PUBLIC SERVICE AND PROCUREMENT CANADA (PSPC)

Amendment no. 015 to Request for Supply Arrangement (RFSA) for

SaaS Method of Supply (GC CLOUD)

Buy&Sell Solicitation Reference Number: EN578-191593/F

THIS AMENDMENT 015 IS RAISED TO:	
1.0	Notify the industry of the second round of Submissions to be evaluated by the Canadian Centre for Cyber Security (CCCS) and give specifications on how to apply, as detailed in Section 1.0, below;
2.0	Respond to questions received regarding the RFSA, as detailed in Section 2.0, below;
3.0	Share the questions that were raised during the SaaS RFSA Industry Day on January 11, 2021, along with the associated responses, as detailed in Section 3.0 below;
4.0	Amend Annex A – Qualification Requirements, to modify Tier 1 M5 and M7, and Tier 2 M8 and M11, as detailed in Section 4.0, below;
5.0	Replace Annex C – SaaS Solutions and Professional Services Ceiling Prices in its entirety with an updated version, as detailed in Section 5.0, below;
6.0	Replace Part 6 – Supply Arrangement in its entirety with an updated version, as detailed in Section 6.0, below;
7.0	Amend Part 7 – Contractor Selection and Resulting Contract Clauses, to modify Section 7.2 Contractor Selection and Section 7.3 Bid Solicitation Process, as detailed in Section 7.0, below;
8.0	Replace Annex F – SaaS Resulting Contract Clauses in its entirety with an updated version, as detailed in Section 8.0, below;
9.0	Replace Annex H – Security Requirements for Foreign Suppliers in its entirety with an updated version, as detailed in Section 9.0, below; and,
10.0	Provide the industry with a copy of the Protected SaaS RFSA Industry Day presentation.

1.0 Information regarding the second round of submissions that will be assessed by CCCS during Wave 2 onboarding:

QUESTIONS	ANSWERS
Q.65 When will the second round of Submissions be evaluated by the Canadian Centre for Cyber Security (CCCS)?	**A.65** The second round opened at 9 a.m. on January 18, 2021 and Submissions will be accepted by the CCCS Client Centre at contact@cyber.gc.ca in order to onboard Suppliers into the CCCS IT Security (ITS) Assessment Program. At 2 p.m. on February 12, 2021 the second intake window will close. Suppliers will be notified of the time and date of opening and closing of the third round of onboarding via Buy & Sell.
Q.66 How do we make a Submission to the CCCS SaaS IT Security Assessment Program?	**A.66** As per A.52 posted under the Amendment 011, the process is as follows: To make a submission to the CCCS SaaS IT Security Assessment Program, a Bidder must complete the following steps: 1) Request the necessary public key for the CCCS Pretty Good Privacy (PGP) key and form to start the onboarding process by contacting the CCCS Contact Centre: contact@cyber.gc.ca or 613-949-7048 or 1-833-CYBER-88. The CCCS Client Services team will reply with the form and instructions as needed; 2) Prepare to enter into a bi lateral non-disclosure agreement (NDA) with the CCCS; 3) Suppliers who meet the requirements under Annex A – Qualifications Requirements for Tier 1 (Protected A) or Tier 2 (Protected B) of the RFSA will provide all documentation for the assessment to the CCCS Contact Centre. When providing documents, PGP encryption program credentials should be used to encrypt the documents. If Suppliers use an alternate encryption method (i.e. a password) CCCS can also collect documents at that time. For additional information on the onboarding process, Suppliers should refer to the Annex L – SaaS IT Security (ITS) Assessment Program: Onboarding Process under the Amendment 007 of the RFSA or/and contact contact@cyber.gc.ca; and 4) The RFSA is intended to be a collaborative qualification process. Should the Submission not

QUESTIONS	ANSWERS
	be complete the CCCS Contact Centre will contact the Supplier and request clarifications and/or missing documents, if required.

2.0 Respond to questions regarding the RFSA:

Note: Questions may have been modified and/or condensed.

