	Platform as aService (PaaS)	Software as aService (SaaS)	Fed RAMP	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
C M-3	Configuration Change Control	(E) Time period = To be defined as part of the tailoring process (G) Configuration change control element = [Central communication process that include [GC governance body]] (G) Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined configuration change conditions] = To be defined as part of the tailoring process (G) Frequency (if selected) = To be defined as part of the tailoring process (G) Configuration change conditions (if selected) = To be defined as part of the tailoring process	X	X	X	X	X						Not Selected	BCR-10 CCC-04 CCC-05 TVM-02	CC7.4	A.12.1.2 A.14.2.2 A.14.2.3 A.14.2.4
C M-4	Security Impact Analysis	Not applicable	X	X	X	X	X						X	BCR-10 TVM-02	CC7.1	A.14.2.3
C M-5	Access Restrictions for Change	Not applicable	X	X	X	X	X						Not Selected	BCR-10 CCC-04 CCC-05 IAM-06	CC7.4	A.9.2.3 A.9.4.5 A.12.1.2 A.12.1.4 A.12.5.1

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture							Cross-Reference to Standards			
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile ULL	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as aService (IaaS)	Platform as aService (PaaS)	Software as aService (SaaS)	Fed RAMP	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
C M-6	Configuration Settings	(A) Checklists = [checklists from one or more of the following Center for Internet Security (CIS), National Institute of Standards and Technology (NIST), Defense Information Systems Agency (DISA)] (C) System components = [any information system component] (C) Operational requirements = To be defined as part of the tailoring process	X	X	X	X	X						X	BCR-10 CCC-05 IVS-12	CC5.1 CC7.4	None
C M-7	Least Functionality	(B) Assignment: To be defined as part of the tailoring process and that follows one or more standards from Center for Internet Security (CIS), National Institute of Standards and Technology (NIST), or Defense Information Systems Agency (DISA)	X	X	X	X	X						X	CCC-04 IAM-03 IAM-13 IVS-06	CC5.1 CC7.1	A.12.5 .1*
C M-7(1)	Least Functionality	Frequency = [at least annually]	X	X	X	X	X						Not Selected	CCC-04 IAM-03 IAM-13 IVS-06	CC7.3	
C M-8	Information System Component Inventory	(D) Information = To be defined as part of the tailoring process (E) Frequency = [at least monthly]	X	X	X	X	X						X	CCC-04 DCS-05	CC5.1	A.8.1.1 A.8.1.2

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture						Cross-Reference to Standards				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile ULL	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as aService (IaaS)	Platform as aService (PaaS)	Software as aService (SaaS)	Fed RAMP	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
CM-8(1)	Information System Component Inventory	Not applicable	X	X	X	X	X						Not Selected	CCC-04 DCS-05	CC7.4	
CM-9	Configuration Management Plan	Not applicable	X	X	X	X	X						Not Selected	BCR-10 CCC-01 CCC-04 CCC-05	CC7.4	A.6.1.1*
CM-10	Software Usage Restrictions	Not applicable	X	X	X	X	X						X		CC3.1	A.18.1.2
CM-11	User Installed Software	(A) Policies = To be defined as part of the tailoring process (B) Methods = To be defined as part of the tailoring process (C) Frequency = [continuously (via CM-7(5))]	X	X	X	X	X						X		CC5.8	A.12.5.1 A.12.6.2
CP-1	Contingency Planning Policy and Procedures	(A) Personnel or roles = To be defined as part of the tailoring process (B)(a) Frequency = [at least every 3 years] (B)(b) Frequency = [at least annually]	X	X	X	X	X						X	AAC-03 BCR-01 BCR-09 GRM-08 GRM-09 IAM-07	CC3.1 CC3.2	A.5.1.1 A.5.1.2 A.6.1.1 A.12.1.1 A.18.1.1 A.18.2.2

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture							Cross-Reference to Standards			
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile ULL	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as aService (IaaS)	Platform as aService (PaaS)	Software as aService (SaaS)	Fed RAMP	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
C P-2	Contingency Plan	(A)(f) Personnel or roles = To be defined as part of the tailoring process (B) Key contingency personnel = To be defined as part of the tailoring process (D) Frequency = [at least annually] (F) Key contingency personnel = To be defined as part of the tailoring process	X	X	X	X	X						X	BCR-01 BCR-02 BCR-09 BCR-11	CC3.1 CC3.3	A.6.1.1 A.17.1.1 A.17.2.1
C P-3	Contingency Training	(A) Time period = [10 days] (C) Frequency = [at least annually]	X	X	X	X	X						X	BCR-01 BCR-02	CC1.3	A.7.2.2*
C P-4	Contingency Plan Testing and Exercises	(A) Frequency = [at least every three years] (A) Tests = To be defined as part of the tailoring process	X	X	X	X	X						X	BCR-01 BCR-02	A1.3	A.17.1.3
C P-9	Information System Backup	(A) Frequency = [daily incremental; weekly full] (B) Frequency = [daily incremental; weekly full] (C) Frequency = [daily incremental; weekly full]	X	X	X	X							X	BCR-01 BCR-04 BCR-11	A1.2 CC5.6	A.12.3.1 A.17.1.2 A.18.1.3
C P-9(1)	Information System Backup	Frequency = [at least annually]	X	X	X	X							Not Selected	BCR-01 BCR-04 BCR-11	A1.3	

