Public Works and Government Services Canada | Travaux publics et Services gouvernementaux Canada

RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:

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

LETTER OF INTEREST
LETTRE D'INTÉRÊT

Comments - Commentaires

Issuing Office - Bureau de distribution

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

Title - Sujet RFI - SaaS Method of Supply	
Solicitation No. - N° de l'invitation EN578-191593/C	**Date** 2018-10-29
Client Reference No. - N° de référence du client 20191593	**GETS Ref. No. - N° de réf. de SEAG** PW-$EEM-039-34003
File No. - N° de dossier 039eem.EN578-191593	**CCC No./N° CCC - FMS No./N° VME**
Solicitation Closes - L'invitation prend fin **at - à 02:00 PM** **on - le 2018-11-19**	**Time Zone** **Fuseau horaire** Eastern Standard Time EST
F.O.B. - F.A.B. **Plant-Usine:** ☐ **Destination:** ☐ **Other-Autre:** ☐	
Address Enquiries to: - Adresser toutes questions à: Vincent Wong	**Buyer Id - Id de l'acheteur** 039eem
Telephone No. - N° de téléphone (819) 639-5603 ( )	**FAX No. - N° de FAX** (819) 953-3703

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

DEPARTMENT OF PUBLIC WORKS AND GOVERNMENT SERVICES CANADA
PORTAGE III 6B1
11 LAURIER ST
Gatineau
Quebec
K1A0S5
Canada

Instructions: See Herein

Instructions: Voir aux présentes

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

Delivery Required - Livraison exigée 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**

Canada

Method of Supply for Software-as-a-Service Requirements: Request for Information / Industry Consultations

1. Purpose and Nature of the Request for Information (RFI)

Public Services and Procurement Canada (PSPC) is requesting Industry feedback on establishing a new method of supply for Software-as-a-Service (SaaS) requirements to align with the new GC Cloud First direction. This new method of supply is intended to initially cover requirements with Protected B data, and in the future, may expand to cover requirements with higher and lower data classifications. This new method of supply is part of the Government of Canada (GC) Cloud Services Procurement Vehicle framework, which is envisioned to consist of various methods of supply satisfying both classified and unclassified cloud requirements. The GC Cloud Services Procurement Vehicle framework will help position the GC and public sector partners to leverage the latest digital technologies to achieve better results for Canadians.

The objectives of this new method of supply are to:

- simplify the procurement process to acquire SaaS solutions and support GC procurement modernization and contract simplification initiatives;
- increase competition and access to the latest SaaS solutions on the market for the GC; and
- increase transparency, openness and fairness in public sector procurement processes.

This RFI formally kicks-off the consultation and engagement phase with Industry and stakeholders to help inform the design and development of the SaaS method of supply. This phase includes initial questions and draft documents for comment and formal industry engagement sessions (e.g. Industry Day and one-on-one sessions). Following the consultation and engagement phase, the intent is to proceed with a subsequent qualification and solicitation phase leading to the establishment of the new method of supply.

2. Background Information

Cloud computing represents a dynamic shift in the way IT services and solutions are delivered. In 2014, the GC and provincial and territorial partners through the pan-Canadian Public Sector Chief Information Officer Council (PSCIOC) initiated a consultation process on adopting cloud computing technology in the public sector. A RFI was published by PSPC, in collaboration with Treasury Board of Canada Secretariat (TBS CIOB), on BuyandSell.gc.ca (EN578-151297/B) in December 2014 seeking comments on cloud adoption affecting four public sector pillars: business, policy, security and procurement. The RFI closed in January 2015 with 67 responses received and subsequent one-on-one meetings with RFI respondents. A summary of the consultation report can be accessed here: https://buyandsell.gc.ca/procurement-data/tender-notice/PW-EEM-039-29691

Following the 2014 RFI, the GC has been actively preparing for the adoption of cloud computing through further consultations and publication of policies and guidance. In 2016 the GC released the IT Strategic Plan and the Cloud Adoption Plan. These documents identified departmental roles and guiding principles for cloud adoption, while also identifying the need for multiple cloud deployment models to support the GC's cloud adoption efforts. More information on the GCs direction on cloud computing can be found in

the published GC IT Strategic Plan 2016-2020 (https://www.canada.ca/en/treasury-board-secretariat/services/information-technology/information-technology-strategy/strategic-plan-2016-2020.html) and the updated GC Cloud Adoption Strategy (https://www.canada.ca/en/treasury-board-secretariat/services/information-technology/cloud-computing/government-canada-cloud-adoption-strategy.html).

In 2016, Shared Services Canada (SSC) initiated a competitive procurement process to establish a source supply for cloud services limited to unclassified data. The solicitation process concluded in the spring of 2018 with the establishment of 26 contracts with qualified vendors offering public cloud services from eight different Cloud Service Providers (CSPs).

During the GC Cloud First Day in February 2018, Minister Qualtrough announced the collaborative initiative for key GC departments (PSPC, SSC, Treasury Board of Canada Secretariat, and the Communications Security Establishment) to establish standard and common sources of supply for public cloud services for various data classification levels.

3. Proposed Procurement Approach

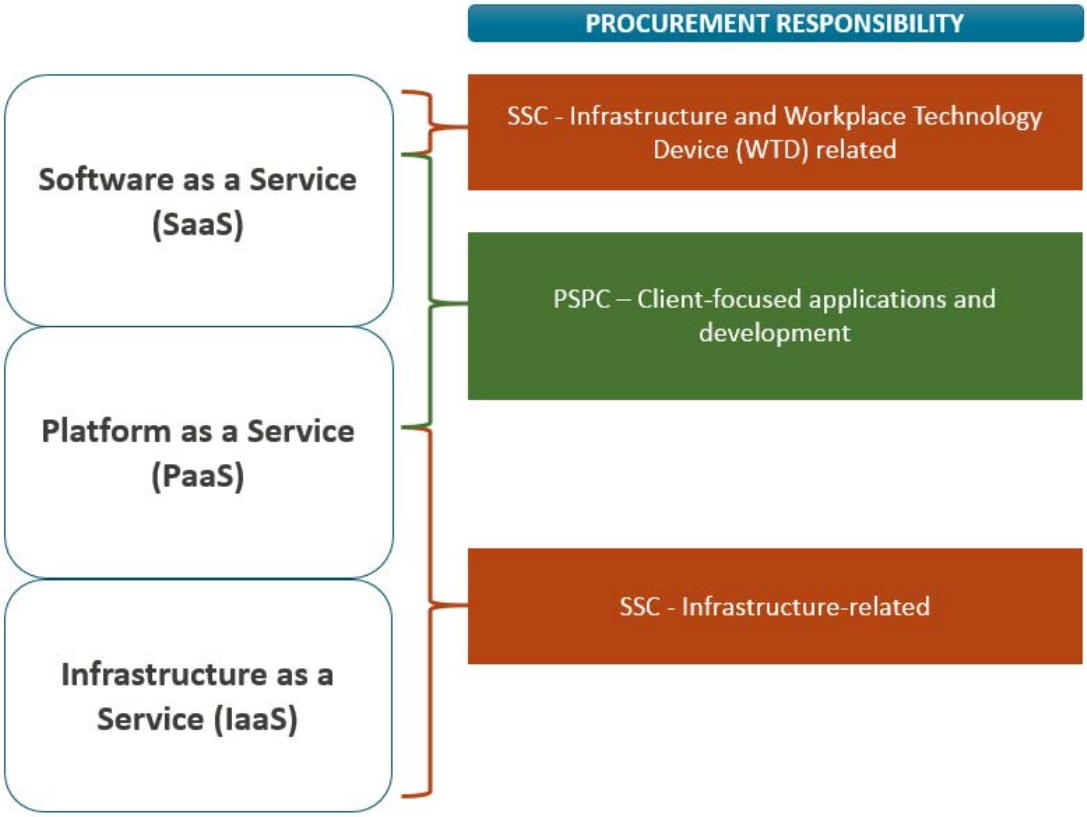
The GC Cloud Services Procurement Vehicle framework represents an innovative approach to procure cloud by leveraging various methods of supply to satisfy cloud requirements for the GC and public sector entities, which may include but not limited to provincial, territorial, and municipal governments.

On September 7, 2018, SSC published an Invitation to Qualify (ITQ) as the first phase of the procurement process for the GC Cloud Services Procurement Vehicle (https://buyandsell.gc.ca/procurement-data/tender-notice/PW-18-00841719) for Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) which would enable the procurement of these services at the Protected level. In parallel with the first phase, this PSPC consultation and engagement process will lay the foundation for the second phase, seeking feedback on proposed design and requirements to procure SaaS services and solutions.

PSPC and SSC jointly support federal organizations in procuring IT goods and services. With respect to procuring cloud-based offerings, the procurement responsibilities of each organization extends to the various elements of cloud stack from the infrastructure to the software application layers. The division of procurement responsibilities reflects the procurement mandates of each respective organization in supporting GC clients.

In line with each organization’s mandate, SSC’s procurement role in cloud-based offerings mirrors their responsibilities in managing the GC infrastructure, networks, common workplace technology devices and cyber security. PSPC’s procurement role is primarily in software application and development space, supporting clients in their service delivery and back-office functions.

Note, the diagram below represents the division of responsibilities only and is not specific to a requirement:



It is proposed that the new SaaS method of supply utilize PSPC's Supply Arrangement methodology, qualifying SaaS suppliers for award of Supply Arrangements with SaaS solution catalogues and to enable subsequent simplified solicitation and contracting processes to facilitate individual client requirements. This consultation and engagement process will help lead into a subsequent solicitation process for the SaaS method of supply.

3.1 Proposed Qualification Approach

As cloud-based offerings increase in the marketplace, the GC recognizes the need to move in an agile manner to facilitate access to such solutions while balancing the complexities associated with adopting new IT delivery methods. The new SaaS method of supply intends to move in phases of qualification to meet the short-term and long-term objectives. SA Qualification will be open to suppliers with SaaS solutions that reside on IaaS and PaaS meeting the GC Security Control Profile for Cloud-based GC Services and associated IT security requirements at the Protected B level.

Draft qualification criteria can be found in draft Request for Supply Arrangement document attached to this RFI for comment. This qualification approach enables GC clients to access readily available SaaS solutions residing on approved cloud infrastructure.

3.2 Questions for Industry Comment

Note: Respondents are invited to respond to any or all questions, as applicable.

General Questions

1. The GC is considering a Supply Arrangement model for the proposed SaaS method of supply. Do you have any concerns with providing your solution(s) through this proposed model?
2. How can the GC best address demand for third-party marketplace solutions offered through Cloud Service Providers (CSP) in the proposed RFSA methodology? How can this method of supply best facilitate access to these SaaS solutions while managing liability and other risks?
3. Are your SaaS solutions available in both English and French? Do they comply with the Official Languages Act?
4. Are the proposed Terms and Conditions (included in the draft RFSA attached to this RFI) appropriate for SaaS solutions? Are there any additional clauses that should be included? Are there any provisions contained within the draft SaaS RFSA which would prevent your organization from submitting an arrangement?
5. Are your SaaS solutions delivered directly or via an authorized third party?
6. Please provide your Service Level Agreement (SLA) offerings for your SaaS solution(s), including but not limited to: maintenance and support model(s), language(s) of support, availability of the solution(s), response times, SLA management report standards, etc.

Financial / Licensing

7. What pricing structure, unit of measure, basis of payment, and method of payment should Canada consider as part of a future RFSA catalog? What are the benefits and drawbacks of each? Please provide user pricing, volume-based pricing, and enterprise-level pricing models.
8. What type of price support would you be willing and able to provide for your SaaS solution(s) pricing (for example: published price list, past invoices, previous GC contracts, GC Advantage price list, etc.).
9. How should the GC approach “Bring your own license (BYOL)” model(s) in the cloud context? Would you accept the BYOL model? If so, please elaborate how the licenses are tracked, managed, patched, etc.? Are there economies or benefits for the GC clients to leverage BYOL, if so please explain? What are the limitations of BYOL?
10. Are your SaaS solutions offered as SaaS only or are they also available on premise or as under a BYOL model which could be hosted on premise or on third-party infrastructure?

SaaS Categorization

11. What is the recommended approach to categorize SaaS solutions? What categorization/coding method is most commonly used and what categories/codes are most commonly available? More specifically:
    a. Are the categories, sub-categories and definitions appropriate for SaaS? If not, how can they be improved?
    b. Which is the preferred methodology for the Supply Arrangements:
        (1) One Supply Arrangement per Software Publisher; or
        (2) One Supply Arrangement with multiple Software Publishers.