QUESTIONS	ANSWERS
Q.67 What level of Security Clearances are required to be awarded a Supply Arrangement (SA) under this RFSA?	**A.67** Suppliers must hold the following clearances to be awarded an SA: DSC – Protected B DOS – Protected B Contractor personnel with privileged access rights will also be required to hold a valid SECRET security clearance with the Canadian Industrial Security Directorate. Foreign Suppliers are required to hold security clearance at a level of Secret, and are encouraged to reach out to the Supply Arrangement Authority in order to request additional information regarding security requirements for Foreign Suppliers. For more information about international contract security requirements, you can also visit: https://www.tpsgc-pwgsc.gc.ca/esc-src/international-eng.html
Q.68 Under Stream 3: Value-Added Reseller (VAR) submission, we understand that the Annex A to be submitted by the VAR only has to refer to the controls from the SaaS publisher submission, in this case, SaaS publisher's Annex A Schedule 1. Is this understanding correct? In addition to the reference to SaaS Publisher responses references, Is there any VAR specific information/documents which needs to be submitted as a part of Annex A response?	**A.68** The Canadian Centre for Cyber Security (CCCS) in collaboration with the Canadian Industrial Security Directorate requires that Resellers holding SAs will also require the industrial security clearances outlined in the RFSA from Canadian Industrial Security Directorate (CISD)/International Industrial Security Directorate (IISD) (DOS/DSC and personnel clearances at the appropriate level.)
Q.69 Under Stream 3: VAR submission, we understand that the Annex B to be submitted by the VAR only has to refer the controls from the SaaS publisher submission, in this case, SaaS publisher's Annex B1. Is that understanding correct? In addition to the references to SaaS Publisher responses reference, Is there any VAR specific information/documents which needs to be submitted as a part of Annex B response?	**A.69** Correct, nothing is required to respond to Annex B. These are the ongoing security & privacy obligations.
Q.70 We understand that the only documents specific for including VAR information are Form 1 (signed by the VAR) & Form 3 (signed by SaaS Publisher). Is this understanding correct?	**A.70** Form 5 – Submission Completeness Review Checklist is also required to be provided.
Q.71 Can the VAR make a single submission with multiple SaaS publishers? If yes, will we need one FORM 1 for the VAR and Form 3, Annexes A, B and D for each SaaS publisher?	**A.71** The VAR would be required to make a separate submission for each specific SaaS publisher in this scenario.
Q.72 In the event that the VAR would want to add additional SaaS publishers in future, please confirm that we only need to provide Form 3, Annexes A, B and D for each SaaS publisher?	**A.72** If a VAR would like to add additional SaaS publishers, they would need to complete a new submission for each SaaS publisher.
Q.73 Regarding the Amendment No 12, Section 4.0 Modification of Annex F to the Limitation of Liability- it appears the proposed limitation of liability is different	**A.73** The Limitation of Liability outlined in AMD 012 has been created in consultation with industry, and has been approved for use in GC cloud procurement