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture							Cross-Reference to Standards			
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile ULL	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as aService (IaaS)	Platform as aService (PaaS)	Software as aService (SaaS)	Fed RAMP	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
CP-10	Information System Recovery and Reconstitution	Not applicable	X	X	X	X							X	BCR-01 BCR-04	CC3.1	A.17.1.2
IA-1	Identification and Authentication Policy and Procedures	(A) Personnel or roles = To be defined as part of the tailoring process (B)(a) Frequency = [at least every 3 years] (B)(b) Frequency = [at least annually]	X	X	X	X	X						X	AAC-03 GRM-06 GRM-08 GRM-09 IAM-02 IAM-07 IAM-12	CC3.2	A.5.1.1 A.5.1.2 A.6.1.1 A.12.1.1 A.18.1.1 A.18.2.2
IA-2	Identification and Authentication (Organizational Users)	Not applicable	X	X	X				X	X	X	X	X	IAM-09 IAM-12	CC5.3	A.9.2.1
IA-2(1)	Identification and Authentication (Organizational Users)	Not applicable	X	X	X				X	X	X	X	X	IAM-09 IAM-12	CC5.3	
IA-2(8)	Identification and Authentication (Organizational Users)	Not applicable	X	X	X				X	X	X	X	Not Selected	IAM-09 IAM-12	CC5.3	
IA-2(9)	Identification and Authentication (Organizational Users)	Not applicable	X	X	X				X	X	X	X	Not Selected		CC5.3	

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture							Cross-Reference to Standards			
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile ULL	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as aService (IaaS)	Platform as aService (PaaS)	Software as aService (SaaS)	Fed RAMP	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
IA-4	Identifier Management	(A) Personnel or roles = To be defined as part of the tailoring process (D) Time period = [at least two years] (E) Time period = [90 days for user identifiers]	X	X	X	X	X						X	DCS-03 IAM-07 IAM-09	CC5.1 CC5.2	A.9.2.1
IA-5	Authenticator Management	(G) Time period = [at least every 180 days]	X	X	X	X	X						X	GRM-09 IAM-07 IAM-09 IAM-12	CC5.1 CC5.2 CC5.3	A.9.2.1 A.9.2.4 A.9.3.1 A.9.4.3
IA-5(1)	Authenticator Management	(a) Password requirements = [case sensitive, minimum of eight characters, and at least one each of upper-case letters, lower-case letters, numbers, and special characters] (b) Number of change characters = [at least one] (d) Lifetime restrictions = [one day minimum, sixty day maximum] (e) Password reuse = [24 generations]	X	X	X				X	X	X	X	X	GRM-09 IAM-07 IAM-09 IAM-12	CC5.1 CC5.3	
IA-5(2)	Authenticator Management	Not applicable	X	X	X				X	X	X	X	Not Selected	GRM-09 IAM-07 IAM-07 IAM-09 IAM-12	CC5.1 CC5.3	

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture							Cross-Reference to Standards			
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile ULL	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as aService (IaaS)	Platform as aService (PaaS)	Software as aService (SaaS)	Fed RAMP	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
IA-5(3)	Authenticator Management	Types of and/or specific authenticators = [a hardware/biometric multi-factor authenticator] Selection: in person; by a trusted third party = [in person] Registration authority = To be defined as part of the tailoring process Personnel or roles = To be defined as part of the tailoring process	X	X	X	X	X						Not Selected	GRM-09 IAM-07 IAM-09 IAM-12	CC5.2	
IA-5(6)	Authenticator Management		X	X	X	X	X						Not Selected	GRM-09 IAM-07 IAM-09 IAM-12	CC5.1	
IA-5(7)	Authenticator Management	Not applicable	X	X	X	X	X						Not Selected	GRM-09 IAM-07 IAM-09 IAM-12	CC5.1 CC7.1	
IA-5(11)	Authenticator Management	Token quality requirements = [As per CSE User Authentication Guidance for IT Systems (ITSP.30.031 V2), or subsequent versions]	X	X	X				X	X	X	X	X		CC5.3	
IA-6	Authenticator Feedback	Not applicable	X	X	X				X	X	X	X	X	IAM-12	CC5.3	A.9.4.2
IA-7	Cryptographic Module Authentication	Not applicable	X	X	X				X	X	X		X	AAC-03 EKM-03	CC5.1	A.18.1.5