Security

12. Canada has a number of policies, guidelines and requirements related to security for SaaS-based solutions, as referenced below.
    i. Security Control Profile for Cloud-based GC Services: https://www.canada.ca/en/treasury-board-secretariat/services/information-technology/cloud-computing/government-canada-security-control-profile-cloud-based-it-services.html
    ii. Direction on the Secure Use of Commercial Cloud Services: Security Policy Implementation Notice (SPIN):https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/direction-secure-use-commercial-cloud-services-spin.html

iii. Direction for Electronic Data Residency: https://www.canada.ca/en/treasury-board-secretariat/services/information-technology/policy-implementation-notices/direction-electronic-data-residency.html

a. Is your organization and solution able to meet the GC requirements outlined above? If not, please specify the requirements and/or clauses that you cannot meet and why.

b. Is your organization and your solution certified ISO 27001/ISO 27017, CSA STAR Level 2 Attestation or Level 2 Certification, and/or AICPA SOC 2, Type II? Has your IaaS/PaaS provider completed the CSE Cloud Assessment Program?

c. Does your solution meet the GC Cloud Security Controls profile as derived from the ITSG-33 PBMM baseline profile (https://www.cse-cst.gc.ca/en/publication/itsg-33)?

d. Does your solution meet the Directive on privacy practices, found at https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18309 and ISO 27018?

e. Does your solution meet TBS Web Standards (i.e. Standard on Web Accessibility - WCAG 2.0 level AA or higher) found at https://tbs-sct.gc.ca/ws-nw/index-eng.asp

f. What would be the estimated time and effort to update/upgrade the proposed SaaS solutions to meet the requirements and certifications listed above?

13. Describe your SaaS solution's security model; including, authentication, access control, data protection, encryption, authorization, masking, tokenization, anonymization and other relevant features.

Data Protection

14. How do your SaaS solutions safeguard sensitive and personal information (e.g. Protected B)?
15. Does your solution allow Canada to store its data on servers that reside in Canada and all data in transit will be appropriately encrypted? (https://www.canada.ca/en/treasury-board-secretariat/services/information-technology/policy-implementation-notices/direction-electronic-data-residency.html)
16. How is data isolated and safeguarded from other clients within the SaaS environment?
17. What exit services strategies and related service guarantees do you provide to ensure that your customers can efficiently and effectively transition to other solutions such as on premise or alternative service providers? Who maintains ownership of the data?
18. Is data encrypted and if so, how? How do you manage encryption keys? Do you offer Bring Your Own Key (BYOK) or Host Your Own Key (HYOK) options? Are all algorithms in line with CSE guidance?
19. How much control do clients have over their data? How much control do you have over your client's data?

Summary

20. Are there any areas of importance that we have not addressed that would impact the GC's ability to acquire, use, benefit from or transition away from? Please identify and explain.
21. Is there anything else that you would like to add that would help us understand your company's feedback or the industry in general?
22. Would your organization wish to participate in any future one-on-one consultations or industry days that may take place after the RFI responses have been collected and reviewed?

4. Legislation, Trade Agreements, and Government Policies

The following is indicative of some of the legislation, trade agreements and government policies that could impact any follow-on solicitation(s):

a) Canadian Free Trade Agreement (CFTA)
b) North American Free Trade Agreement (NAFTA) and/or successor agreements
c) Canada-European Union Comprehensive Economic and Trade Agreement (CETA)
d) Canada-Chile Free Trade Agreement (CCFTA)
e) Canada Peru Free Trade Agreement (CPFTA)
f) Canada-Columbia Free Trade Agreement
g) Canada-Panama Free Trade Agreement
h) Canada-Honduras Free Trade Agreement
i) Canada-Korea Free Trade Agreement
j) World Trade Organization – Agreements on Government Procurement (WTO-AGP)
k) Defence Production Act
l) Industrial and Regional Benefits (IRBs)
m) Defence Procurement Strategy (DPS)
n) Controlled Goods Program (CGP)
o) Federal Contractors Program for Employment Equity (FCP-EE)
p) Comprehensive Land Claim Agreements (CLCAs)

5. Proposed Schedule:

The following is an overview of the proposed schedule:

- October 2018: Request for Information (RFI)
- November 2018: Industry Engagement Session(s) and One on One sessions
- January/February 2019: Request for Supply Arrangement (RFSA) Qualification / Solicitation
- March 2019: Supply Arrangement Issuance / Award

6. Important Notes to Respondents

Interested Respondents may submit their responses to the PSPC Contracting Authority, identified below, preferably via email:

Name:	Vincent Wong
Title:	Supply Team Leader Public Services and Procurement Canada Acquisitions Branch
Address:	Les Terrasses de la Chaudière 10 rue Wellington Gatineau (Québec)
Telephone:	819-639-5603
E-mail:	Vincent.Wong@tpsgc-pwgsc.gc.ca

A point of contact for the Respondent should be included in the package.

Changes to this RFI may occur and will be advertised on the Government Electronic Tendering System. Canada asks Respondents to visit Buyandsell.gc.ca regularly to check for changes, if any.

6.1 Closing date for the RFI

Responses to this RFI are to be submitted to the PSPC Contracting Authority identified above, on or before November 19, 2018.

6.2 Treatment of Responses

This RFI is neither a call for tender nor a Request for Proposal (RFP). No agreement or contract will be entered into based on this RFI. The issuance of this RFI is not to be considered in any way a commitment by the GC, nor as authority to potential respondents to undertake any work that could be charged to Canada. This RFI is not to be considered as a commitment to issue a subsequent solicitation or award contract(s) for the work described herein.

Although the information collected may be provided as commercial-in-confidence (and, if identified as such, will be treated accordingly by Canada), Canada may use the information to assist in drafting performance specifications (which are subject to change) and for budgetary purposes.

Respondents are encouraged to identify, in the information they share with Canada, any information that they feel is proprietary, third party or personal information. Please note that Canada may be obligated by law (e.g. in response to a request under the Access of Information and Privacy Act) to disclose proprietary or commercially-sensitive information concerning a respondent (for more information: http://laws-lois.justice.gc.ca/eng/acts/a-1/).

Respondents are asked to identify if their response, or any part of their response, is subject to the Controlled Goods Regulations.

A review team composed of representatives of the GC will review the responses. Canada reserves the right to hire an independent consultant, if Canada considers it necessary, to review any response received as a result of this RFI. Not all members of the review team will necessarily review all responses.

Participation in this RFI is encouraged, but is not mandatory. There will be no short-listing of potential suppliers for the purposes of undertaking any future work as a result of this RFI. Similarly, participation in this RFI is not a condition or prerequisite for the participation in any potential subsequent solicitation.

Canada may, in its sole discretion, contact any respondents to follow up with additional questions or for clarification of any aspect of a response. Canada may, in its sole discretion, contact any respondents to follow up with additional questions or for clarification of any aspect of a response during one on ones meetings.

Respondents will not be reimbursed for any cost incurred by participating in this RFI.

The RFI closing date published herein is not the deadline for comments or input. Comments and input will be accepted any time up to the time when/if a follow-on solicitation is published.

6.3 National Security Exception

Canada may invoke, prior to the solicitation phase of this procurement, the national security exception provided for in the trade agreements to which Canada is a party, current and future, with respect to the Cloud Service Provider Information Technology Security (CSP ITS) Assessment and Supply Chain Integrity (SCI) Process of this procurement. Upon invocation, all requirements and procedures of the CSP ITS Assessment and SCI Process portions of this procurement would be excluded from all of the obligations of the trade agreements, for each and all purposes.

DRAFT

REQUEST FOR SUPPLY ARRANGEMENT (RFSA)

FOR

SOFTWARE AS A SERVICE (SaaS)

TABLE OF CONTENTS

PART 1 - GENERAL INFORMATION

1.1 Introduction

The Request for Supply Arrangements (RFSA) is divided into six parts plus attachments and annexes, as follows:

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

Part 2 Supplier Instructions: provides the instructions applicable to the clauses and conditions of the RFSA;

Part 3 Arrangement Preparation Instructions: provides Suppliers with instructions on how to prepare the arrangement to address the evaluation criteria specified;

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

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

Part 6 Supply Arrangement: includes the Supply Arrangement (SA) with the applicable clauses and conditions;

Part 7 Bid Solicitation and Resulting Contract Clauses: includes the instructions for the bid solicitation process within the scope of the SA and general information for the conditions which will apply to any contract entered into pursuant to the SA.

The Annexes include the SaaS Categories and Descriptions, SaaS Solutions and Ceiling Prices, SaaS Solution Usage Terms and Conditions, SaaS Solution Programs Terms and Conditions, and any other annexes.

1.2 Summary

(a) Public Works and Government Services Canada (PWGSC), on behalf of Canada, is implementing this procurement vehicle for the delivery of various Software as a Service (SaaS) Solutions, including associated maintenance and support, as required by Canada, in support of its various programs, operational needs and projects. It should be noted that this procurement vehicle is one of a number of vehicles that may be used to acquire such SaaS Solutions.

(b) The RFSA is being issued to satisfy the requirement of Canada to establish Supply Arrangements, including a Catalogue (hereinafter referred to as the Software as a Service Catalogue) for commercial SaaS Solutions and associated maintenance and support.

(c) The RFSA is also being used to establish Supply Arrangements with Aboriginal firms as defined under the Procurement Strategy for Aboriginal Business (PSAB) to allow for the possibility of Clients setting aside their requirements.

(d) Any requirement for delivery to a destination in a land claims area will be actioned as a separate requisition outside of the Supply Arrangements.

(e) Any resulting Supply Arrangements may be used to acquire Goods for 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 (each a "Client").

(f) A Notice and the RFSA will be posted continuously on the Government Electronic Tendering Service (GETS) to allow suppliers to become qualified at any given time. The Notice will contain information on which Software Category will be processed and the date when arrangements should be submitted.

(g) As cloud-based offerings increase in the marketplace, Canada recognizes the need to move in an agile manner to facilitate access to SaaS Solutions while balancing the complexities associated with adopting new IT delivery methods. Qualification for Supply Arrangements will be open to suppliers with SaaS solutions that reside on IaaS and PaaS meeting the GC Security Control Profile for Cloud-based GC Services and associated IT security requirements at the Protected B level.

(h) The order of evaluation of Arrangements will be at Canada's sole discretion. The intent is to evaluate Arrangements on a first in first out basis however this may change, as required, to meet Canada's operational requirements.

(i) Canada will not award a Supplier a SA or delay award of contract(s) to other Suppliers if a Supplier has not submitted completed documentation in its response or has submitted documentation that deviates from the terms of the RFSA.

(j) Contracts resulting from the SaaS Supply Arrangements may be subject subject to the provisions of the World Trade Organization Agreement on Government Procurement (WTO-AGP), the North American Free Trade Agreement (NAFTA), the Canada-European Union Comprehensive Economic and Trade Agreement (CETA), and the Canadian Free Trade Agreement (CFTA).

(k) This RFSA allows suppliers to use the epost Connect service provided by Canada Post Corporation to transmit their arrangement electronically. Suppliers must refer to Part 2 of the RFSA entitled Supplier Instructions for further information on using this method.

1.3 Security Requirements

There are general security requirements associated with the Software as a Service delivery model, as described in Annex F. The SaaS Solutions to be procured under this SA may also be subject to additional security requirements, depending on the clients' individual needs.

1.4 Debriefings

Suppliers may request a debriefing on the results of the request for supply arrangements process. Suppliers should make the request to the Supply Arrangement Authority within 15 working days of receipt of the results of the request for supply arrangements process. The debriefing may be in writing, by telephone or in person.

1.5 Key Terms

To be defined following industry consultations.

PART 2 - SUPPLIER INSTRUCTIONS

2.1 Standard Instructions, Clauses and Conditions

All instructions, clauses and conditions identified in the Request for Supply Arrangements (RFSA) by number, date and title are set out in the Standard Acquisition Clauses and Conditions Manual https://buyandsell.gc.ca/policy-and-guidelines/standard-acquisition-clauses-and-conditions-manual) issued by Public Works and Government Services Canada.

Suppliers who submit an arrangement agree to be bound by the instructions, clauses and conditions of the RFSA and accept the clauses and conditions of the Supply Arrangement and resulting contract(s).

The 2008 (2017-04-27) Standard Instructions - Request for Supply Arrangements - Goods or Services, are incorporated by reference into and form part of the RFSA.

Subsection 5.4 of 2008, Standard Instructions - Request for Supply Arrangements - Goods or Services, is amended as follows:

Delete: 60 days
Insert: 180 days

2.2 Submission of Arrangements

If the Supplier chooses to submit its arrangement electronically using epost Connect service, Canada requests that the Supplier submits its arrangement in accordance with section 08 of the 2008 standard instructions. Suppliers are required to provide their arrangement in a single transmission. The epost Connect service has the capacity to receive multiple documents, up to 1GB per individual attachment. The approved formats for documents are any combination of:

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

If the Supplier chooses to submit its arrangement by Email, Canada requests that the Supplier submits its arrangement in accordance with the following:

(i) **Email submission**: Arrangements must be submitted by email to *[Email address to be provided at RFSA release time].*

(ii) **Format of Email Attachments**: The approved formats for email attachments are any combination of:

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

(iii) **Email Size:** Suppliers should ensure that they submit their response in multiple emails if any single email, including attachments, exceeds 5 MB.

(iv) **Email Title: Suppliers are requested to include the RFSA No. in the "subject" line of each email forming part of the response.**

Due to the nature of the Request for Supply Arrangements, transmission of arrangements by mail or by facsimile to PWGSC will not be accepted.