QUESTIONS	ANSWERS
from, and expands a vendor's liability in some areas, from the Information Management/Information Technology (IM/IT) Limitation of Liability. Would the PSPC be amenable to replacing this limitation of liability with the IM/IT limitation of liability, N0000C.	contracts. Canada is not willing to consider revisions to the Public Cloud Limitation of Liability at this time.
Q.74 For 6.3, 'Standard Clauses and Conditions', PSPC notes that the resulting SACC clauses (different from General Conditions 2020) are as set forth in the SACC Manual. Will the individual agency or PSPC, when issuing solicitations or Task Authorizations under the SaaS Supply Arrangements, cite the specific SACC general terms (if different from 2020) or supplemental terms which apply for that solicitation? Otherwise a vendor can interpret this provision to mean that all SACC provisions which 'may apply' to a solicitation, will apply, which may create an ambiguous or conflicting result.	**A.74** Section 6.3 of Part 6 of the RFSA provides the link to where SACC clauses can be found. Section 6.3.1 identifies the SACC manual clauses and conditions that apply to the RFSA.
Q.75 Citing Form 3, 'SaaS Publisher Authorization Form', sub point (ii), third party SaaS providers offer access to their platforms exclusively subject to their terms and their specific subscription model. They will not agree to any new or different terms which conflict with, change, or are different from the terms they offer as a 'one-to-many' offering to any end customer. Most large, well known SaaS providers require the end user to agree to and sign a license or subscription agreement directly with that provider to gain access and use to its platform. Does PSPC recognize and agree to clarify in this agreement that a) it agrees it may be subject to such terms if the platform is 're-sold' to it by a vendor and b) those third party SaaS provider's terms would prevail over any inconsistent or conflicting terms in this RFSA and specifically the terms relevant to the 'Solution' in Annex F the Resulting Contract provisions?	**A.75** No, PSPC does not agree to be subject to end user license agreements or third party terms and conditions. As per section 3.2(c)(v) of the RFSA, "Only terms and conditions in the SLA related to service levels and service delivery will apply. Any terms and conditions of the SLA not related to service levels and service delivery, as detailed below, will be deemed stricken and will not apply." Section 3.2(c)(v) also specifies that: "Suppliers must submit their published service level agreements (SLA), to be included in Annex D – SaaS Solution Service Level Agreements (SLA). Similarly, any terms contained in Annex D – SaaS Solution Service Level Agreements which include pricing information, such as (but not limited to) those that attempt to impose financial conditions, pricing terms, or compliance penalties, shall be deemed stricken and are of no force or effect.
Q.76 For Annex F Section 8, 'Task Authorization', page 14, if a Supplier is awarded a Supply Arrangement under this RFSA, would the Supplier be compelled to respond to each Task Authorization or solicitation issued by an eligible department? Or, can a Supplier elect not to respond to a Task Authorization or solicitation under this RFSA without consequence or sanction?	**A.76** Supply Arrangement holders are not obligated to respond to every bid solicitation issued against the RFSA, nor are they required to accept all contracts or tasks requested by an authorized client department against a Supply Arrangement. A Supplier can elect not to respond to a Task Authorization or bid solicitation under this RFSA without consequence.
Q.77 Generally- would the SaaS Professional Services require a vendor also to engage in Cyber security services scope for the purchasing department's environments, including, but not limited to, managed security services, cyber defense services (such as penetration testing, vulnerability assessment services, threat hunting and incident response services), or any monitoring, scanning, testing assessments or remediation for security vulnerabilities in specifically Canada's environments? If the answer is yes, would Canada or its procuring agencies be amenable to incorporate into a Task Authorization additional terms which set forth parameters around the nature and respective duties associated with this sensitive scope?	**A.77** This is outside of the scope of the professional services included in the RFSA, which are limited to: (a) Quick Start Guide ("QSG") training and services package; (b) implementation services; (c) training services; (d) data cleansing, migration and transition services; and (e) advisory services. It is important to also note that each individual TA issued against a Contract resulting from the RFSA will define the scope of work for that TA and any security requirements that would apply to the resources/Contractor who is performing the Work. The parameters for the Work (including security requirements) will be defined in the individual Contracts or TAs issued against the Supply Arrangement.
Q.78 Generally- In light of the COVID-19 outbreak, the vendor has had to adjust its infrastructure to provide for its personnel to work from their homes until such time as government jurisdictions lift prohibitions or limitations to in-person working arrangements and	**A.78** This can be addressed in the individual TAs issued against the Contracts resulting from a SaaS Supply Arrangement.