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture							Cross-Reference to Standards			
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile ULL	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as aService (IaaS)	Platform as aService (PaaS)	Software as aService (SaaS)	Fed RAMP	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
IA-8	Identification and Authentication (Non-Organizational Users)	Not applicable	X	X	X				X	X	X	X	X	IAM-07 IAM-09 IAM-12	CC5.3	A.9.2.1
IR-1	Incident Response Policy and Procedures	(A) Personnel or roles = To be defined as part of the tailoring process (B)(a) Frequency = [at least every 3 years] (B)(b) Frequency = [at least annually]	X	X	X	X	X						X	AAC-03 GRM-06 GRM-08 GRM-09 IAM-07 SEF-02	CC3.2	A.5.1.1 A.5.1.2 A.6.1.1 A.12.1.1 A.18.1.1 A.18.2.2
IR-2	Incident Response Training	(A) Time period = To be defined as part of the tailoring process (C) Frequency = [at least annually]	X	X	X	X	X						X	SEF-02 SEF-03	CC1.3	A.7.2.2*
IR-4	Incident Handling	Not applicable	X	X	X	X	X						X	SEF-02 SEF-05	CC6.2	A.16.1.4 A.16.1.5 A.16.1.6
IR-5	Incident Monitoring	Not applicable	X	X	X	X	X						X	SEF-02 SEF-04 SEF-05	CC6.2	None
IR-6	Incident Reporting	(A) Time period = [the time periods specified in the GC Cyber Security Event Management Plan (GC CSEMP)] (B) Authorities = [organizations specified in the GC Cyber Security Event Management Plan (GC CSEMP)]	X	X	X	X	X						X	SEF-01 SEF-03	CC6.1	A.6.1.3 A.16.1.2

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture							Cross-Reference to Standards			
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile ULL	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as aService (IaaS)	Platform as aService (PaaS)	Software as aService (SaaS)	Fed RAMP	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
IR-7	Incident Response Assistance	Not applicable	X	X	X	X	X						X	SEF-02 SEF-03 SEF-04	CC6.1	None
IR-8	Incident Response Plan	(A)(h) Personnel or roles = To be defined as part of the tailoring process (B) Assignment = To be defined as part of the tailoring process (C) Frequency = [at least annually] (E) Assignment = To be defined as part of the tailoring process	X	X	X	X	X						X	SEF-02 SEF-04 SEF-05	CC6.2	A.16.1.1
IR-9	Information Spillage Response		X	X	X	X	X						Not Selected		CC6.2	None
MA-1	System Maintenance Policy and Procedures	(A) Personnel or roles = To be defined as part of the tailoring process (B)(a) Frequency = [at least every 3 years] (B)(b) Frequency = [at least annually]	X	X	X	X	X						X	AAC-03 DCS-04 DCS-08 GR-M-06 GR-M-08 GR-M-09 IAM-07	CC3.2	A.5.1.1 A.5.1.2 A.6.1.1 A.12.1.1 A.18.1.1 A.18.2.2
MA-2	Controlled Maintenance	(C) Personnel or roles = To be defined as part of the tailoring process (F) Maintenance-related information = To be defined as part of the tailoring process	X	X	X	X	X						X	BCR-07 DCS-08	CC5.6 CC7.1	A.11.2.4* A.11.2.5*

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture							Cross-Reference to Standards			
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile ULL	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as aService (IaaS)	Platform as aService (PaaS)	Software as aService (SaaS)	Fed RAMP	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
MA-4	Non-Local Maintenance	Not applicable	X	X	X	X	X						X	BCR-07 BCR-10 IAM-03	CC5.1 CC5.3 CC6.1	None
MA-5	Maintenance Personnel	Not applicable	X	X	X	X	X						X	BCR-07 IAM-03 IAM-09	CC1.4 CC5.6	None
MA-6	Timely Maintenance	(A) System components = To be defined as part of the tailoring process (A) Time period = To be defined as part of the tailoring process	X	X	X	X	X						Not Selected	BCR-07	A1.2	A.11.2.4
MP-1	Media Protection Policy and Procedures	(A) Personnel or roles = To be defined as part of the tailoring process (B)(a) Frequency = [at least every 3 years] (B)(b) Frequency = [at least annually]	X	X	X	X							X	AAC-03 DSI-04 GRM-06 GRM-08 GRM-09 HRS-11 IAM-07	CC3.2	A.5.1.1 A.5.1.2 A.6.1.1 A.12.1.1 A.18.1.1 A.18.2.2
MP-2	Media Access	(A) Types of media = [IT media (digital and non-digital)] (A) Personnel or roles = [authorized administrators]	X	X	X	X							X	HRS-05 HRS-11	CC5.5	A.8.2.3 A.8.3.1 A.11.2.9
MP-3	Media Marking	(B) Types of system media = [no removable media types] (B) Controlled areas = [controlled areas that meet the requirements of the GC Industrial Security Program]	X	X	X	X							Not Selected	DSI-04 HRS-11	CC5.7	A.8.2.2

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture							Cross-Reference to Standards			
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile ULL	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as aService (IaaS)	Platform as aService (PaaS)	Software as aService (SaaS)	Fed RAMP	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
MP-4	Media Storage	(A) Types of media = [all types of digital and non-digital media with sensitive information] (A) Controlled areas = [controlled areas that meet the requirements of the GC Industrial Security Program]	X	X	X	X							Not Selected	HRS-05 HRS-11	CC5.5	A.8.2.3 A.8.3.1 A.11.2.9
MP-5	Media Transport	(A) Types of media = [all media with sensitive information] (A) Security safeguards = To be defined as part of the tailoring process	X	X	X	X							Not Selected	SEF-04 STA-05	CC5.7	A.8.2.3 A.8.3.1 A.8.3.3 A.11.2.5 A.11.2.6
MP-6	Media Sanitization	(A) System media = To be defined as part of the tailoring process (A) Sanitization = To be defined as part of the tailoring process	X	X	X	X							X	DSI-07 HRS-05	CC5.5	A.8.2.3 A.8.3.1 A.8.3.2 A.11.2.7
MP-7	Media Use	(A) Selection: restricts; prohibits = [prohibits] (A) Types of system media = [unauthorized removable media] (A) Information systems or components = [all components] (A) Security safeguards = [technical safeguards]	X	Not allocated	X	X							X		CC5.6	A.8.2.3 A.8.3.1