2.3 Federal Contractors Program for Employment Equity - Notification

The Federal Contractors Program (FCP) for employment equity requires that some contractors make a formal commitment to Employment and Social Development Canada (ESDC) - Labour to implement employment equity. In the event that this Supply Arrangement would lead to a contract subject to the Federal Contractors Program (FCP) for employment equity, the bid solicitation and resulting contract templates would include such specific requirements. Further information on the Federal Contractors Program (FCP) for employment equity can be found on Employment and Social Development Canada (ESDC) - Labour's website.

2.4 Enquiries - Request for Supply Arrangements

All enquiries must be submitted in writing to the Supply Arrangement Authority.

Suppliers should reference as accurately as possible the numbered item of the RFSA to which the enquiry relates. Care should be taken by Suppliers 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 Suppliers do so, so that the proprietary nature of the question(s) is eliminated, and the enquiry can be answered to all Suppliers. Enquiries not submitted in a form that can be distributed to all Suppliers may not be answered by Canada.

2.5 Applicable Laws

The Supply Arrangement (SA) and any contract awarded under the SA must be interpreted and governed, and the relations between the parties determined, by the laws in force in Ontario, Canada.

Suppliers may, at their discretion, substitute the applicable laws of a Canadian province or territory of their choice without affecting the validity of the arrangement, 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 Suppliers.

2.6 Suppliers

(a) **Software Publishers as Suppliers**: Software Publishers are permitted to submit an Arrangement(s) and qualify as a Supplier in their own right. A Software Publisher directly contracting with Canada must submit the certification Form 2.

(b) **Resellers as Suppliers**: Entities other than Software Publishers are permitted to submit an Arrangement and qualify as a Supplier in their own right. An entity other than a Software Publisher directly contracting with Canada must submit certification from a Software Publisher, in accordance Form 3, that the Supplier has been authorized to supply the Software Publisher's SaaS.

PART 3 - ARRANGEMENT PREPARATION INSTRUCTIONS

3.1 Arrangement Preparation Instructions

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

Section I: Technical Arrangement
Section II: Financial Arrangement
Section III: Certifications
Section IV: Additional Information, if applicable

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

3.2 Section I: Technical Arrangement

(a) In the technical arrangement, Suppliers should explain and demonstrate how they propose to meet the requirements contained in the RFSA and provide all documents and information that is requested. The technical Arrangement should address clearly and in sufficient depth the points that are subject to the evaluation criteria against which the Arrangement will be evaluated.

(b) Canada requests that the Suppliers address and present topics and information in the format outlined in the applicable annex and/or form of the RFSA.

(c) **The technical Arrangement consists of:**

(i) **Arrangement Submission Form**: Form 1 - Arrangement Submission Form must accompany the Arrangement. It provides a common form in which Suppliers can provide information required, such as a contact name, the Supplier's Procurement Business Number, the Suppliers status under the Federal Contractors Program for Employment Equity, etc. If Canada determines that the information required by the Arrangement Submission Form is incomplete or requires correction, Canada will provide the Supplier with an opportunity to submit the required corrections.

(ii) **SaaS Solution Usage Terms and Conditions:** Suppliers must submit SaaS Solution Usage Terms and Conditions to be included in Annex C - SaaS Solution Usage Terms and Conditions of the resulting SA.

SaaS Usage Terms and Conditions that apply to Canada's use of the SaaS Solution(s) may consist of a single document which applies to all SaaS Solutions or may consist of multiple SaaS Solution specific documents. Should a Supplier submit multiple SaaS Solution specific documents, the Supplier must clearly outline which SaaS Solutions listed in Annex C – SaaS Solutions and Ceiling Prices the terms apply to.

The following are examples of terms that may be addressed in the SaaS Solution Usage Terms and Conditions:

(a) license type (e.g. User, Entity, etc.);
(b) license term (e.g. Monthly, Annual, etc.);
(c) metric (how the usage is measured);

(d) rights to use;
(e) limitations of use; and
(f) Warranty.

The Supplier acknowledges and agrees that by submitting an Arrangement that any terms contained in Annex C - SaaS Solution Usage Terms and Conditions that purport to interpret the RFSA, or are the same or similar subject matter or related to, the terms contained in the RFSA and Resulting Contract Clauses are deemed stricken and are of no force or effect.

(iii) **Service Level Agreements (SLA)**: Suppliers must submit published service level agreements (SLA) that outline the service level agreements to be included in Annex D – SaaS Solution Service Level Agreements (SLA).

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

Service Level Agreements may consist of a single document which applies to all SaaS Solutions or may consist of multiple SaaS Solution specific documents. Should a Supplier submit multiple SaaS Solution specific SLA documents, the Supplier must clearly outline which SaaS Solution listed in Annex B - SaaS Solutions and Ceiling Prices, the SLA applies to. If SLA terms are already specified in the SaaS Usage Terms and Conditions, duplicate terms need not be provided.

The following are examples of terms that may be addressed in the Supplier's Service Level Agreement:

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

The Supplier acknowledges and agrees that by submitting an Arrangement that any terms contained in Annex D - SaaS Solution Service Level Agreements (SLA) that purport to interpret the RFSA, or are the same or similar subject matter or related to, the terms contained in the RFSA and Resulting Contract Clauses are deemed stricken and are of no force or effect.

(iv) **Program Terms and Conditions**: Suppliers may submit Program Terms and Conditions that apply to Canada as a major Customer of the SaaS Solutions, to be included in Annex E – SaaS Solution Program Terms and Conditions of the resulting SA.

For the purpose of Supplier's Programs, Canada must be treated as a single entity. Programs targeting specific Client(s) are not permitted.

Examples of Programs include enterprise programs, volume based programs, and business level agreements.

The following may be addressed in these terms:

(a) Additional grants, rights, or entitlements;

(b) Volume discount programs.

The Supplier acknowledges and agrees that by submitting an Arrangement any terms contained in Annex E – SaaS Solution Program Terms and Conditions that purport to interpret the RFSA or that conflict with, or are of a similar nature or related to, those contained in the RFSA are deemed stricken and are of no force or effect**.**

(v) **Form 6 - Mandatory Vendor Arrangement Submission Checklist** must accompany the Arrangement. It provides a common form in which Suppliers can verify that their arrangement includes all of the required information to be deemed complete, prior to submitting. If Canada determines that the checklist and/or Arrangement submission is incomplete or requires correction, Canada will provide the Supplier with an opportunity to submit the required corrections.

The Supplier acknowledges and agrees that by submitting an Arrangement that all other terms submitted as part of the Technical Arrangement are deemed stricken and form no part of the supply Arrangement.

3.3 Section II: Financial Arrangement

(a) In the Financial Arrangement, the Suppliers must submit a list of SaaS Solutions with ceiling prices. It is required that the list of SaaS Solutions and ceiling prices section of the Arrangement be submitted as per the template provided in Annex B – SaaS Solutions and Ceiling Prices of the RFSA. The Financial Arrangement should address clearly and in sufficient depth the points that are subject to the evaluation criteria against which the Arrangement will be evaluated.

(b) The following must be addressed in the Supplier's Annex B – SaaS Solutions and Ceiling Prices:

(A) **Software Publisher's Part No.:** Supplier must provide the part number that the Software Publisher uses to identify the SaaS Solution commercially;

(B) **SaaS Solution's Name:** Supplier must provide the commercial name that the Software Publisher uses to identify the SaaS Solution commercially.

(C) **Software Publisher's Name:** Supplier must provide the name of the Software Publisher that owns the Intellectual Property rights to the SaaS Solution;

(D) **Cloud Service Provider (CSP):** Supplier must identify the existing Cloud Service Provider (CSP), who's Commercially Available Cloud Services will be used to supply to Canada the proposed Software as a Service (SaaS).

(E) **Ceiling Unit Price:** Suppliers must submit ceiling unit prices for all items proposed in Annex B – SaaS Solution and Ceiling Prices. The prices must be:

(a) Ceiling unit price;

(b) in Canadian dollars;

(c) exclusive of Goods and Services Tax or Harmonized Sales tax; and

(d) for a period no greater than one year.

(F) **License Type:** Supplier must enter the license type (such as “per user”, “per entity”, etc.) under which the SaaS will be provided to Canada;

(G) **SaaS Category:** the Supplier must enter the applicable category or categories of the SaaS Solution(s). The SaaS category must correspond with the category descriptions under Annex A - SaaS Categories and Descriptions.

(H) **Language(s) available:** The Supplier must provide the language(s) under which the SaaS Solution is available, designated as “EN” for English, “FR” for French, or “EN, FR” for both;

(I) **SaaS Solution Information:** The Supplier may provide a web site URL containing information on the SaaS Solution.

(c) **Price reference**: Supplier must provide a price reference(s) to substantiate that their proposed prices are fair and reasonable. Examples of acceptable price references include, but are not limited to, the following:

1) a current published price list indicating the percentage discount available to Canada; or
2) copies of paid invoices for the like quality and quantity of the goods, services or both sold to other customers; or
3) 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
4) price or rate certifications; or
5) GSA Advantage prices; or
6) any other supporting documentation as requested by Canada.

3.4 Section III: Certifications

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

PART 4 - EVALUATION PROCEDURES AND BASIS OF SELECTION

4.1 Evaluation Procedures

(a) Arrangements will be assessed in accordance with the entire requirement of the Request for Supply Arrangements including the technical evaluation criteria.

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

(c) **Requests for Clarifications**: If Canada seeks clarification or verification from a Supplier about its Arrangement, the Supplier will have 2 working days (or a longer period if specified in writing by the Supply Arrangement Authority) to provide the necessary information to Canada. Failure to meet any deadline will render the Arrangement non-responsive, on “hold”, or will create delay in processing a Supplier's SA

(d) **Right of Canada:**

(i) Canada reserves the right to reject any of the SaaS Solutions proposed by a Supplier and enter into negotiation related to any ceiling prices under Annex B – SaaS Solutions and Ceiling Prices;

(ii) Canada reserves the right to reject or negotiate any of the terms and conditions proposed by a Supplier and submitted under Annex C – SaaS Solution Usage Terms and Conditions and/ Annex D - SaaS Solution Service Level Agreements (SLA) and/or Annex E - SaaS Solution Program Terms and Conditions. No Supply Arrangement will be awarded unless and until Canada has approved all such terms and conditions;

(iii) Canada reserves the right to reject proposed products under a specific SaaS Category or to request that a Supplier reclassify the SaaS Solution(s) which it deems to not correspond with the category definitions under Annex A – SaaS Categories and Descriptions;

4.2 Technical and Financial Evaluation

(a) Arrangements will be reviewed to determine whether they meet the mandatory requirements of the RFSA. All elements of the RFSA that are mandatory requirements are identified specifically with the words “must” or “mandatory”. Supplier’s with Arrangement(s) that do not comply with each and every mandatory requirement will be notified by the Supply Arrangement Authority and will be provided with a time frame within which to meet the requirement. Failure to comply with the request of Canada and meet the requirements within that time period will render the Arrangement non-responsive, disqualified**,** on “hold”, or will create delay in processing a Supplier's SA.

4.2.1 Mandatory Technical Criteria

The mandatory technical requirements are as follows:

(i) Arrangement Submission Form as per Article 3.2 (c)(i);

(ii) SaaS Solution Usage Terms and Conditions as per Article 3.2 (c)(ii);

(iii) Certifications as per Article 3.4; and,

(iv) Financial Viability as per Article 4.4.

4.2.2 Financial Evaluation

The mandatory financial requirements are as follows:

(i) SaaS Solutions and Ceiling Prices as per Article 3.3 (a) and (b); and

(ii) Price reference(s) as per Article 3.3 (c).

4.2 Basis of Selection

4.2.1 Basis of Selection - Mandatory Technical and Financial Evaluation Criteria

An arrangement must comply with the requirements of the Request for Supply Arrangements and meet all mandatory technical evaluation criteria and financial evaluation criteria to be declared responsive.

4.3 Financial Viability

SACC Manual clause S0030T (2014-11-27) Financial Viability.

PART 5 – CERTIFICATIONS AND ADDITIONAL INFORMATION

Suppliers must provide the required certifications and additional information to be issued a supply arrangement (SA).

The certifications provided by Suppliers to Canada are subject to verification by Canada at all times. Unless specified otherwise, Canada will declare an arrangement non-responsive, or will declare a contractor in default if any certification made by the Supplier is found to be untrue whether made knowingly or unknowingly during the arrangement evaluation period, or during the period of any supply arrangement arising from this RFSA and any resulting contracts.

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

5.1 Certifications Required with the Arrangement

Suppliers must submit the following duly completed certifications as part of their arrangement.

5.1.1 Integrity Provisions - Declaration of Convicted Offences

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

5.1.2 Additional Certifications Required with the Arrangement

To be determined following industry consultations.

5.2 Certifications Precedent to the Issuance of a Supply Arrangement and Additional Information

The certifications and additional information listed below should be submitted with the arrangement, but may be submitted afterwards. If any of these required certifications or additional information is not completed and submitted as requested, the Supply Arrangement Authority will inform the Supplier 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 arrangement non-responsive.

To be determined following industry consultations.