QUESTIONS	ANSWERS
safety conditions improve. To this end, would Canada be amenable to including a provision either in the RFSA or allow inclusion at the SOW or Task Authorization level a requirement that the parties will work together to address impacts to the Services in light of the recently declared Pandemic COVID-19? And, would the vendor be able to negotiate into a Task Authorization with the procuring agency a set of protocols designed to address those requirements which would follow or govern vendors' personnel in providing Services from their home residence?	Due to the Covid pandemic, most of the TAs that PSPC is currently issuing specify that work will be completed at the location of the Contractor's choosing; however, in some circumstances this will not be possible due to security restrictions. This can be discussed with the procuring department prior to the Contract or the TA being issued.
Q.79 When SaaS services are provided on a subscription basis (annual commitments, pre-paid), how is this obligation reconciled with the "Contract Period", or lack of a specific contract period? Is there an expectation that subscriptions can be terminated early, and/or reduced in volume?	**A.79** There are two options available in the Resulting Contract Clauses – which option is used will depend on how the SaaS is sold OR the requirements detailed in the bid solicitation. 1. The first option is a fixed Contract period, where Canada "opts out" or does not agree to an auto renewal but rather subscribes to the SaaS for a fixed period. 2. The second option is a subscription service without a defined Contract period, where Canada does allow for auto renewal but requires a notification prior to auto renewal, and also requires a grace period of 4 weeks to terminate the Contract in the event that Canada fails to cancel the subscription before the auto-renewal. In either of these options, Canada retains the right to decrease consumption without penalty. The Resulting Contract Clauses also include a Termination for Convenience clause that would allow Canada to terminate the Services and receive a refund of any pre-paid amount beyond the month that the Services are terminated.
Q.80 Section 4.1(f) refers to "all required security standards" – why doesn't this reference the specific annexes (A & B) that address security? Otherwise, this is too vague.	**A.80** The reason that this does not reference the specific Annexes where security requirements are addressed is because there are many elements to IT Security beyond Annex A & B, including Supply Chain Integrity requirements, mandatory qualification requirements (for Tier 1 and Tier 2), Security and Privacy Obligations, Security Requirements that apply to Professional Services only, and security requirements for the Contractor (such as DOS, DSC, and personnel clearances) which vary based on whether the Contractor is Canadian or foreign, as well as requirements that may apply to a client's unique Contract being issued against the SaaS SA. Therefore, it is not possible to reference all security requirements that will apply to each Supply Arrangement or Contract issued against a Supply Arrangement at the RFSA stage.
Q.81 Section 5.6 requires a warranty of non-infringement. What if there are pending IP infringement claims from patent trolls that a vendor is actively litigating. Can these be excluded from the warranty? Can the warranty remedy be linked exclusively to the indemnification obligation?	**A.81** If a Supplier is aware of IP infringement claims, they would not be able to certify "no claims", but would still be able to warrant that, **to the best of its knowledge**, nothing in the Solution, or in Canada's use of the Solution, **does or** will infringe or constitute a misappropriation of the intellectual property or other rights of a third party. These types of claims cannot be excluded from the warranty nor can the warranty remedy be linked exclusively to the indemnification obligation.
Q.82 Section 9.4 (Most Favored Pricing) does not take into account that additional obligations Canada imposes on vendors to provide the SaaS services in Canada and the cost of such obligations likely necessitates pricing higher than charged to other customers. Section 9.4 should come with a	**A.82** Canada has considered this request and the Price Certification wording detailed in Section 9.4 shall remain the same. While there may be costs associated with qualification to sell SaaS Solutions to the Government of Canada, it is up to the Supplier to determine whether the benefits of qualifying and selling SaaS to the GC through this vehicle outweigh

QUESTIONS	ANSWERS
qualification that includes under similar terms and conditions.	the costs. Furthermore, the Price Certification clause in Section 9.4 does make reference to like quality and quantity of goods, services, or both.
Q.83 Appendix C has a separate set of security obligations. Are these necessary in addition to Annex A & B of the RFP? To the extent there is a conflict, which security obligation prevails?	**A.83** Appendix C contains ongoing Security Obligations that apply throughout the period of the Contract(s), and are necessary to ensure that the Supplier continues to meet its obligations. The details regarding which document shall prevail in the event of a conflict are outlined in Section of the RFSA, entitled “Priority of Documents”. Appendix C falls under Annex F – Resulting Contract Clauses as it is an Appendix to the resulting Contract(s). Additionally, the ongoing security and privacy obligations that are attached to the Resulting Contract Clauses apply during the Contract period, whereas the RFSA Security Requirements are assessed prior to SA award. There are separate and unique security requirements that apply to the Supply Arrangement vs the Resulting Contracts.
Q.84 There does not appear to be a distinction between the provider of the Software as a Service, and the provider of the cloud infrastructure. The security obligations of Tier 2 M6, for example, are controlled by the Cloud Service Provider (CSP).	**A.84** Where the SaaS provider and CSP are separate, the mandatory security requirements would be assessed at all layers (Supplier, SaaS provider, and cloud service provider)
Q.85 For Tier 2 M8, is it sufficient to provide validation of the cloud infrastructure provider?	**A.85** Suppliers must provide their certifications as outlined in the RFSA. In the case where the Supplier is presenting a Submission against the RFSA is not the cloud infrastructure providers, CCCS is aware that it may be a challenge to obtain a copy of IaaS reports. In this case, the Supplier should indicate to CCCS what Cloud Infrastructure Provider they are using, and provide the certificates as well as a letter that indicates that they are a registered partner with the main hyper scale provider, as this indicates their level of expertise with the platform.
Q.86 For Tier 2 M12, can we rely on ISO/IEC 27018 of the CSP?	**A.86** Both the SaaS Publisher and the Cloud Service Provider must meet the requirements identified in M12.
Q.87 The RFP (Annex B) requires that the security requirements be flowed down to Sub-processors, which will include the CSP. If Canada already has an agreement with the CSP, can we rely on that contractual obligation? The CSP will not accept contractual liability to us for Canada requirements.	**A.87** We have reviewed this request previously under Q29, published AMD 004 and our position remains unchanged.
Q.88 Annex B, Section 5 (Auditing Compliance) and Section 12 (Auditing Compliance) – this isn’t something we will be able to provide. The auditing is done independently by the cloud infrastructure provider and the results are shared with customers. We will not be able to conduct an audit of the CSP's environment.	**A.88** See response to Q.85
Q.89 Various parts of the RFP request exact location of data centers. For security reasons, the CSP does not disclose exact physical locations of its infrastructure. How can we comply?	**A.89** The information requested regarding the location of data centers will be provided to CCCS through a non-disclosure agreement. Please refer to Q50, published under AMD 007, which outlines what steps are being taking to protect information that has been disclosed. If required, a Cloud Service Provider can also provide this information directly to CCCS through a non-disclosure agreement rather than providing this information to the Supply Arrangement holder or to PSPC.
Q.90 Is this currently your position that all OEMs need these to pass the security assessment: • FSC at Secret level • DSC at PB level	**A.90** The following levels of Security are required, regardless of stream (Stream 1 - Protected B, Stream 2 - Protected A, or Stream 3 - VAR Protected A) DOS – Protected B DSC – Protected B