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture						Cross-Reference to Standards				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile ULL	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as aService (IaaS)	Platform as aService (PaaS)	Software as aService (SaaS)	Fed RAMP	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
PE-1	Physical and Environmental Protection Policy and Procedures	(A) Personnel or roles = To be defined as part of the tailoring process (B)(a) Frequency = [at least every 3 years] (B)(b) Frequency = [at least annually]	X	X	X	X							X	AAC-03 BCR-03 BCR-05 BCR-06 BCR-08 DSI-07 DCS-04 GRM-06 GRM-08 GRM-09 IAM-07	CC3.2	A.5.1.1 A.5.1.2 A.6.1.1 A.12.1.1 A.18.1.1 A.18.2.2
PE-2	Physical Access Authorizations	(C) frequency [annually]	X	X	X	X							X	DCS-02 DCS-06 DCS-09 IVS-01	CC5.5	A.11.1.2*

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture							Cross-Reference to Standards			
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile ULL	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as aService (IaaS)	Platform as aService (PaaS)	Software as aService (SaaS)	Fed RAMP	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
PE-3	Physical Access Control	<p>(A) Entry/exit points = To be defined as part of the tailoring process</p> <p>(A)(b) Selection (one or more): [Assignment: organization-defined physical access control systems/devices]; guards] = [controlled areas that meet the requirements of the GC Industrial Security Program]</p> <p>(A)(b) Physical access control systems/devices (if selected) = To be defined as part of the tailoring process</p> <p>(B) Entry/exit points = To be defined as part of the tailoring process</p> <p>(C) Security safeguards = To be defined as part of the tailoring process</p> <p>(D) Circumstances for escorts and monitoring = To be defined as part of the tailoring process</p> <p>(F) Physical access devices = To be defined as part of the tailoring process</p> <p>(F) Frequency = [annually]</p> <p>(G) Frequency = [only when keys are lost, combinations are compromised or individuals are transferred or terminated]</p>	X	X	X			X					X	DCS-02 DCS-06 DCS-09 IVS-01	CC5.5	A.11.1.1 A.11.1.2 A.11.1.3

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture							Cross-Reference to Standards			
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile ULL	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as aService (IaaS)	Platform as aService (PaaS)	Software as aService (SaaS)	Fed RAMP	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
PE-4	Access Control for Transmission Medium	(A) Lines = To be defined as part of the tailoring process (A) Security safeguards = To be defined as part of the tailoring process	X	X	X			X					Not Selected	BCR-03 DCS-06 IVS-12	CC5.5	A.11.1.2 A.11.2.3
PE-5	Access Control for Output Devices	Not applicable	X	X	X			X					Not Selected	BCR-06 DCS-06	CC5.5	A.11.1.2 A.11.1.3
PE-6	Monitoring Physical Access	(B) Frequency = [at least monthly] (B) Events = To be defined as part of the tailoring process	X	X	X			X					X	DCS-02 DCS-06 DCS-09	CC5.5	None
PE-8	Access Records	(A) Time period = [a minimum of 1 year] (B) Frequency = [at least monthly]	X	X	X			X					X	DCS-02	CC5.5	None
PE-9	Power Equipment and Power Cabling	Not applicable	X	X	X			X					Not Selected	BCR-08	A1.2	A.11.1.4 A.11.2.1 A.11.2.2 A.11.2.3
PE-10	Emergency Shutoff	(B) Location by system or components = To be defined as part of the tailoring process	X	X	X			X					Not Selected	BCR-08	A1.2	A.11.2.2*
PE-11	Emergency Power	(A) Selection (one or more): an orderly shutdown of the information system; transition of the information system to long-term alternate power = To be defined as part of the tailoring process	X	X	X			X					Not Selected	BCR-08	A1.2	A.11.2.2*
PE-12	Emergency Lighting	Not applicable	X	X	X			X					X	BCR-08	A1.2	A.11.2.2*

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture							Cross-Reference to Standards			
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile ULL	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as aService (IaaS)	Platform as aService (PaaS)	Software as aService (SaaS)	Fed RAMP	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
PE-13	Fire Protection	Not applicable	X	X	X			X					X	BCR-03 BCR-05 BCR-08	A1.2	A.11.1.4 A.11.2.1
PE-14	Temperature and Humidity Controls	(A) Acceptable levels = To be defined as part of the tailoring process (B) Frequency = [continuously]	X	X	X	X							X	BCR-05 BCR-06 BCR-08	A1.2	A.11.1.4 A.11.2.1 A.11.2.2
PE-15	Water Damage Protection	Not applicable	X	X	X			X					X	BCR-05 BCR-06	A1.2	A.11.1.4 A.11.2.1 A.11.2.2
PE-16	Delivery and Removal	(A) Types of system components = [all information system components]	X	X	X			X					X	DSI-04 DCS-04 DCS-07 DCS-08	CC5.5	A.8.2.3 A.11.1.6 A.11.2.5
PE-18	Location of Information System Components	(A) Physical and environmental hazards = To be defined as part of the tailoring process following any related provisions of the GC Industrial Security Program	X	X	X			X					Not Selected	BCR-05 BCR-06 DCS-02 DCS-07 DCS-09		A.8.2.3 A.11.1.4 A.11.2.1
PL-1	Security Planning Policy and Procedures	(A) Personnel or roles = To be defined as part of the tailoring process (B)(a) Frequency = [at least every 3 years] (B)(b) Frequency = [at least annually]	X	X	X	X	X						X	AAC-03 CCC-01 GR-M-06 GR-M-08 GR-M-09 GR-M-11 IAM-07	CC3.1 CC3.2	A.5.1.1 A.5.1.2 A.6.1.1 A.12.1.1 A.18.1.1 A.18.2.2