PART 6 - SUPPLY ARRANGEMENT

6.1 Arrangement

The Supply Arrangement (SA) is issued to allow Canada to set up a competitive procurement vehicle to acquire Software as a Service (SaaS) Solutions, including associated maintenance and support, as required by Canada, in support of its various programs, operational needs and projects, through a SaaS catalogue (herein after referred to as the SaaS Catalogue), that will amalgamate the SaaS Solutions under all issued SAs. SaaS Solutions are listed by each Supplier under Annex B - SaaS Solutions and Ceiling Prices and fall under one or more of the SaaS categories listed in Annex A - SaaS Categories and Descriptions.

6.2 Security Requirements

The Supplier must meet the security requirements as indicated in Annex F – Security Requirements, as applicable.

6.3 Standard Clauses and Conditions

All clauses and conditions identified in the Supply Arrangement and resulting contract(s) by number, date and title are set out in the Standard Acquisition Clauses and Conditions Manual (https://buyandsell.gc.ca/policy-and-guidelines/standard-acquisition-clauses-and-conditions-manual) issued by Public Works and Government Services Canada.

6.3.1 General Conditions

2020 (2017-09-21) General Conditions - Supply Arrangement - Goods or Services, apply to and form part of the Supply Arrangement.

6.3.2 Supply Arrangement Reporting

The Supplier must compile and maintain records on its provision of goods, services or both to the federal government under contracts resulting from the Supply Arrangement. This data must include all purchases, including those paid for by a Government of Canada Acquisition Card.

The data must be submitted or made available for download on a quarterly basis to the Supply Arrangement Authority.

The quarterly reporting periods are defined as follows:

- 1st quarter: April 1 to June 30;
- 2nd quarter: July 1 to September 30;
- 3rd quarter: October 1 to December 31;
- 4th quarter: January 1 to March 31.

The data must be submitted or made available for download to the Supply Arrangement Authority no later than 30 calendar days after the end of the reporting period.

6.4 Term of Supply Arrangement

6.4.1 Period of the Supply Arrangement

The period for awarding contracts under the Supply Arrangement is from _____ to _____.

6.4.2 Comprehensive Land Claims Agreements (CLCAs)

The Supply Arrangement (SA) is for the delivery of the requirement detailed in the SA to the Identified Users across Canada, excluding locations within Yukon, Northwest Territories, Nunavut, Quebec, and Labrador that are subject to Comprehensive Land Claims Agreements (CLCAs). Any requirement for deliveries to locations within CLCAs areas within Yukon, Northwest Territories, Nunavut, Quebec, or Labrador will have to be treated as a separate procurement, outside of the supply arrangement.

6.5 Authorities

6.5.1 Supply Arrangement Authority

The Supply Arrangement Authority is:

Name: _____
Title: _____

Public Works and Government Services Canada
Acquisitions Branch
Software Procurement Directorate

Les Terrasses de la Chaudière, 4th Floor
10 Wellington St. ,
Gatineau, Quebec K1A 0H4

Telephone: ____ - ___ - ____
Facsimile: 819-956-2675
E-mail address: _____

The Supply Arrangement Authority is responsible for the issuance of the Supply Arrangement, its administration and its revision, if applicable.

6.5.2 Supplier's Representative

Fill in or delete, as applicable.

6.6 Identified Users

The Supply Arrangement may be used to acquire SaaS Solutions by any Government Department, Departmental Corporate or Agency, or other body of Canada (including those described in the Financial Administration Act as amended from time to time), and any other party for which PWGSC has been authorized to act.

6.7 On-going Opportunity for Qualification

A Notice will be posted continuously on the Government Electronic Tendering Service (GETS) to allow new Suppliers to become qualified.

6.8 Priority of Documents

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

(a) the articles of the Supply Arrangement;
(b) the general conditions 2020 (2017-09-21), General Conditions - Supply Arrangement - Goods or Services
(c) Annex ___, _____; (*if applicable*)
(d) Annex ___, _____; (*if applicable*)
(e) the Supplier's arrangement dated _____ (*insert date of arrangement*) *(if the arrangement was clarified or amended, insert at the time of issuance of the arrangement:* "as clarified on _____" ***or*** "as amended _____"*. (Insert date(s) of clarification(s) or amendment(s), if applicable)*.

6.9 Certifications and Additional Information

6.9.1 Compliance

Unless specified otherwise, the continuous compliance with the certifications provided by the Supplier in its arrangement or precedent to issuance of the Supply Arrangement (SA), and the ongoing cooperation in providing additional information are conditions of issuance of the SA and failure to comply will constitute the Supplier in default. Certifications are subject to verification by Canada during the entire period of the SA and of any resulting contract that would continue beyond the period of the SA.

6.10 Applicable Laws

The Supply Arrangement (SA) and any contract resulting from the SA must be interpreted and governed, and the relations between the parties determined, by the laws in force in _____ *(insert the name of the province or territory as specified by the Supplier in the arrangement, if applicable).*

PART 7 - BID SOLICITATION AND RESULTING CONTRACT CLAUSES

7.1 Bid Solicitation Documents

The bid solicitation will contain as a minimum the following:

(a) security requirements (*if applicable*);

(b) a complete description of the Software as a Services to be provided;

(c) 2003, Standard Instructions - Goods or Services - Competitive Requirements; ***OR*** 2004, Standard Instructions - Goods or Services - Non-competitive Requirements;

Subsection 3.a) of Section 01, Integrity Provisions - Bid of the Standard Instructions 2003 or 2004 (as applicable) incorporated by reference above is deleted in its entirety and replaced with the following:

a. at the time of submitting an arrangement under the Request for Supply Arrangements (RFSA), the Bidder has already provided a list of names, as requested under the *Ineligibility and Suspension Policy*.During this procurement process, the Bidder must immediately inform Canada in writing of any changes affecting the list of directors."

(d) bid preparation instructions;

(e) instructions for the submission of bids (address for submission of bids, bid closing date and time);

(f) evaluation procedures and basis of selection;

(g) financial capability (*if applicable*);

(h) certifications*;*

(i) conditions of the resulting contract.

The bid solicitation templates will be developed following industry consultations.

7.2 Bid Solicitation Process

Bids will be solicited for specific requirements within the scope of the Supply Arrangement (SA) from Suppliers who have been issued a SA.

The bid solicitation will be posted on the Government Electronic Tendering Service (GETS) or sent directly to Suppliers.

7.2 Resulting Contract Clauses

The terms and conditions of any contract awarded under the Supply Arrangement will be defined following industry consultations.

ANNEXES

Annex A - SaaS Categories and Descriptions

Category ID	Category	Subcategory	Description
100	Data Management Software		**Corporate Data Management Software delivers, enables and supports Data Management as a corporate platform. Corporate Data Management Software provides the management of corporate data resources and services by developing and execution of the architectures, policies, practices and procedures that properly manage the full data life cycle needs at a corporate level.**
102	Data Management Software	**Business Intelligence Software**	Business Intelligence Software provides business information, data and reporting on a work group or entity wide basis. Functionality, design components and interfaces enable data-mining, scheduled and ad-hoc reporting and interoperability with other software such as performance measurement.
104	Data Management Software	**Data Warehouse Software**	Data Warehouse Software enables the creation and management of a data repository as a data warehouse and includes the functionality to retrieve and analyze data, to extract, transform and load data, and to manage the data dictionary.
106	Data Management Software	**Relational Database Management Systems Software**	Relational Database Management Systems Software controls the creation, maintenance, and the use of a database including data that is stored in the form of tables and the relationship among the data is also stored in the form of tables.
108	Data Management Software	**Database Modeling Software**	Database Modeling Software aids in the modeling and graphical design of a database and determines the manner in which data is stored, organized and manipulated in a database.
110	Data Management Software	**Database Tools, Utilities & Management Software**	Database Tools, Utilities and Management Software are interactive tools; utilities and service management packs that manage, analyze and report test data results within a database environment.

Category ID	Category	Subcategory	Description
112	Data Management Software	Extract, Transformation and Load Software	Extract, Transformation and Load (ETL) Software aids in the extraction, transformation and load of data from outside sources into a database or data integration applications.
114	Data Management Software	Master Data Management Software	Master Data Management Software providing processes for collecting, aggregating, matching, consolidating, quality-assuring, persisting and distributing data throughout an organization to ensure consistency and control in the ongoing maintenance and application use of this information.
116	Data Management Software	On-Line Analytical Processing Software	On-Line Analytical Processing (OLAP) Software provides multidimensional analytical processing, queries and reporting of data and information online.
118	Data Management Software	Personal Database Software	Personal Database Software has database functionality and design that is typically of a personal or client workstation nature, as compared to a large corporate relational database. This software stores user-entered data in a structured file format, supporting ad-hoc queries, provides tools for sorting, selecting, and viewing user-specified records and generates reports on records matching user-specified criteria
120	Data Management Software	Web Analytical Software	Web Analytical Software is used to collect, analyze and report on website activities. The measurements and analysis is typically used to report, improve and or optimize websites and Internet activities
200	Information Management Software		**Corporate Information Management Software delivers, enables and supports Information Management as a Corporate Platform. Corporate Information Management provides the management of information resources and services by developing and execution of the architectures, policies, practices and procedures that properly manage the full information life cycle needs at a corporate level.**

Category ID	Category	Subcategory	Description
202	Information Management Software	Case Management Software	Case Management Software is a product group that provides management of case(s) including collaborative communication, assessment, planning, implementation, coordinated work-flow, monitoring, and evaluation functionality and design and integrates/patterns contents from different data sources while tracing (audit trail) the status of ongoing data, information, and decisions.
204	Information Management Software	Content Management Software	Content Management Software provides the collection, taxonomy analysis of information and search and retrieval functionality and design. This software can also automatically scan content according to a predefined set of rules for future cross-referenced retrieval. Additional capabilities include the application of common publishing templates for common look and feel within a work-group or entity wide application.
206	Information Management Software	Digital Asset Management Software	Digital Asset Management Software manages the annotation, cataloguing, storage, retrieval and distribution of digital assets such as audio, video, and other media content.
208	Information Management Software	Document Management Software	Document Management Software provides storage, processing, management and retrieval capabilities for electronic documents and files. Document Management Software often interfaces with word processing, image recognition, text retrieval and database systems and data.
210	Information Management Software	Document Scanning and Image Recognition Software	Document Scanning and Image Recognition Software automates the process of scanning and identifying content in hard-copy documents through optical character recognition processes and procedures.
212	Information Management Software	Electronic Forms Software	Electronic forms software enables users to design and utilize forms electronically and is often used to create data entry systems that interface with data repositories or databases.
214	Information Management Software	Feedback Management Software	Feedback Management Software enables organizations to centrally manage deployment of client surveys while dispersing authoring and analysis throughout an organization. Often

Category ID	Category	Subcategory	Description
			used to process client feedback using Internet technologies.
216	Information Management Software	Knowledge Management Software	Knowledge Management Software provides a wide variety of methods that can be used to simulate the performance of the expert with a knowledge base. This software uses some knowledge representation to capture the Subject Matter Expert's (SME) knowledge and a process of gathering that knowledge from the SME and codifying it according to the formalism, which is called knowledge engineering.
218	Information Management Software	Portal Software	Portal Software creates, enables and makes possible Internet, Intranet, Extra-net and or Virtual Private Network(s) containing multiple channel services, processes or methodology to meet electronic organizational demand. Functionality and design integrates multiple platforms and data streams of input into a single dynamic, real time client user environment.
220	Information Management Software	Records Management Software	Records Management Software offers record management functionality and procedures that process files and records within an organization and typically includes classification, storage and archival or destruction of records.
222	Information Management Software	Search and Information Access Software	Search and Information Access Software provides an entry point for access to information. Information sources can be single repositories or multiple sources of information. Search and Information Access capabilities often include looking up and retrieving information that has multiple dimensions or facets thereby enabling users to explore, locate, organize, and retrieve data and information.
224	Information Management Software	Social Media Software	Social Media Software provides platforms for social communication such as blogs, social networking, etc and often includes collaborative authoring that includes wikis, bookmarking, etc and multimedia such as photo, audio and or video sharing.

Category ID	Category	Subcategory	Description
226	Information Management Software	Web Content Management Software	Web Content Management Software provides management functionality and features that automate or and or improve the authoring, editing and administration procedures for web content publishing and distribution.
228	Information Management Software	Workflow & Collaboration Software	Workflow and Collaboration Software automates and manages the workflow of a work-group or entity. This software enables information or tasks to be passed from one or more participants and or resources, according to a set of procedural rules.
230	Information Management Software	Incident and Field Resource Management Software	Incident and Field Resource Management Software provides response management of incidents and resources for resolution in emergency and non-emergency environments. Incident and Field Management Software also provides policy and procedural functions and features, reporting capabilities, as well as alerting, messaging and group communications functions and performance elements.
300	Enterprise Resource Management Software		**Corporate Resource Management Software delivers, enables and supports Resource Management as a Corporate Platform. Corporate Resource Management provides the management of corporate information resources and services by development and executes the architectures, policies, practices and procedures that properly identifies and manages the full resource life cycle needs at a corporate level.**
302	Enterprise Resource Management Software	Bar-Coding & Labeling Software	Bar Coding and Labeling Software provides UPC bar code scanning, processing and storing functionality and design. Bar Coding and Labeling Software typically provides the ability to design and print labels and bar codes, supports bar code readers and supports major bar code standards while integrating with software applications and development tools such as inventory and financial management business functions.