QUESTIONS	ANSWERS
And are these requirements limited to the SA holder (stream 3 -resellers) or must both the SA holder and SaaS Publisher also have to meet the SRCL?	As part of CCCS' assessment, they require that both the CSP and/or the SaaS Publisher meet the requirements of the SRCL (DSC/DOS – Protected B). In addition, the way that the RFSA is currently structured, a VAR applying under Stream 3 would also be required to hold the industrial security clearances detailed above as they are the holders of the SA.
Q.91 Can Canada please confirm how many agreements have been issued to date under this procurement?	**A.91** For a list of SAs that have been awarded to date, please see the "Related award notices" section of the RFSA posted here: https://buyandsell.gc.ca/procurement-data/tender-notice/PW-EEM-003-35660
Q.92 In Annex A Qualifications, under Tier 1 Assurance (Up to and including Protected A Data) under the requirement to demonstrate compliance for Tier 1 column of M7 Supply Chain Risk Management, the requirement states: To be considered compliant, the provided documentation demonstrating compliance by providing at least one of the following three options: 1. ISO/IEC 27036 Information technology -- Security techniques – Information security for supplier relationships (Parts 1 to 4); 2. NIST Special Publication 800-161 - Supply Chain Risk Management Practices for Federal Information Systems and Organizations; or 3. ITSG-33 security control for SA-12 and SA-12(2) where the organized defined security safeguards is documented in a Supply Chain Risk Management (SCRM) plan. The SCRM Plan must describe the Software as a Service Provider's approach to SCRM and demonstrate how the Supplier of the proposed Commercially Available Public Software as a Service will reduce and mitigate supply chain risks Can the Crown please confirm that they will accept self-assessment documentation for the three options to substantiate M7 Supply Chain Risk Management?	**A.92** Suppliers are required the have the ISO 27001, ISO 27017 and SOC 2 Type 2 certificates and full audit reports for Tier 2. For Tier 1, either ISO 27001 or SOC 2 Type 2 is required. For Annex A Tier 1 M7, certification and assessment reports are not necessary but strongly recommended as a self-assessed CSP will be assessed with higher risk. For Tier 2 M11, certification and assessment reports are required and evidence for each control is required.
Q.93 In the contractual clauses of the RFSA, there is a provision which allows the supplier to make representations (inquiries process) in order to explain why a clause is too restrictive. Is there a document or template that we should use in such a case, or is a letter from the supplier acceptable? In addition is there is a deadline within the process or a particular period for this "inquiries process"? Finally, if there is such a process, what is the response time?	**A.93** Suppliers can ask questions and request changes to the RFSA's terms and conditions and the resulting contract by submitting their questions by email to our generic email address: TPSGC.LENQS-SAAS.PWGSC@tpsgc-pwgsc.gc.ca There is no deadline for asking questions. The response time will depend on the nature of the question; in some cases we will need to consult with other teams (CCCS, CISD/IISD, legal services, etc.).
Q.94 Annex A Stream 1 Tier 2 M12 states that ISO 27018 certification documents, which must have been issued within 12 months prior to the submission date must be provided. Does this mean that the ISO 27018 must have been issued in the last 12 months, or more than 12 months ago?	**A.94** The ISO 27018 must have been issued within the 12 months preceding the submission date.
Q.95 If there is nothing to disclose, is it necessary to submit a Declaration of Convicted Offences form?	**A.95** No, if there is nothing to disclose, then it is not necessary to submit a Declaration of Convicted Offences form with your submission. The conditions under which a Declaration of Convicted Offences form must be submitted are detailed at the following link: https://www.tpsgc-pwgsc.gc.ca/ci-if/declaration-eng.html
Q.96 If a client has already purchased the SaaS solution through another method of procurement, can	**A.96** Yes they can, assuming the Solution is available through the vehicle. If the Solution is not