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture							Cross-Reference to Standards			
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile ULL	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as aService (IaaS)	Platform as aService (PaaS)	Software as aService (SaaS)	Fed RAMP	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
PL-2	System Security Plan	(B) Personnel or roles = To be defined as part of the tailoring process (C) Frequency = [at least annually]	X	X	X	X	X						X	CCC-01 CCC-05	CC3.1 CC3.3	A.14.1.1
PL-4	Rules of Behavior	(C) Frequency = [at least every 3 years]	X	X	X	X	X						X	GRM-07 HRS-06 HRS-07 HRS-08 HRS-10	CC2.3	A.7.1.2 A.7.2.1 A.8.1.3
PL-7	Security Concepts of Operation	(B) Frequency = [at least annually]	X	X	Not allocated		X						Not Selected			A.14.1.1*
PL-8	Information Security Architecture	(B) Frequency = [at least annually]	X	X	X	X	X						Not Selected		CC3.2	A.14.1.1*
PS-1	Personnel Security Policy and Procedures	(A) Personnel or roles = To be defined as part of the tailoring process (B)(a) Frequency = [at least every 3 years] (B)(b) Frequency = [at least annually]	X	X	X	X	X						X	AAC-03 GRM-06 GRM-07 GRM-08 GRM-09 HRS-03 HRS-07 IAM-07	CC3.2	A.5.1.1 A.5.1.2 A.6.1.1 A.12.1.1 A.18.1.1 A.18.2.2
PS-2	Position Categorization	(C) Frequency = [at least every three years]	X	X	X	X	X						X	DSI-06 HRS-02 HRS-03 HRS-04 HRS-07	CC1.4	None

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture							Cross-Reference to Standards			
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile ULL	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as aService (IaaS)	Platform as aService (PaaS)	Software as aService (SaaS)	Fed RAMP	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
PS-3	Personnel Screening	(B) Conditions requiring rescreening and, where rescreening is so indicated, the frequency of such rescreening = [the TBS Standard on Security Screening and any related provisions of the Industrial Security Program]	X	X	X	X	X						X	HRS-02	CC1.4	A.7.1.1
PS-4	Personnel Termination	(A) Time period = [same day] (C) Information security topics = To be defined as part of the tailoring process in accordance with the TBS Standard on Security Screening and any related provisions of the Industrial Security Program (F) Personnel or roles = To be defined as part of the tailoring process (F) Time period = To be defined as part of the tailoring process	X	X	X	X	X						X	HRS-01 HRS-04 IAM-11	A1.2 CC5.2 CC5.4 CC5.6	A.7.3.1 A.8.1.4

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture							Cross-Reference to Standards			
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile ULL	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as aService (IaaS)	Platform as aService (PaaS)	Software as aService (SaaS)	Fed RAMP	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
PS-5	Personnel Transfer	(B) Transfer or reassignment actions = To be defined as part of the tailoring process following the TBS Standard on Security Screening and any related provisions of the Industrial Security Program (B) Time period = [within 5 days of the formal transfer action] (D) Personnel or roles = To be defined as part of the tailoring process (D) Time period = To be defined as part of the tailoring process	X	X	X	X	X						X	HRS-04 IAM-11	CC5.4 CC5.5	A.7.3.1 A.8.1.4
PS-6	Access Agreements	(B) Frequency = [at least annually] (C)(b) Frequency = [at least annually]	X	X	X	X	X						X	HRS-03 HRS-04 HRS-06 HRS-07 IAM-09 IAM-10	CC1.4	A.7.1.2 A.7.2.1 A.13.2.4
PS-7	Third-Party Personnel Security	(D) Personnel or roles = To be defined as part of the tailoring process (D) Time period = [the same day]	X	X	X	X	X						X	HRS-03 HRS-07 IAM-10 STA-05	CC1.2 CC1.4 CC4.1 CC5.5	A.6.1.1* A.7.2.1*
PS-8	Personnel Sanctions	(B) Personnel or roles = To be defined as part of the tailoring process (B) Time period = To be defined as part of the tailoring process	X	X	X	X	X						X	GRM-07 HRS-04	CC1.1	A.7.2.3