Category ID	Category	Subcategory	Description
304	Enterprise Resource Management Software	Budget Preparation Software	Budget Preparation Software is used to plan fiscal budgets and often includes scenario planning of a strategic nature. Budgets are typically involving corporate finances, decision analysis and or investment decision processes.
306	Enterprise Resource Management Software	Customer Relationship Management Software	Customer Relationship Management Software (CRM) manages interactions with customers and or clients and provides entity wide management of client or customer data and information for data mining, profiling and return on investment analysis. CRM will typically organize, automate and augment business processes and procedures. CRM will often act as an interface for entity wide systems such as accounting, human resources and database.
308	Enterprise Resource Management Software	Enterprise Resource Planning Software	Enterprise Resource Planning Software provides entity wide planning and management of resources so as to allow and improve the information flow between business units and functions inside an enterprise. Typically will use a central database on a common platform so as to consolidate business policies, processes and procedures in a uniform manner enterprise wide.
310	Enterprise Resource Management Software	Finance & Accounting Software	Finance and Accounting Software provides accounting, financial management and financial asset control functionality and design. Standard capabilities include General Ledger (GL), Accounts Receivable (AR), Accounts Payable (AP), Inventory, Purchase Order (PO) and Point of Sale (POS). This software also tracks securities and investments, debts, rates, budgeting, grants, loans, downloads financial transactions and investment status from online data sources, forecasts future revenue, income, and or cash flow programs, modules or components.
312	Enterprise Resource Management Software	Financial Auditing Software	Financial Auditing Software allows for the audit review and analysis of the financial statements of an organization allowing for conclusions on whether or not those financial statements are relevant, accurate, complete, and fairly represent the organization’s position.

Category ID	Category	Subcategory	Description
314	Enterprise Resource Management Software	Governance Risk, Compliance & Incident Management	Governance Risk, Compliance & Incident Management Software covers activities including corporate governance, enterprise risk management and corporate compliance verification and validation against applicable laws and regulations.
316	Enterprise Resource Management Software	Grants & Contributions Management Software	Grants and Contributions Management Software assists in the designing, building and deploying of grants. This software controls all aspects of the funding process - from initial requests, through assessments and recommendations, to authorizations, payments and subsequent monitoring of outcomes.
318	Enterprise Resource Management Software	Human Resource Evaluation & Selection Systems Software	Human Resource Evaluation and Selection Systems Software assists in employee management within an organization. This software provides forms, coordinates procedures, tallies results and or statistics in an effort to effectively evaluate, manage and inform the human resources of an organization.
320	Enterprise Resource Management Software	Human Resource Management Systems Software	Human Resources Management Systems Software captures and records human resource data through database, reporting and analysis features and functions. Human Resource Management Systems Software typically interfaces with other corporate administrative applications.
322	Enterprise Resource Management Software	Inventory & Asset Management Software	Inventory and Asset Management Software manages assets from acquisition, usage to disposal and provides management and administrative functionality, design, components and interfaces. This software also provides asset record keeping, asset tracking, bar code software and interfaces with common databases.
324	Enterprise Resource Management Software	Library Management Systems Software	Library management systems software is an enterprise resource planning system for a library, used to track items owned, orders made, bills paid, and patrons who have borrowed or are using library assets.

Category ID	Category	Subcategory	Description
326	Enterprise Resource Management Software	Pension Software	Pension Software manages, collects, and allocates retirement benefits.
328	Enterprise Resource Management Software	Performance Measurement Software	Performance Management Software supports performance & accountability frameworks and provides tools to aide in collecting supporting data that is used for performance measurement, evaluations, and audits.
330	Enterprise Resource Management Software	Procurement & Contract Management Software	Procurement and Contract Management Software helps to automate the purchasing function of organizations and establish effective process and compliance management.
332	Enterprise Resource Management Software	Property Management Software	Property Management Software coordinates personal property, equipment, tooling and physical capital assets that are acquired and used to build, repair and maintain end item deliverable. Property management involves the processes, systems and manpower required to manage the life cycle of all acquired property as defined above including acquisition, control, accountability, maintenance, utilization, and disposition.
334	Enterprise Resource Management Software	Salary Management & Payroll Software	Salary Management and Payroll Software allow an organization to effectively manage salaries in accordance with complex taxation requirements and other organizational requirements.
336	Enterprise Resource Management Software	Transactional Processing & Transaction Management	Transactional Processing & Transaction Management Software handles transaction and batch processing of large number of documents, providing transformation, business process and preservation.
338	Enterprise Resource Management Software	Vendor Management Software	Vendor Management Software provides tools for engaging and managing the relationship with vendors.

Category ID	Category	Subcategory	Description
400	**Development Environments Software**		**Development Environments Software delivers, enables and supports software development as an operating environment and platform. Software Development Environments Software facilitates the design and creation of software and web applications.**
402	**Development Environments Software**	**Application Life-Cycle Management Software**	Application Life-Cycle Management (ALM) software manages the life of an application through governance, development and maintenance. It is comprised of tools that facilitate and integrate requirements management, architecture, coding, testing, tracking, and release management.
404	**Development Environments Software**	**Software Development Platform Software**	Application Development Software is used to develop software products in a planned and structured process and includes tools in which computer programs are coded.
406	**Development Environments Software**	**Software Testing Software**	Software Testing Software assesses the functionality, reliability, security and performance of software in a development environment.
408	**Development Environments Software**	**Systems Architecture Design Software**	Systems Architecture Design Software aids in designing the architecture, components, modules, interfaces, and data for a system
410	**Development Environments Software**	**Web Development Software**	Web Development Software provides tools to assist in developing web sites and applications. This can include web design, web content development, client liaison, client-side/server-side scripting, and e-commerce development.
500	**Middleware Software**		**Middleware Software delivers, enables and supports the middle layers of the OSI Stack as an Enterprise Platform; Middleware provides the software functions as an intermediate layer between applications and operating system or database management systems, or between client and server.**
502	**Middleware Software**	**Application Infrastructure Software**	Application Infrastructure Software provides a secure and flexible environment to build, deploy and run applications.

Category ID	Category	Subcategory	Description
504	Middleware Software	Application Integration & Connectivity Software	Application Integration & Connectivity Software enables the integration of systems and applications
506	Middleware Software	Business Process Management Software	Business Process Management Software helps optimize performance by discovering, documenting, automating, and continuously improving business processes.
508	Middleware Software	E-Commerce Software	E-Commerce Software automates and integrates B2B, B2C and C2B processes between disparate systems
510	Middleware Software	Managed File Transfer Software	Managed file transfer software provides a single platform supporting all methods of business file-transfer including automated, ad-hoc and collaborative processes, resulting in a centralized and fully governed file transfer solution.
512	Middleware Software	Message Oriented Middleware Software	Message Oriented Middleware (MOM) Software provides software infrastructure focused on sending and receiving messages between disparate systems
514	Middleware Software	SOA Governance Software	SOA Governance Software establishes decision rights for the development, deployment, operations and management of web services and monitors and reports on decisions and results.
600	Network Infrastructure Software		**Network Infrastructure Software delivers, enables and supports the infrastructure found within a Computer Networks. Network Infrastructure provides the network components, functions and features related to network resources and services.**
602	Network Infrastructure Software	Archive Software	Archiving Software handles documents in such a way that information can be created, shared, organized and stored efficiently and appropriately.
604	Network Infrastructure Software	Backup Software	Backup Software provides a user the ability to make an exact duplicate of an original source file, data, database, system or server and to perform a recovery of the data.

Category ID	Category	Subcategory	Description
606	Network Infrastructure Software	Data Migration Software	Data Migration Software aids in the process of transferring data between storage types, formats, or computer systems.
608	Network Infrastructure Software	Fax Software	Fax Software automates the process of sending, receiving, and managing fax traffic for an entire network. This software integrates with any existing email system giving users full faxing capabilities.
610	Network Infrastructure Software	File and Print Services Software	File and Print Services Software provides a method of filing and printing computer data typically on a network. Essentially, file services organize files into a database for the storage, organization, manipulation, and retrieval by the computer's operating system.
612	Network Infrastructure Software	Network Communications Software	Network Communications Software allows independent and potentially non-concurrent applications on a distributed system to communicate with each other.
614	Network Infrastructure Software	Network Storage Software	Network Storage Software provide file-based data storage services and provide block-based storage services in support of devices responsible for holding and retaining data on a network.
616	Network Infrastructure Software	Remote Desktop Software	Remote Desktop Software provides access and a graphical interface to another computer.
618	Network Infrastructure Software	Switching Software	Switching Software acts as a virtual hardware switch to forward packets to require ports based on the packet address.
620	Network Infrastructure Software	Unified Communications Software	Unified Communications software provides a set of integrated real-time collaboration services for voice, data and video. Functionality may include rich presence, enterprise IM, online meetings, etc.
700	Operating Systems Software		**Operating Systems Software delivers, enables and supports operating systems and how a hardware platform controls software applications and related devices found in a system infrastructure environment. It is low-level software that schedules tasks, allocates storage, handles**

Category ID	Category	Subcategory	Description
			the interface to peripheral hardware and presents a default interface to the user.
702	**Operating Systems Software**	**Desktop Operating System Software**	Desktop Operating Systems Software is an operating system designed for client workstations such as desktops, notebooks, and laptops
704	**Operating Systems Software**	**Mainframe Operating System Software**	Mainframe Operating Systems Software is an operating system designed for mainframe systems
706	**Operating Systems Software**	**Mobile Operating System Software**	Mobile Operating Systems Software is an operating system designed for mobile and small form factor devices such as phones, net-books and tablets .
708	**Operating Systems Software**	**Real-Time Operating System Software**	Real-Time Operating System Software is an operating system designed for real-time applications.
710	**Operating Systems Software**	**Server Operating System Software**	Server (Network) Operating Systems software is an operating system designed for sharing resources between client processes typically found within a network.
800	**Virtualization Software**		**Virtualization Software delivers, enables and supports virtual environments, processors and applications by isolating system resources from underlying computing or application services. Virtualization provides the components, functions and features including host and or guest systems, machines or types.**
802	**Virtualization Software**	**Application Virtualization Software**	Application Virtualization Software allows for the creation of application packages independent of any operating system. The application package can be installed and isolated from the host operating system but is still able to interact with the host and other applications. Virtual applications can be freely installed or removed without disrupting the host.
804	**Virtualization Software**	**Desktop Virtualization Software**	Desktop Virtualization Software allows for the creation and modification of an operating system independent from the hardware. The virtual desktop should be able to run on multiple different hardware platforms and move

Category ID	Category	Subcategory	Description
			freely from one to another when required without modifications.
806	Virtualization Software	Server Virtualization Software	Server Virtualization Software allows for the creation of multiple guest operating systems (Guest OS/VM) within a server host operating system (Host OS). It allows for unmodified guest operating systems to run in isolation while using the same instruction set as the Host OS. These environments utilize some resource sharing and process isolation.
808	Virtualization Software	Storage Virtualization Software	Virtualization Storage Software provides block or file allowing delivery through various protocols such as Fibre Channel or Network File System. Storage systems can provide either block-accessed storage, or file accessed storage. Access is delivered over various protocols or file systems thereby allowing separation of the logical storage from the physical storage or eliminating dependencies between data access file and location of physical data.
810	Virtualization Software	Virtualization Backup & Recovery Software	Virtualization Backup and Recovery Software provides recovery techniques with virtualized servers to improve system up time and recovery time objectives as well as recovery point objectives. This software also ensures the integrity of the data to retrieve.
812	Virtualization Software	Virtualization Management Software	Virtualization Management Software provides complete management tools to manage and optimize a virtualized environment.
814	Virtualization Software	Virtualization Monitoring Tools Software	Virtualization Monitoring Tools Software provides complete monitoring tools to monitor and set host configuration standards, infrastructure capacity, application performance and workload ownership of a virtualized environment.
816	Virtualization Software	Virtualization Security Software	Virtualization Security Software is security software specific to virtualized systems and includes software such as anti-virus, firewall, or network security.