QUESTIONS	ANSWERS
they leverage the SaaS SA for the Professional Services component only?	available through the vehicle they will need to procure professional services for the Solution outside of the RFSA.
Q.97 Is it possible for SaaS contracts to be multi-year?	**A.97** The RFSA does not impose any contract term limitations. This is not to say that a client would not have departmental constraints, or otherwise, but the RFSA itself does not contain any restrictions with respect to the contract period/option years.
Q.98 Under section 4.1 Solution Services: e) Usage Grant. The Contractor grants to Canada the non-exclusive, non-assignable right to access and use the Solution from an unlimited number of locations, devices and operating environments, through secure, wireless, mobile or other connection, via the internet, a web browser or other access connection technology which may become available. Does this mean that unlimited free licenses are an expectation?	**A.98** Section 4.1(e) of the resulting contract terms is not stating that unlimited licenses must be provided, but rather that the Solution be available for use on an unlimited number of locations, devices and operating environments. It is the right to access and use of the Solution that is in question here, not the number of licences to be provided.
Q.99 We work with multiple departments within the government, and our pricing model is customized to fit each department's needs. We do not have a standard pricing structure. How will this process will affect pricing and contracts currently active?	**A.99** The RFSA process will not have any effect on contracts currently active. For information on how to prepare the Annex C - SaaS Solutions and Professional Services Ceiling Prices please see Part 3.3 Section II: Financial Submission.
Q.100 With respect to Tier 1, M7 – Supply Chain Risk Management will PSPC confirm that if a Supplier can demonstrate alignment with at least one of these options through a self-evaluated questionnaire with attestation, the supplier will be deemed compliant to the requirement?	**A.100** See response to Q92.
Q.101 We are requesting consideration for the modification of the text of *Annex F, Resulting Contract Clauses, Section 3.5* to the following: "If the Contractor is unable to provide the Services with no less favourable core features and functionality, the Contractor will provide written Notice to Canada identifying the circumstance, and alternative options, specifically including a reduction in pricing. If no proposed alternative option is acceptable to Canada, the Contractor agrees to consent to a termination of the Contract pursuant to Section 7.5.3(c)b.(ii)"	**A.101** This request is accepted, and the changes are reflected in the updated version of Annex F referenced in Section 8.0 of this amendment below.
Q.102 We are requesting consideration for the modification of the text of *Annex F, Resulting Contract Clauses, Section 7.6(b)* to the following: "The Contractor agrees that, in the period leading up to the end of the Contract Period, if Migration or Transition Services are requested by Canada, it will reasonably assist Canada in the transition from the Contract to a new contract with another supplier and or migrate Client's Data to a new supplier environment, that there will be no charge for the services below other than those charges set out in the Basis of Payment."	**A.102** This request is accepted, and the changes are reflected in the updated version of Annex F referenced in Section 8.0 of this amendment below.

3.0 Respond to Industry day Q+A:

Note: Questions may have been modified and/or condensed**.**

INDUSTRY DAY QUESTIONS	INDUSTRY DAY ANSWERS
IDQ.20 Will this vehicle be used to procure professional services as well or is this vehicle's primary role to secure SaaS Solutions?	**IDA.20** This vehicle will be used to procure SaaS Solutions and associated professional services. When you submit Annex C, you are permitted to include professional services; however they are limited in scope to those that are related to the SaaS solutions being sold through the vehicle. Section