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture							Cross-Reference to Standards			
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile ULL	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as aService (IaaS)	Platform as aService (PaaS)	Software as aService (SaaS)	Fed RAMP	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
RA-1	Risk Assessment Policy and Procedures	(A) Personnel or roles = To be defined as part of the tailoring process (B)(a) Frequency = [at least every 3 years] (B)(b) Frequency = [at least annually]	X	X	X	X	X						X	AAC-03 GR-M-08 GR-M-09 GR-M-10 GR-M-11 IAM-07	CC3.1	A.5.1.1 A.5.1.2 A.6.1.1 A.12.1.1 A.18.1.1 A.18.2.2
RA-2	Security Categorization	Not applicable	X	X	X	X	X						X	AAC-03 DSI-01 DSI-06 DCS-01 GR-M-02 GR-M-10 GR-M-11	CC3.1	A.8.2.1
RA-3	Risk Assessment	(B) Selection: security plan; risk assessment report; [Assignment: organization-defined document] = To be defined as part of the tailoring process (B) Document (if selected) = [security assessment report] (C) Frequency = [at least every 3 years or when a significant change occurs] (D) Personnel or roles = To be defined as part of the tailoring process (E) Frequency = [at least every 3 years or when a significant change occurs]	X	X	X	X	X						X	BCR-09 GR-M-02 GR-M-08 GR-M-10 GR-M-11	CC3.1	A.12.6.1*

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture							Cross-Reference to Standards			
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile ULL	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as aService (IaaS)	Platform as aService (PaaS)	Software as aService (SaaS)	Fed RAMP	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
RA-5	Vulnerability Scanning	(A) Frequency = [monthly for operating systems/infrastructure, web applications, and database management systems] (D) Response times = [within 30 days for high-risk vulnerabilities and 90 days for moderate-risk vulnerabilities from the date of discovery] (E) Personnel or roles = To be defined as part of the tailoring process	X	X	X	X	X						X	AAC-02 TVM-02	CC4.1	A.12.6.1*
RA-5(1)	Vulnerability Scanning		X	X	X	X	X						Not Selected	AAC-02 TVM-02	CC4.1	
SA-1	System and Services Acquisition Policy and Procedures	(A) Personnel or roles = To be defined as part of the tailoring process (B)(a) Frequency = [at least every 3 years] (B)(b) Frequency = [at least annually]	X	X	X	X	X						X	AAC-03 CCC-01 GRM-06 GRM-09 IAM-07	CC3.2	A.5.1.1 A.5.1.2 A.6.1.1 A.12.1.1 A.18.1.1 A.18.2.2
SA-2	Allocation of Resources	Not applicable	X	X	X	X	X						X	DSI-06 GRM-01	CC1.3 CC3.3	None
SA-3	System Development Lifecycle	(A) SDLC = To be defined as part of the tailoring process	X	X	X	X	X						X	BCR-10 CCC-01 CCC-03	CC7.1 CC7.4	A.6.1.1 A.6.1.5 A.14.1.1 A.14.2.1 A.14.2.6

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture							Cross-Reference to Standards			
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile ULL	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as aService (IaaS)	Platform as aService (PaaS)	Software as aService (SaaS)	Fed RAMP	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
SA-4	Acquisition Process	Not applicable	X	X	X	X	X						X	BCR-10 CCC-01 CCC-02 CCC-03 GRM-01 IVS-04	CC7.1	A.14.1.1 A.14.2.7 A.14.2.9 A.15.1.2
SA-5	Information System Documentation	(C) Actions = To be defined as part of the tailoring process (E) Personnel or roles = To be defined as part of the tailoring process	X	X	X	X	X						X	BCR-04 BCR-10 CCC-02 CCC-03	CC1.3 CC5.1 CC7.1	A.12.1.1*
SA-8	Security Engineering Principles	Not applicable	X	X	X	X	X						Not Selected	AIS-01 BCR-10 CCC-02 CCC-03	CC7.1	A.14.2.5
SA-9	External Information System Services	(A) Security controls = [applicable security controls if GC data is processes or stored within the external system] (C) Processes, methods, and techniques = [processes, methods, and techniques specified if GC data is processes or stored within the external system]	X	X	X	X	X						X	CCC-02 HRS-06 STA-03 STA-05 STA-09	CC4.1	A.6.1.1 A.6.1.5 A.7.2.1 A.13.1.2 A.13.2.2 A.15.2.1 A.15.2.2

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture							Cross-Reference to Standards			
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile ULL	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as aService (IaaS)	Platform as aService (PaaS)	Software as aService (SaaS)	Fed RAMP	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
SA-10	Developer Configuration Management	(A) [Selection (one or more): design; development; implementation; operation = [development, implementation, and operation] (B) Configuration items under CM = To be defined as part of the tailoring process (E) Personnel = To be defined as part of the tailoring process	X	X	X	X	X						Not Selected	BCR-04 BCR-10 CCC-02 CCC-03	CC7.1 CC7.4	A.12.1.2 A.14.2.2 A.14.2.4 A.14.2.7
SA-11	Developer Security Testing	(B) Selection (one or more): unit; integration; system; regression = To be defined as part of the tailoring process (B) Depth and coverage = To be defined as part of the tailoring process	X	X	X	X	X						Not Selected	BCR-04 BCR-10 CCC-02 CCC-03 DSI-05	CC7.1	A.14.2.7 A.14.2.8
SA-15	Development Process, Standards, and Tool		X	X	X	X	X						Not Selected			A.6.1.5 A.14.2.1
SC-1	System and Communications Protection Policy and Procedures	(A) Personnel or roles = To be defined as part of the tailoring process (B)(a) Frequency = [at least every 3 years] (B)(b) Frequency = [at least annually]	X	X	X	X	X						X	AIS-04 AAC-03 GRM-06 GRM-08 GRM-09 IAM-07	CC3.2	A.5.1.1 A.5.1.2 A.6.1.1 A.12.1.1 A.18.1.1 A.18.2.2
SC-2	Application Partitioning	Not applicable	X	X	X				X	X	X	X	Not Selected	AIS-01 IVS-08 IVS-09	CC5.1	None