Category ID	Category	Subcategory	Description
900	Operations Management Software		**Operations Management Software delivers, enables and supports Management Operational components, functions and features. Operations Management provides the tools, utilities and components needed to manage the provisioning, capacity, performance and availability of the computing, networking and application environment.**
902	Operations Management Software	**Change and Configuration Management Software**	Change & Configuration Management Software provides process automation, change control; build management, traceability and reporting.
904	Operations Management Software	**Desktop Management Software**	Desktop Management Software provides functionality and features to manage the desktop remotely from a central administrative location.
906	Operations Management Software	**Help Desk & Call Center Software**	Help Desk and Call Centre Software offers service desk support functions, incident management, problem management, change management, improved support staff productivity, administration and reporting functionality, information and management tools. This software may also provides contact management functions, scheduling and calendar functions and supports messaging and group communication functions.
908	Operations Management Software	**Network Management Software**	Network Management Tools software offers network management functions that provide control of a network, maximize its efficiency and productivity and minimize system errors. Network management functionality typically includes fault, account, configuration, security and performance components.
910	Operations Management Software	**Patch Management Software**	Patch Management Software manages the deployment of patches in an automated fashion.
912	Operations Management Software	**Performance Testing & Analysis Software**	Performance Testing & Analysis Software enables testing network and IT systems for performance, interoperability and compliance with standards and functional specifications; simulating users, traffic, and transactions, and other parameters, in order to determine and

Category ID	Category	Subcategory	Description
			optimize system availability, capacity, security and other parameters.
914	Operations Management Software	Software Asset Management Software	Software Asset Management Software that manages and optimizes the purchase, deployment, maintenance, utilization, and disposal of software applications within an organization.
916	Operations Management Software	Storage Management Software	Storage Management Software provides centralized visibility and control across physical and virtual heterogeneous storage environments to improve storage utilization, optimizes resources, increases data availability, and reduces capital and operational costs.
1000	Client Productivity Software		**Client Productivity Software delivers, enables and supports client-computing productivity. Client Productivity Software provides components, functions, features that enhance client productivity by making information or knowledge accessible, useable and complete.**
1002	Client Productivity Software	Adaptive Computing Technology Software	Adaptive Computing Technology Software delivers, enables and supports Clients in the performance of computing tasks that the client was formerly unable or had great difficulty in attaining or accomplishing respectively. Adaptive Computing Technology Software accessibility functions, enhancements and or changes to the methods of client interoperability or interaction with computing devices thereby making information or technology more accessible, useable and complete from a client perspective.
1004	Client Productivity Software	Calendar & Scheduling Software	Calendaring & Scheduling Software delivers, enables and supports Users by providing an electronic version of a calendar and or allowing Users to schedule time and events through appointment books, address books and or contact lists. Calendar & Scheduling provides individual, group or entity wide calendaring & scheduling functions and features.

Category ID	Category	Subcategory	Description
1006	Client Productivity Software	Desktop Publishing Software	Desktop Publishing Software delivers, enables and supports Users in creating, automating and or publishing client desktop information in hard or soft copy. Desktop Publishing Software provides assemble, edit and publishing functions and features in various input/output formats.
1008	Client Productivity Software	Electronic Mail and Messaging Software	Electronic Mail and Messaging Software delivers, enables and supports Users by providing Electronic Mail and or Messaging. Electronic Mail and Messaging Software allows the client to compose, receive, view, edit, manage and or send electronic mail or messages from one client to others.
1010	Client Productivity Software	Graphic Design, Imaging & Viewing Software	Graphic Design, Imaging & Viewing Software delivers, enables and supports Graphic creation, view, edit and or manipulation of graphic digital imagery. Graphic Design, Imaging & Viewing Software provides functions and features in various input/output formats.
1012	Client Productivity Software	Multimedia Streaming Software	Multimedia Streaming Software delivers, enables and supports Software are licensed software applications that allow Users to transfer multimedia data so that it can be processed as a steady continuous stream. Multimedia Streaming Software allows users to convert the data in real time into playable audio/video as it arrives. The user needs a player, which sends the data as a steady stream to the application that is processing and converting it to sound or pictures.
1014	Client Productivity Software	Office Automation Suite Software	Office Automation Suite Software delivers, enables and supports Software are licensed software applications that bundle common office functionality such as word processing, spreadsheets, presentation graphics, personal information management and Electronic Messaging into an integrated suite of functionality.

Category ID	Category	Subcategory	Description
1016	Client Productivity Software	Personal Information Management Software	Personal Information Management Software delivers, enables and supports Software are licensed software applications that provides personal organization functionality such as task management, calendaring, messaging and organization components. This software also provides contact management functions, scheduling and calendar functions and supports messaging and group communication functions.
1018	Client Productivity Software	Portable Document Software	Portable Document Software delivers, enables and supports Software are licensed software applications that enables Users to create, convert, and/or view portable document format (PDF) files.
1020	Client Productivity Software	Project Management Software	Project Management Software delivers, enables and supports Software are licensed software applications that enable Users to manage plan, organize, display, monitor and control project work and the resources applied to it.
1022	Client Productivity Software	Structured Content Authoring Software	Structured Content Authoring Software delivers, enables and supports Software are licensed Software applications that enable users to open, create, edit, manage and save structured data such as XML.
1024	Client Productivity Software	Training and E-Learning Software	Training and E-Learning Software delivers, enables and supports Software are Licensed Software Applications that enables Users to learn or train on specific subject matter by executing special training modules on a computing device. This type of software can include Computer Based Training (CBT), Web Based Training (WBT) or Video Conferencing Software Based Training Software (VCBT).
1026	Client Productivity Software	Translation Software	Translation Software delivers, enables and supports Software are Licensed Software Applications that enable Users to translate content by providing multilingual and bilingual translation utilities with multiple lexicons, dictionaries and repositories. Translation software can also localize terminologies, maintain translation memory and or reference repositories of word pairs.

Category ID	Category	Subcategory	Description
1100	Scientific & Engineering Software		**Scientific and Engineering Software delivers, enables and supports specialized Scientific and Engineering components, functions and features. Scientific and engineering software provides the scientific or engineering functional resources and services required within a scientific or engineering computing environment.**
1102	Scientific & Engineering Software	**CAD, CAE & CAM Software**	Computer aided design (CAD), engineering (CAE) and manufacturing (CAM) software provides design, engineering, and or manufacturing tools to create, manage and output technical drawings and processes.
1104	Scientific & Engineering Software	**Engineering Analysis Software**	Engineering Analysis Software has the functionality of separating engineering designs into the mechanisms of operation or failure, analyzing or estimating each component of the operation or failure mechanism in isolation, and re-combining the components according to basic physical principles and natural laws.
1106	Scientific & Engineering Software	**Equipment Control Systems Software**	Equipment Control Systems Software manages, commands, directs or regulates the behaviour of other devices or systems.
1108	Scientific & Engineering Software	**Geographic Information Systems (GIS) Software**	Geographic Information System Software captures, stores, analyzes, manages, and presents data that is linked to a location. GIS is the merging of cartography and database technology.
1110	Scientific & Engineering Software	**Geo-spatial Software**	Geo-spatial Software is software that uses analytical methods with terrestrial or geographic data sets.
1112	Scientific & Engineering Software	**Lab & Medical Equipment Software**	Lab and medical equipment software interfaces with lab and/or medical equipment to control and/or receive, interpret, and manipulate data output from the device.
1114	Scientific & Engineering Software	**Mapping and Cartography Software**	Mapping and cartography software offers users the ability to create and work with geographic maps, information or data functions.

Category ID	Category	Subcategory	Description
1116	**Scientific & Engineering Software**	**Mathematical and Computational Software**	Mathematical and computational software is used to model, analyze, or calculate numeric, symbolic, or geometric data.
1118	**Scientific & Engineering Software**	**Statistical Analysis Software**	Statistical analysis software is used for data analysis, manipulation, and the planning of the collection of data, in terms of the design of surveys and experiments.
1200	**Security Operations Software**		**Security Operations Software delivers enables and supports operational components, functions and features required to secure a computer system, network and environment. Security Operations Software provides the security programs, applications, architectures, policies, practices and procedures to securely manage full life cycle requirements of a secure enterprise.**
1202	**Security Operations Software**	Anti-Malware Software	Anti-Malware Software provides protection against threats from spyware, viruses, worms, spam, etc. attacking hosts, networks or applications by detecting and/or preventing infections or malicious behavior, reporting on malicious events and providing remediation tools to remove or quarantine malicious code.
1204	**Security Operations Software**	Application White-Listing Software	Application White-Listing Software permits only authorized applications to run on a system
1206	**Security Operations Software**	Biometric Software	Biometric Software provides the function of uniquely recognizing humans based form of identity for access management, access control, and surveillance. Functions can include face, voice and/or fingerprint recognition. This biometric data and information can be analyzed and processed and then used for computer processing and authentication.
1208	**Security Operations Software**	Business Continuity Software	Business Continuity Software aids in the prevention and recovery from disruptions of computer systems.
1210	**Security Operations Software**	Computer Forensics Software	Computer Forensics Software outlines and explains the current state of a digital artifact.

Category ID	Category	Subcategory	Description
1212	Security Operations Software	Content Classification & Marking Software	Content Classification & Marking Software identifies and marks classified and protected information
1214	Security Operations Software	Data Loss Prevention Software	Data Loss Prevention Software identifies, monitors and protects data in use, data in motion and data at rest through deep content inspection and contextual analysis of transactions.
1216	Security Operations Software	Encryption Software	Encryption Software encrypts and decrypts data, usually in the form of files on (or sectors of) hard drives and removable media, email messages, or network transmissions.
1218	Security Operations Software	Endpoint Security Software	Endpoint Security Software distributes security applications to end-user devices (endpoints) on a network in a centrally managed fashion.
1220	Security Operations Software	Firewall Software	Firewall Software is designed to prevent unauthorized access to or from a private network by permitting or denying computer applications based upon a set of rules and other criteria. Firewalls typically function as filters, gateways, and/or proxies.
1222	Security Operations Software	Identity Management Software	Identity Management Software identifies individuals in a system and controls access to resources in that system by placing restrictions on the established identities.
1224	Security Operations Software	Internet Monitoring, Filtering & Access Control So	Internet Monitoring, Filtering & Access Control Software is used to monitor, filter and control inappropriate use of the Internet.
1226	Security Operations Software	Intrusion Prevention and Detection Software	Intrusion Prevention and Detection Software inspects inbound and outbound network activity and identifies and prevents suspicious patterns that may indicate a network or system attack attempting to break into or compromise a system.
1228	Security Operations Software	Mobility Security Software	Mobility Security Software provides automatic security controls for mobile users that allow enterprises to deploy wireless tools that maintain security rules. In addition, they provide reporting tools to ensure that users are maximizing and controlling wireless costs.

Category ID	Category	Subcategory	Description
1230	Security Operations Software	Security Information Event Management Software	Security Information Event Management Software collects, retains and reports on activity log data from anywhere in the IT infrastructure. It provides the tools to track and correlate events across multiple sources ensuring immediate notification of suspicious activity.
1232	Security Operations Software	Privacy Software	Privacy Software protects the privacy of users. This software typically works in conjunction with Internet usage to control or limit the amount of information made available to third-parties. This software can apply encryption or filtering of various kinds to mask information about a user's identity.
1234	Security Operations Software	Public Key Infrastructure (PKI) Software	Public Key Infrastructure Software creates, manages, distributes, uses, stores, and revokes digital certificates. In cryptography, a PKI is an arrangement that binds public keys with respective user identities by means of a certificate authority (CA).
1236	Security Operations Software	Remote Access Software	Remote Access Software facilitates communication with a device from a remote location through a data link. Typically this is performed using a virtual private network (VPN).
1238	Security Operations Software	Security Risk Management and Policy Compliance Software	Security Risk and Policy Compliance Software is used to manage, monitor, report on, and audit both security risks and policies to address those risks. Solutions often include remediation management, compliance and enforcement, policy assessment, vulnerability management, remediation, and reporting towards the objective of sustainable compliance.
1240	Security Operations Software	Unified Threat Management Software	Unified Threat Management Software is an all-inclusive security product that has the ability to perform multiple security functions in a single application including network fire-walling, network intrusion prevention and gateway anti-virus (AV), gateway anti-spam, VPN, content filtering, load balancing and reporting.

Annex B - SaaS Solutions and Ceiling Prices

Note to Supplier: This form must be completed and submitted as part of the Supplier's response to the RFSA.

PRODUCT LIST AND CEILING PRICES								
Item NO.	**Software Publisher's Part No.**	**SaaS Solution's Name**	**Software Publisher's Name**	**Ceiling Unit Price**	**License Type**	**Software Category**	**Language (s) available**	**SaaS Solution Information**
	(enter the Part Number that the Software Publisher uses to identify the SaaS Solution)	(enter the name that the Software Publisher uses to identify the SaaS Solution.	(enter the name of the Software Publisher that produces the SaaS Solution)	(enter ceiling price per license in Canadian Dollars)	(enter the license type such as "per user", "per entity", etc. **and** subscription, term)	(enter the applicable category per Annex A – SaaS Categories and Descriptions)	(enter the language of the SaaS Solution such as English, and French)	(enter a web site URL containing SaaS Solution information)
1								
2								
3								

Annex C - SaaS Solution Usage Terms and Conditions

Only terms which are presented in full and directly included in Annex C – SaaS Solution Usage Terms and Conditions form part of the Supply Arrangement. Any terms or conditions that are purported to be incorporated by reference through URLs, read me files or otherwise form no part of the Supply Arrangement unless such terms are presented in full and included at Annex C – SaaS Solution Usage Terms and Conditions.

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

Note to Suppliers:
The Supplier must submit Terms and Conditions that apply to the use of its SaaS Solution(s). However, if there are any discrepancies between the Supplier's Terms and Conditions and those in the body of the RFSA and Resulting Contract clauses, the Terms and Conditions of the RFSA shall prevail.