INDUSTRY DAY QUESTIONS	INDUSTRY DAY ANSWERS
	3.3(b) of the RFSA lists the types of professional services that can be procured through the vehicle. These include: Quick Start Guide ("QSG") training and services, implementation services, training services, data cleansing, migration and transition services, and advisory services.
IDQ.21 Would PSPC want Platform as a Service (PaaS) solutions to apply through this RFSA?	**IDA.21** The RFSA is limited to Software as a Service (SaaS) solutions. PaaS solutions are unable to apply through the RFSA.
IDQ.22 What will be the order of evaluation for submissions to CCCS; i.e. will the first applicants on in Wave 2 be processed first?	**IDA.22** CCCS will onboard applicants, then all the submissions will be sent to their coordinators who will reach out for any additional documentation to assist with the assessment process. When a vendor responds with all documentation, their order in the assessment will be determined. So it is not necessarily the order that they are onboarded, but rather the order in which all documentation is received in order to be prepared for the kick off meeting and the assessment process.
IDQ.23 How long is the CCCS evaluation process expected to take for each Cloud services solution submitted?	**IDA.23** From the kick off meeting where the vendor explains their services submitted to CCCS, it normally takes between 3-5 months, but it all depends on how much information is provided, and how flexible the vendor is.
IDQ.24 Can updates to the GC Security Control Profile Traceability Matrix (i.e. ITSG-33 security controls) be submitted during the CCCS evaluation process?	**IDA.24** CCCS need to see evidence in the form of policies and procedures for the controls to show that they are met. If you do have policies and procedures that you can share with CCCS, you can give this during the onboarding process. Otherwise CCCS will follow up for these during the evaluation process.
IDQ.25 Some Cloud solution components may require support from technical resources located outside of Canada (e.g. Tier 3 support). Will this be permitted and are there any additional security requirements or a special remote access procedure that will need to be followed? Will these resources require GC personnel security clearances?	**IDA.25** If there are domestic personnel requiring access to protected information, they will require reliability status clearance, unless they are determined to be admin or privileged user, whereby they would require secret clearance. Internationally, it may be permitted, but the foreign organization would be required to go through a security screening process. To obtain a reliability status equivalency, the company must provide certain proofs including, but not limited to, an Attestation Form, Background Verification Form, completed DSC, and IT Checklists. To obtain a secret status equivalency, the foreign supplier has to be located in a country that has a bilateral agreement in place with Canada (see link below for a list of those countries). In those cases, the foreign supplier would have to see assurance from the national security authority for that country, and that could take up to a year. https://www.tpsgc-pwgsc.gc.ca/esc-src/international-eng.html

INDUSTRY DAY QUESTIONS	INDUSTRY DAY ANSWERS
IDQ.26 Can you please confirm how existing SaaS products/vendors that have already been certified by CCCS/PSPC/Contract Security Program for up to Protected B will be handled?	**IDA.26** If you have been through the process for the PSPC RFSA already in CCCS's wave 1, there is no need to apply again. If you have been assessed by CCCS outside of this vehicle, you could still apply to wave 2. If you have already been assessed by CCCS, you have to submit the summary report that they provided you, then CCCS will onboard the vendor into the program, and verify that there are no changes, and the same products have been assessed. For the Contract Security Program, you are required to have the security certifications and documentation that are detailed in the RFSA (Annex G or H). If you have obtained these outside the vehicle, or already met the security requirements with CISD/IISD, and already have your Designated Organization Screening (DOS), Document Safeguarding Capability (DSC), or personnel clearances, you would not have to go through the process again, and clearances would have to be confirmed with CISD/IISD as applicable.
IDQ.27 How long is the process with CCCS expected to take?	**IDA.27** The onboarding process with CCCS is about 28 days. You will receive an email about a week after you have been onboarded, and the kickoff meeting with CCCS will come shortly thereafter. Following the kickoff meeting it will be approximately 3-5 months, which also includes the Supply Chain Integrity assessment process.
IDQ.28 How do we check which hosted platforms have been assessed by CCCS?	**IDA.28** These are listed on the Cloud Brokering website (https://cloud-broker.canada.ca/s/central-provider-page-v2?language=en_CA). If you are hosted on your own platform, CCCS can assess that as well, it just may be a little bit longer as it is a full stack component, and it will require more in terms of physical security elements.
IDQ.29 What is the process to get a non-disclosure agreement (NDA) signed?	**IDA.29** While Wave 2 is open please email contact@cyber.gc.ca. When contacted, CCCS will start the NDA process. They will also send a submission package and a PGP key. If you do not want to use a PGP key, they recommend using a password encryption to send all of your documentation to them.
IDQ.30 Can you confirm that FSC (Secret) is required for organizations who are proposing solutions only in the Protected A stream?	**IDA.30** For an organization that is accessing protected information, a DOS will be initiated and granted for the organization. An FSC is required for accessing classified information, and so would not be granted to an organization. However the company security officer and some of the privileged user that will be identified will need secret level clearance. The Contract Security Program has a process in place that will allow the personnel to be cleared to a secret level clearance, though the organization may only hold a DOS.