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture							Cross-Reference to Standards			
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile ULL	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as aService (IaaS)	Platform as aService (PaaS)	Software as aService (SaaS)	Fed RAMP	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
S C-5	Denial of Service Protection	(A) Types of denial of service attacks = To be defined as part of the tailoring process (A) Security safeguards = To be defined as part of the tailoring process	X	X	X				X	X	X		X	AIS-01 TVM-01	CC5.1	None
S C-7	Boundary Protection	(B) Selection: physically; logically = To be defined as part of the tailoring process	X	X	X				X	X			X	AIS-01 EKM-03 IVS-06 IVS-09 IVS-12 STA-09	CC5.1 CC5.6	A.13.1.1 A.13.1.3 A.13.2.1 A.14.1.3
S C-7(5)	Boundary Protection		X	X	X				X	X			Not Selected	AIS-01 IVS-06 IVS-09 IVS-12 STA-09	CC5.6	
S C-7(12)	Boundary Protection	Host-based boundary protection mechanisms = To be defined as part of the tailoring process Information system components = To be defined as part of the tailoring process	X	X	X	X	X						Not Selected	AIS-01 IVS-06 IVS-09 IVS-12 STA-09	CC5.6	
S C-8	Transmission Confidentiality and Integrity	(A) Selection (one or more): confidentiality; integrity = [confidentiality and integrity]	X	X	X				X	X	X	X	Not Selected	AIS-01 AIS-04 DSI-03 DSI-04 (mapped to SC-9) EKM-03	CC5.7	A.8.2.3 A.13.1.1 A.13.2.1 A.13.2.3 A.14.1.2 A.14.1.3

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture						Cross-Reference to Standards				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile ULL	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as aService (IaaS)	Platform as aService (PaaS)	Software as aService (SaaS)	Fed RAMP	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
S C-10	Network Disconnect	(A) Time period = [no longer than 30 minutes for RAS-based sessions or no longer than 60 minutes for non-interactive user sessions]	X	X	X				X	X	X	X	Not Selected	AIS-01 IAM-12	CC5.1 CC5.6	A.13.1.1
S C-12	Cryptographic Key Establishment and Management	(A) Requirements for key generation, distribution, storage, access, and destruction = [CSE-approved cryptography]	X	X	X	X	X						X	AIS-01 EKM-02	CC5.1	A.10.1.2
S C-13	Cryptographic Protection	(A) Cryptographic uses and type of cryptography required for each use = [CSE-compliant cryptography as per CSE's Cryptographic Algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B Information (ITSP.40.111), or subsequent versions]	X	X	X				X	X	X	X	X	AIS-01 AAC-03 EKM-02 EKM-03	CC5.1	A.10.1.1 A.14.1.2 A.14.1.3 A.18.1.5
S C-15	Collaborative Computing Devices	(A) Exceptions = [no exceptions]	X	X	X								X		CC5.1	A.13.2.1*
S C-17	Public Key Infrastructure Certificates	(A) Certificate policy = To be defined as part of the tailoring process	X	X	X	X	X						Not Selected	AIS-01 EKM-02	CC5.1	A.10.1.2
S C-20	Secure Name / Address Resolution Service (Authoritative Source)	Not applicable	X	Not allocated	X				X				X		CC5.1 CC5.6	None

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture							Cross-Reference to Standards			
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile ULL	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as aService (IaaS)	Platform as aService (PaaS)	Software as aService (SaaS)	Fed RAMP	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
S C-21	Secure Name / Address Resolution Service (Recursive or Caching Resolver)	Not applicable	X	Not allocated	X				X	X	X	X	X	IVS-06	CC5.1	None
S C-22	Architecture and Provisioning for Name / Address Resolution Service	Not applicable	X	X	X				X				X	IVS-06	A1.1	None
S C-23	Session Authenticity	Not applicable	X	X	X				X	X	X	X	Not Selected	EKM-03	CC5.1 CC5.3	None
S C-23 (1)	Session Authenticity		X	X	X				X	X	X	X	Not Selected		CC5.3	
S C-23 (3)	Session Authenticity	Randomness requirements = To be defined as part of the tailoring process	X	X	X				X	X	X	X	Not Selected		CC5.3	
S C-39	Process Isolation	Not applicable	X	Not allocated	X				X	X	X		X		CC5.1	None
SI-1	System and Information Integrity Policy and Procedures	(A) Personnel or roles = To be defined as part of the tailoring process (B)(a) Frequency = [at least every 3 years] (B)(b) Frequency = [at least annually]	X	X	X	X	X						X	AAC-03 CCC-04 DSI-04 GRM-06 GRM-08 GRM-09 IAM-07 TVM-02	CC3.2	A.5.1.1 A.5.1.2 A.6.1.1 A.12.1.1 A.18.1.1 A.18.2.2