Annex D – SaaS Service Level Agreements (SLA)

Only terms which are presented in full and directly included in Annex D – SaaS Service Level Agreements (SLA) form part of the Supply Arrangement. Any terms or conditions that are purported to be incorporated by reference through URLs, read me files or otherwise form no part of the Supply Arrangement unless such terms are presented in full and included at Annex D – SaaS Service Level Agreements (SLA).

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

Note to Suppliers:
The Supplier must submit Terms and Conditions that apply to the use of its SaaS Solution(s). However, if there are any discrepancies between the Supplier's Terms and Conditions and those in the body of the RFSA and Resulting Contract clauses, the Terms and Conditions of the RFSA shall prevail.

Annex E - SaaS Solution Program Terms and Conditions

The terms of this SaaS Solution Program may replace or modify the terms under Annex C – SaaS Solution Usage Terms and Conditions. In the event of conflict, the terms of Annex D – SaaS Solution Program Terms and Conditions supersede the terms of Annex C – SaaS Solution Usage Terms and Conditions. *However, if there are any discrepancies between the Supplier's SaaS Solution Program Terms and Conditions and those in the body of the RFSA and Resulting Contract clauses, the Terms and Conditions of the RFSA shall prevail.*

Only terms which are presented in full and directly included in Annex D – SaaS Solution Program Terms and Conditions form part of the Supply Arrangement. Any terms or conditions that are purported to be incorporated by reference through URLs, read me files or otherwise form no part of the Supply Arrangement unless such terms are presented in full and included at Annex D – SaaS Solution Program Terms and Conditions.

Note to Suppliers:
The Supplier may submit the SaaS Solution Program Terms and Conditions that apply to the Crown as a major client of a Software Publisher's SaaS Solutions. For the purpose of programs, the Crown must be treated as a single entity. Department specific programs are not permitted. Examples of programs include enterprise programs, volume based programs, and business level agreements.

Annex F – Security Requirements

1. Note to Suppliers: The wording provided does not represent the entirety of Canada's security requirements and are included in this section in order to provide Respondents advance notice of potential requirements. Canada will determine the substance and content that reflects Canada's security requirements. Any Respondents who do not currently possess any of the anticipated security clearances are encouraged to initiate the relevant security process.

2. Security Requirements:

(a) There will be security requirements for the RFSA. Preliminary security requirements for the RFSA and resulting contracts are outlined below to assist Respondents in preparing for the RFSA security requirements.

(b) As there will be security requirements for the RFSA and resulting contracts, Canadian Respondents that do not currently have personnel and organization security clearances through the Canadian federal government, or Respondents that do not meet the anticipated security requirements outlined below, should begin the clearance process early by contacting the Industrial Security Program (ISP) of Public Service Procurement Canada (PSPC) (https://www.tpsgc-pwgsc.gc.ca/esc-src/index-eng.html) website.

3. Communications Security Establishment (CSE) Cloud Service Provider Information Technology Security (CSP ITS) Assessment

Canada is considering making it a requirement of the RFSA that all CSP's being named within a proposed Supply Arrangement have completed the CSP ITS Assessment prior to the completion of any transactions against that Supply Arrangement for requirements related to Protected Data. The CSP ITS Assessment Process, includes all measures that may be used to assess the Respondents and their solutions for security vulnerabilities during the solicitation process and continued obligations imposed during the resulting contract period.

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

For 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.

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 _____;

(ii) Industrial Security Manual (Latest Edition)

For Foreign Suppliers:

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 SaaS Solutions, 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, clause (7).

(d) The foreign recipient Bidders must provide assurance that it can receive and store **CANADA PROTECTED B** 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** 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** 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 compute**r** system any **CANADA PROTECTED B** 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 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 supplier 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.

PART 7 RESULTING CONTRACT CLAUSES

7.5 a) <u>Security Requirements for Canadian Suppliers:</u>

1. The Contractor/Offeror must, at all times during the performance of the Contract/Standing Offer, hold a valid Designated Organization Screening (DOS) with approved Document Safeguarding at the level of PROTECTED B, issued by the Canadian Industrial Security Directorate (CISD), **Public Works and Government Services Canada (PWGSC**).
2. The Contractor/Offeror personnel requiring access to PROTECTED information, assets or work site(s) must EACH hold a valid RELIABILITY STATUS, granted or approved by the CISD/PWGSC.
3. 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.
4. Subcontracts which contain security requirements are NOT to be awarded without the prior written permission of CISD/PWGSC.
5. The Contractor/Offeror must comply with the provisions of the:
6. Security Requirements Check List and security guide (if applicable), attached at Annex _____;
7. Industrial Security Manual (Latest Edition)

(b) <u>Security Requirements for Foreign Suppliers:</u>

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 Work described in the SaaS Solutions, in addition to the Privacy and Security Requirements. These security requirements are in addition to those requirements identified below in Section 7.5.1 - Protection and Security of Data Stored in Databases.

1. The Foreign recipient **Contractor / Subcontractor** must be from a Country within the North Atlantic Treaty Organization (NATO), the European Union (EU) or from a country with which Canada has an international bilateral security instrument. The Contract Security Program (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.
2. The Foreign recipient **Contractor / Subcontractor** must provide proof that they are incorporated or authorized to do business in their jurisdiction.
3. The Foreign recipient **Contractor / Subcontractor** must provide assurance that it can receive and store **CANADA PROTECTED** information/assets on its site or premises as indicated in Part 7 and as listed in the IT Security Requirements.
4. The Foreign recipient **Contractor's / Subcontractor's** location of work performance must meet the security requirements as listed in the IT Security Requirements.
5. 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.
6. The Foreign recipient **Contractor / Subcontractor** must provide the **CANADA PROTECTED** information/ assets a degree of safeguarding no less stringent than that provided by the Government of Canada in accordance with the National Policies, National Security legislation and regulations and as prescribed by the Canadian DSA.
7. 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).
8. The Foreign recipient **Contractor / Subcontractor** must identify an authorized Contract Security Officer (CSO) and an Alternate Contract Security Officer (ACSO) (if applicable) to be responsible for the overseeing of the security requirements, as defined in this contract. This individual will be appointed by the proponent foreign recipient **Contractor'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.
9. The Foreign recipient **Contractor / Subcontractor** must not grant access to **CANADA PROTECTED B** information, except to its personnel subject to the following conditions:

   a. Personnel have a need-to-know for the performance of the **contract / subcontract**;

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

c. 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

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

10. 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**, furnished to the foreign recipient **Contractor / Subcontractor** or produced by the foreign recipient **Contractor / Subcontractor**, must also be safeguarded as follows:

11. 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.

12. All Personal Information, provided to the foreign recipient **Contractor / Subcontractor** or produced by the Foreign recipient **Contractor / Subcontractor**, must:

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

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

13. The foreign recipient **Contractor / Subcontractor** must not use the Personal Information for any purpose other than for the performance of the **contract / subcontract** without the prior written approval of Canada. This approval must be obtained from the Canadian Designated Security Authority (DSA).

14. The Foreign recipient **Contractor / Subcontractor** must immediately report to its respective national DPA and the Contracting Authority (in collaboration with the Canadian DSA), all cases in which it is known or there is reason to suspect that any Personal Information provided or generated pursuant to this **contract / subcontract** have been lost, or in contravention of these security requirements, accessed, used or disclosed to unauthorized persons.

15. The Foreign recipient **Contractor / Subcontractor** must ensure that all the databases including the backup database used by organizations to provide the services described in the proposed SaaS Solutions, containing any **CANADA PROTECTED** Information, related to the Work, are located within Canada.

16. 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** information/assets until authorization to do so has been confirmed by the Canadian DSA.

See 7.5.2 for security measures required for the treatment and access to Personal Information.

17. Subcontracts which contain security requirements are NOT to be awarded without the prior written permission of the Canadian DSA.
18. The foreign recipient **Contractor / Subcontractors** must ensure that the appropriate security clauses, as determined by the Canadian DSA, are inserted in all subcontracts that involve access to Personal Information provided to or generated under this Contract and/or 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.
19. The Foreign recipient **Contractor / Subcontractor** requiring access to Canadian Government site(s), under this contract, must submit a Request for Site Access to the Departmental Security Officer of **(Name of Government of Canada Department).**
20. 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.
21. Upon completion of the Work, the foreign recipient **Contractor / Subcontractor** must return to the Government of Canada, all Personal Information furnished or produced pursuant to this **contract / subcontract**, including all Personal Information released to and/or produced by its subcontractors.
22. The Foreign recipient **Contractor / Subcontractor** must comply with the provisions of the Security Requirements Check List attached at Annex _____.

7.5.1 Protection and Security of Data Stored in Databases

1. The foreign recipient **Contractor / Subcontractor** must ensure that all the databases used by organizations to provide the services described in the proposed SaaS Solutions containing any Personal Information, related to the Work, are located in Canada.
2. 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).
3. 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.
4. 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.
5. 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.

6. 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.

7.5.2 Personal Information

Interpretation

1. 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;

2. 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.

3. If there is any inconsistency between the General Conditions and these supplemental general conditions, the applicable provisions of these supplemental general conditions prevail.

Ownership of Personal Information and Records

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.

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**.

Collection of Personal Information

1. 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:

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

   b. the ways the Personal Information will be used;

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

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

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

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

2. 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.

3. 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.

4. 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.

Maintaining the Accuracy, Privacy and Integrity of Personal Information

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

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

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

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

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

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

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

g. include a notation on any Record(s) that an individual has requested be corrected if the foreign recipient **Contractor / Subcontractor** has decided not to make the correction for any reason. Whenever this occurs, the foreign recipient **Contractor / Subcontractor** must immediately advise the Contracting Authority of the details of the requested correction and the reasons for the foreign recipient **Contractor's/Subcontractor's** decision not to make it. If directed by the Contracting Authority to make the correction, the Contractor must do so;

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

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

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

Safeguarding Personal Information

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

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

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

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

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

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

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

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

a. 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**.

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:

a. 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**);

b. 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);

c. 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

d. 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 C**ontractor / Subcontractor**.

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:

a. 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;

b. a list of the types of Personal Information used by the foreign recipient **Contractor / Subcontractor** in connection with the Work;

c. a list of all locations where hard copies of Personal Information are stored;

d. 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;

e. a list of every person to whom the foreign recipient **Contractor / Subcontractor** has granted access to the Personal Information or the Records;

f. a list of all measures being taken by the foreign recipient **Contractor / Subcontractor** to protect the Personal Information and the Records;

g. 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

h. an explanation of any new measures the foreign recipient **Contractor / Subcontractor** intends to implement to safeguard the Personal Information and the Records.

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.

Statutory Obligations

1. 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.
2. 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.

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.

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.

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.

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.

b. Bid Submission Requirements

a) The Bidder should clearly demonstrate its data residency compliance and provide a data center deployment plan(s) which should include specifics on:

i. location(s) (country and city) of primary data center(s);
ii. location(s) (country and city) of secondary data center(s) and backup centers;
iii. location(s) (country and city) of all the infrastructure components (including, but not limited to, database servers, SANS, application servers); and
iv. location(s) (country and city) of the SOC, NOC and the Service Desk.

The Bidder should clearly demonstrate its business entities and personnel location compliance and provide:

i. location(s) (country and city) of all business entities performing Work under the Contract; and

ii. location(s) of all personnel performing the Work under the Contract.

b) The bidder should implement safeguards to ensure that all publicly accessible government websites and web services are configured to provide service only through a secure connection, in accordance with Section 6.2.4 of the Policy on the Management of Information Technology and the Policy on Government Security.

Bidder will implement a secure web connection that:

- is configured for HTTPS
- has HSTS enabled
- implements TLS 1.2, or subsequent versions, and uses supported cryptographic algorithms and certificates, as outlined in CSE's
  - ITSP.40.062 Guidance on Securely Configuring Network Protocols, Section 3.1 for AES cipher suites
  - ITSP.40.111 Cryptographic Algorithms for Unclassified, Protected A, and Protected B Information
- disables known-weak protocols such as all versions of Secure Sockets Layer (SSL) (e.g. SSLv2 and SSLv3) and older versions of TLS (e.g. TLS 1.0 and TLS 1.1), as per CSE ITSP.40.062
- disables known-weak ciphers (e.g. RC4 and 3DES)

c) The Bidder should demonstrate its ability to comply with the IT security requirements by maintaining policies and procedures that support IT security throughout the Contract by providing evidence of any existing policies and procedures that support the security control families described in Annex 2 and ITSG-33.

The Bidder should describe how its policies and procedures align to the security control families by providing the following information on current policies and procedures:

i) name of policy and/or procedure
ii) its purpose
iii) its scope
iv) the roles and responsibilities that are described within the policy and/or procedure
v) how it ensures coordination among organizational entities
vi) how it ensures compliance within the organization

d) The Bidder should provide an IT security topology diagram which should include the following components:

i. interfaces - separate bullet for each category
ii. web
iii. applications
iv. databases
v. security devices
vi. system management
vii. backup infrastructure

The Bidder should provide one or more of the following, which define information systems components and functions to be separated by boundary protection devices:

1. Information system design documentation;
2. Information system architecture

e) The Bidder should describe the experience of the security organization that will be responsible in ensuring the security of the solution, including the name of each person, their role & description of their duties, their experience, and certifications.

f) The Bidder should provide its proposed approach to data segregation, that should include:

i. information system design documentation;
ii. information system architecture; and

iii. process and procedures to support data segregation .

g) The Bidder should provide its proposed approach to the disposal and sanitization of Canada's data, including:

i. a plan for hard-drive sanitation or an action plan if the system is hosted in a virtual environment that will ensure Canada's data is not obtainable;
ii. a plan for data disposal;
iii. system disposal processes and procedures;
iv. a plan for destruction of duplicate records that may be stored in a records management system or backups; and
v. the process it plans to follow when the system is no longer required and is being decommissioned.

vi. Review and update cycles to support continuous improvement and maturing measurement capabilities.

h) The Bidder should provide its proposed approach to continuous monitoring of and include the following components:

1. The strategy for continuous monitoring
2. Established measures, metrics, and status monitoring and control assessments frequencies;
3. Details of data collection and its reporting aspects;
4. Analysis methods of the data gathered and Report findings accompanied by recommendations;
5. Response mechanisms to assessment findings to include making decisions to either mitigate technical, management and operational vulnerabilities; or accept the risk; or transfer it to another authority; and
6. Review and update cycles to support continuous improvement and maturing measurement capabilities.

i) The Bidder should provide proof of its security certification(s) and applicable audit standards for its proposed solution in the form of a copy of a valid certificate or audit standard and describe how the certification or audit standard was assessed and obtained (e.g.: 3rd party, self-assessment) for each IT Security certification and audit standard held, such as:

i) FedRAMP;
ii) Cloud Security Alliance – STAR;
iii) COBIT;
iv) ISO 27001;
v) PCI DSS;
vi) CMM; and
vii) others.

The Bidder should also stipulate if the certification or audit standard applies to the whole solution or to a specified portion of their solution.

j) The Bidder should provide details on its proposed solution's Identity, Credential and Access Management level of assurance capabilities with respect to TBS Standard on Identity and Credential Assurance. The Bidder should identify the level of assurance and demonstrate how it meets the requirements of that level.

FORMS

FORM 1 - ARRANGEMENT SUBMISSION FORM		
Supplier's full legal name		
Authorized Representative of Supplier for evaluation purposes (e.g., clarifications)	Name	
	Title	
	Address	
	Telephone #	
	Fax #	
	Email	
Supplier's Procurement Business Number (PBN) [*See the Standard Instructions 2008*]		
List of the Board of Directors Member *[Suppliers are requested to indicate the name(s) of all of the Board of Director member(s) in its Company.]*	Name: Name: Name: ...	
Jurisdiction of Contract Province in Canada the Supplier wishes to be the legal jurisdiction applicable to the Supply Arrangement and to any resulting Contracts (if other than the province of Ontario (Canada).		
Number of FTEs *[Suppliers are requested to indicate, the total number of full-time-equivalent positions that would be created and maintained by the Supplier as a result of its participation within this procurement vehicle. This information is for information purposes only and will not be evaluated.]*		
Security Clearance Level of Supplier *[Suppliers are requested to include both the level and the date it was granted.]*		
Aboriginal Businesses *[Suppliers are requested to indicated if they meet the requirements as outlined in Set-Asides Program for Aboriginal Businesses (SPAB).]*		
Canadian Small and Medium Enterprises (CSME) *[Suppliers are requested to indicated if they meet the definition of a Canadian Small and Medium Enterprise (OSME indication: 100 to 500 Employees = Medium; 10 to 100 = Small; 1 to 10 = Micro).]*		
Canadian Enterprise *[Suppliers are requested to indicated if they are Canadian Suppliers.]*		
Green Procurement *[Suppliers must commit to providing delivery of all goods in an environmentally friendly manner.]*		
Green Company *[Suppliers are requested to identify if their facilities operate with an Environmental Management System (EMS) certified by a qualified registrar as complying with the ISO 14001 standard.]*		

Supplier Certification that all SaaS Solutions are "Off-the-Shelf" [Suppliers are requested to certify that all proposed SaaS Solutions in response to this RFSA are "Off-the-Shelf", meaning that each software component is commercially available and requires no further research or development and is part of an existing product line with a field-proven operational history (that is, it has not simply been tested in a laboratory or experimental environment). If any of the SaaS Solution proposed is a fully compatible extension of a field-proven product line, it must have been publicly announced on or before the date that the Arrangement is submitted. By submitting an Arrangement, the Supplier is certifying that all the SaaS Solutions proposed are Off-the-shelf.]	
On behalf of the Supplier, by signing below, I confirm that I have read the entire Request for Supply Arrangement including the documents incorporated by reference and I certify that: 1. The Supplier considers itself and its products able to meet all the mandatory requirements described in the RFSA; 2. All the information provided in response to the RFSA is complete, true and accurate; and 3. If the Supplier enters into an Arrangement with Canada and if it is awarded Contracts, it will accept all the terms and conditions set out in the resulting Contract clauses included in the RFSA.	
Signature of Authorized Representative of Supplier	

Form 2

Software Publisher Certification Form

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

The Supplier certifies that it is the Software Publisher of all the following SaaS Solutions and that it has all the rights necessary to license them in accordance with the terms and conditions of the SA to Canada:

_____

_____

_____

_____

_____

[Suppliers should add or remove lines as needed, or attach the product list as an appendix.]

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 _____

Email for authorized signatory of SP _____

Date signed _____

RFSA Number _____

Form 3

Software Publisher Authorization Form

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

This confirms that the Software Publisher identified below understands and acknowledges that the Supplier named below has submitted an Arrangement in response to the Request for Supply Arrangement dated _____, reference number _____ issued by PWGSC.

The Software Publisher hereby confirms that

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

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

[*Identify all of the Licensing Entities' proprietary SaaS Solutions that are proposed by the reseller*.]

_____
_____
_____
_____

[*Suppliers should add or remove lines as needed,* or attach the product list as an appendix.]

Name of Supplier _____

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 _____

Email for authorized signatory of SP _____

Date signed _____

RFSA Number _____

Form 4

Open Source Software Certification Form

The Supplier certifies that all the following software products are non-proprietary software (Open Source Software) and that the licenses therefrom allow for the redistribution of the software under the terms and conditions of the resulting Contract under the Supply Arrangement.

_____

_____

_____

_____

_____

_____

_____

[Suppliers should add or remove lines as needed, or attach the product list as an appendix]

Name of Supplier _____

Signature of authorized signatory of Supplier _____

Print Name of authorized signatory of Supplier _____

Print Title of authorized signatory of Supplier _____

Address for authorized signatory of Supplier _____

Email for authorized signatory of Supplier _____

Date signed _____

RFSA Number _____

Form 5

Certification Requirements for the Set-Aside Program for Aboriginal Business

The Supplier:
(i) certifies that it meets, and will continue to meet throughout the duration of the Arrangement, the requirements described in Annex 9.4 Requirements for the Set-aside Program for Aboriginal Business, of the Supply Manual (https://buyandsell.gc.ca).
(ii) agrees that any subcontractor it engages under the Arrangement must satisfy the requirements described in the above-mentioned annex.
(iii) agrees to provide to Canada, immediately upon request, evidence supporting any subcontractor's compliance with the requirements described in the above-mentioned annex.

The Supplier must check the applicable box below:
( ) The Supplier is an Aboriginal business that is a sole proprietorship, band, limited company, co-operative, partnership or not-for-profit organization.
OR
( ) The Supplier is either a joint venture consisting of two or more Aboriginal businesses or a joint venture between an Aboriginal business and a non-Aboriginal business.*

The Supplier must check the applicable box below:
( ) The Aboriginal business has fewer than six full-time employees.
OR
( ) The Aboriginal business has six or more full-time employees.

The Supplier must, upon request by Canada, provide all information and evidence supporting this certification. The Supplier must ensure that this evidence will be available for audit during normal business hours by a representative of Canada, who may make copies and take extracts from the evidence. The Supplier must provide all reasonably required facilities for any audits.

By submitting an Arrangement, the Supplier certifies that the information submitted by the Supplier in response to the above requirements is accurate and complete.

Name of Supplier _____

Signature of authorized signatory of Supplier _____

Print Name of authorized signatory of Supplier _____

Print Title of authorized signatory of Supplier _____

Address for authorized signatory of Supplier _____

Email for authorized signatory of Supplier _____

Date signed _____

RFSA Number _____

*** Aboriginal Joint Venture**: a joint venture consisting of two or more Aboriginal businesses or Aboriginal business(es) and a non-Aboriginal business(es), provided that the Aboriginal business(es) has at least 51 percent ownership and control of the joint venture. The joint venture has to respect the Aboriginal content requirement of 33% of the value of the work under a Contract has to be performed by the Aboriginal business(es).

Form 6

Submission Completeness Review Checklist

SUPPLIER'S NAME:

1) Technical Arrangement, Financial Arrangement and Certifications:

- *a)* ☐ Technical Arrangement
- *b)* ☐ Financial Arrangement
- *c)* ☐ Certifications

FORMS:

1) Arrangement Submission Form (RFSA Form 1)

- *a)* ☐ Supplier's full legal name
- *b)* ☐ Authorized Representative of Supplier for the evaluation purposes
- *c)* ☐ Supplier's Procurement Business Number (PBN)
- *d)* ☐ List of the Board of Directors Member
- *e)* ☐ Jurisdiction of Contract
- *f)* ☐ Number of FTEs
- *g)* ☐ Security Clearance Level of Supplier
- *h)* ☐ Aboriginal Businesses
- *i)* ☐ Canadian Small and Medium Enterprises (CSME)
- *j)* ☐ Canadian Enterprise
- *k)* ☐ Green Procurement
- *l)* ☐ Green Company
- *m)* ☐ Supplier Certification that all SaaS Solutions are "Off-the-Shelf"
- *n)* ☐ Signature of Authorized Representative of Supplier

2) Software Publisher Certification Form *(Mandatory when the Supplier itself is the Software Publisher) (RFSA Form 2)* ☐

3) Software Publisher Authorization Form *(Mandatory when the Supplier is not the Software Publisher) (RFSA Form 3)* ☐

4) Open Source Product(s) Certification Form *(Mandatory when the Supplier is offering open source software in its Annex B) (RFSA Form 4)* ☐

5) Certification Requirements for the Set-Aside Program for Aboriginal Business *(Mandatory when the Supplier is an aboriginal business and wants to be identified as such) (RFSA Form 5)* ☐

ANNEXES:

1) SaaS Solutions and Ceiling Prices (RFSA Annex B)

- *a)* ☐ Must be submitted using the format outlined in Annex B
- *b)* ☐ Item No. included for each product.
- *c)* ☐ Software Publisher's Part No. *(the part number the Software Publisher uses to identify the SaaS Solution commercially)*
- *d)* ☐ Software Publisher's Product Name *(the commercial product name that the Software Publisher uses to identify the SaaS Solution.*

e) ☐ Software Publisher's Name *(the name of the Software Publisher that produces the SaaS Solution)*

f) ☐ *Cloud Service Provider (CSP): Supplier must identify the existing Cloud Service Provider (CSP), who's Commercially Available Cloud Services will be used to supply to Canada the proposed Software as a Service (SaaS).*

g) ☐ Ceiling Unit Price *(required for every line item)*

h) ☐ License Type *(the license type under which the SaaS Solution will be offered to Canada; such as "per user", "per entity " and whether the is per subscription term is monthly or annual, etc.)*

i) ☐ SaaS Category *(the applicable software category of the product corresponding with the category descriptions under Annex G - Software Categories & Descriptions)*

j) ☐ Language(s) available *(the language(s) under which the SaaS Solution is available such as English, French and/or other)*

k) ☐ SaaS Solution Information *(a web site URL containing SaaS Solution information)*

2) SaaS Solution Usage Terms and Conditions (RFSA Annex C)

Required usage terms and conditions:

a) ☐ License type (e.g.Per User, per Entity, etc.); PAGE # _____
(Include definitions of the license types identified in Annex B)

b) ☐ Subscription Term (e.g. Monthly, Annual, etc.); PAGE # _____
(Include definitions of the license model identified in Annex B)

c) ☐ Metric (how the usage is measured); PAGE # _____

d) ☐ Rights to use; PAGE # _____

e) ☐ Limitations of use; PAGE # _____

f) ☐ Warranty. PAGE # _____

Service Level Agreement (SLA):

a) ☐ Hours of support; PAGE # _____

b) ☐ Contact and procedure information for accessing Support; PAGE # _____

c) ☐ Procedures for resolution of problems; PAGE # _____

d) ☐ Response times; PAGE # _____

e) ☐ Procedures on how and when all telephone, fax or email communications will be responded to; PAGE # _____

f) ☐ Support web site availability to Canada's users (ex: 24 hours a day, 365 days a year, and 99% of the time). PAGE # _____

3) Program Terms and Conditions (Annex D)

a) ☐ SaaS Solution Programs include enterprise programs, volume based programs, and business level agreements etc. that apply to Canada (as a single Entity) as a major Customer of a Software Publisher's SaaS Solutions. *(I.E. Additional grants, rights, or entitlements, Volume discount programs)*

Name of Authorised Signatory of Supplier: _____

Signature of Authorised Signatory of Supplier: _____