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture							Cross-Reference to Standards			
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile ULL	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as aService (IaaS)	Platform as aService (PaaS)	Software as aService (SaaS)	Fed RAMP	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
SI-2	Flaw Remediation	(C) Time period = [30 days of release of updates]	X	X	X	X	X						X	AIS-03 CCC-05 TVM-02	CC6.1 CC6.2 CC7.3	A.12.6.1 A.14.2.2 A.14.2.3 A.16.1.3
SI-3	Malicious Code Protection	(C)(a) Frequency = [at least weekly] (C)(a) Selection (one or more); endpoint; network entry/exit points = [For CSPs - to include endpoints, For GC - to include endpoints and network entry/exit points] (C)(b) Selection (one or more); block malicious code; quarantine malicious code; send alert to administrator; [Assignment: organization-defined action] = [quarantine malicious code] (C)(b) Action (if selected) = To be defined as part of the tailoring process but to include [alerting administrator or defined security personnel]	X	X	X				X	X	X		X	AIS-03 CCC-04 TVM-01	CC5.8	A.12.2.1
SI-3(1)	Malicious Code Protection	Not applicable	X	X	X	X	X						Not Selected	AIS-03 CCC-04 TVM-01	CC5.8	
SI-3(2)	Malicious Code Protection	Not applicable	X	X	X				X	X	X		Not Selected	AIS-03 CCC-04 TVM-01	CC5.8	

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture							Cross-Reference to Standards			
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile ULL	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as aService (IaaS)	Platform as aService (PaaS)	Software as aService (SaaS)	Fed RAMP	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
SI-4	Information System Monitoring	(A)(a) Monitoring objectives = [monitoring objectives consistent with the GC CSEMP] (B) Techniques and methods = To be defined as part of the tailoring process (G) Information system monitoring information = To be defined as part of the tailoring process (G) Personnel or roles = To be defined as part of the tailoring process (G) Selection (one or more): as needed; [Assignment: organization-defined frequency] = To be defined as part of the tailoring process (G) Frequency (is selected) = To be defined as part of the tailoring process	X	X	X	X	X						X	AIS-03 CCC-04 GRM-11 IAM-05 IVS-01 SEF-03 TVM-02	CC3.2 CC6.1	None
SI-5	Security Alerts, Advisories, and Directives	(A) External organizations = [to include GC Computer Incident Response Team (GC CIRT)] (C) Selection (one or more): [Assignment: organization-defined personnel or roles]; [Assignment: organization-defined elements within the organization]; [Assignment: organization-defined external organizations] = To be defined as part of the tailoring process but to include [to	X	X	X	X	X						X	SEF-01 SEF-03 TVM-01 TVM-02	CC6.1 CC7.3	A.6.1.4*

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture						Cross-Reference to Standards				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile ULL	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as aService (IaaS)	Platform as aService (PaaS)	Software as aService (SaaS)	Fed RAMP	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
		include system security personnel and administrators with configuration/patch-management responsibilities] (C) Personnel or roles (if selected) = To be defined as part of the tailoring process but to include [system security personnel and administrators with configuration/patch-management responsibilities] (C) Elements within the organization (if selected) = To be defined as part of the tailoring process (C) External organizations (if selected) = To be defined as part of the tailoring process														
SI-8	Spam Protection	Not applicable	X	X	X	X	X						Not Selected	EKM-03 TVM-01	CC5.8	None
SI-10	Information Input Validation	(A) Information inputs = To be defined as part of the tailoring process	X	X	X				X	X	X	X	Not Selected	AIS-03	PI1.2	None
SI-12	Information Output Handling and Retention	Not applicable	X	X	X	X	X						X	DSI-04 GRM-02	PI1.4	None
SI-16	Memory Protection	(A) Security safeguards = To be defined as part of the tailoring process	X	X	X				X				X		CC5.1	None

			Responsibility for Control Implementation			Suggested Allocation of Control to Cloud Computing Reference Architecture						Cross-Reference to Standards				
ID	Security Control Name	Recommended Assignment Values	GC Cloud Profile ULL	GC	CSPs	Cloud Provider Organization	Cloud Consumer Organization	Facility & Hardware	Resource Abstraction and Control Layer	Infrastructure as aService (IaaS)	Platform as aService (PaaS)	Software as aService (SaaS)	Fed RAMP	CSA CCM v3.0.1	AICPA Trust Services Criteria SOC	ISO/IEC 27001:2013 (* means not fully satisfied)
P M-1	Information Security Program Plan	4.b. Frequency = [at least annually]	X	Not allocated	X	X							Not Selected			A.5.1.1 A.5.1.2 A.6.1.1 A.18.1.1 A.18.2.2
P M-2	Senior Information Security Officer	Not applicable	X	Not allocated	X	X							Not Selected			A.6.1.1*
P M-10	Security Authorization Process	Not applicable	X	Not allocated	X	X							Not Selected			A.6.1.1*
P M-13	Information Security Workforce	Not applicable	X	Not allocated	X	X							Not Selected			A.7.2.2*
P M-15	Contacts With Security Groups and Associations	Not applicable	X	Not allocated	X	X							Not Selected			A.6.1.4