INDUSTRY DAY QUESTIONS	INDUSTRY DAY ANSWERS
IDQ.31 Can you please explain the difference between a SaaS application provider and a Cloud Service Provider in the context of this RFSA?	**IDA.31** The SaaS application provider and the CSP may be the same, but if the SaaS solution is hosted on a third-party's cloud, then they would be different. From a security perspective, CCCS recommends a previously assessed Cloud Service Provider, a previously assessed IaaS, and a previously assessed PaaS service. Otherwise, CCCS would have to assess the SaaS provider itself, as some controls may be inherited and they need to understand what these inherited components are.
IDQ.32 Can a SaaS publisher assign more than one privileged user?	**IDA.32** There currently is no cap on the amount of admins or privileged users that a SaaS publisher can assign, however a limit may be set at a later date.
IDQ.33 Are there specific security requirements for Canadian companies working with off-shore IT teams?	**IDA.33** All companies would have to follow the security requirements of the contract. Where you are using foreign resources, there would be additional requirements. For reliability status, equivalency would need to be proven, which can take up to 5 days. Roles with privileged access would require secret clearance or the equivalency of, and that can take up to a year, as that would be done through the security authority of that country.
IDQ.34 Can you clarify the DSC requirement process for companies applying to the Protected A stream?	**IDA.34** Once the DOS is approved, the Contract Security Program will reach out to the company security officer (CSO) to confirm what the presence in Canada is, and where the information is being hosted (whether in your facility or another facility that has already been assessed and approved). From there, it will be determined what requirements are necessary. We cannot give specifics of what requirements are, as every company and every site is different.
IDQ.35 Is an existing on-premises deployment sufficient justification for a sole-source of the SaaS equivalent (ie. a migration to SaaS)? What if a Bring Your Own License (BYOL) is possible, to reduce the SaaS 'pay as you go' costs?	**IDA.35** This would not be sufficient sole-source justification. A BYOL model would not be possible in this case, as all we are allowing on the RFSA is SaaS. In a BYOL model the client would already own their own licenses, so they wouldn't necessarily be procuring SaaS, they would be hosting their existing licenses, so that would not be applicable.
IDQ.36 How are PSPC and Shared Services Canada (SSC) coordinating to ensure the GC has the best solutions as well as standards are maintained?	**IDA.36** In terms of standards, we do have the same cloud security requirements across the GC. In terms of overlap on the products that are available, it would be up to the client departments to determine which avenue they wanted to take if there were two procurement vehicles available for the same solution. We cannot comment on what is available through SSC; however, we can say that we have made the RFSA known to SSC, and they have been briefed on the process of applying, how departments can access it, and how CCCS is assessing it, as well as the requirements of the RFSA.
IDQ.37 Is there a list of countries with which Canada has agreements that facilitate the security clearance process for off-shore personnel?	**IDA.37** The list of countries that have a bilateral security agreement with Canada can be found in the following link: https://www.tpsgc-pwgsc.gc.ca/esc-src/international-eng.html

INDUSTRY DAY QUESTIONS	INDUSTRY DAY ANSWERS
IDQ.38 As a SaaS solution provider we do not directly provide the services required to stand up the software. We have a large partner network that stands up our software and customizes it for the requirement of the specific organization. Do our partners that stand up our software also need to qualify through the RFSA process?	**IDA.38** You may list professional services that are not offered by the SaaS solution provider, however if there were personnel security requirements that needed to be met for those professional services, then they would need to be assessed and met by the company that is offering those services. The SaaS solution provider would be responsible for ensuring that the requirements of the contract were met in providing that work, which would typically entail a separate arrangement or subcontract with those companies.
IDQ.39 Regarding the cloud service providers that are already certified, is it only their Canada regions that are certified? Or does it apply to other regions as well?	**IDA.39** Only their Canadian regions were assessed, as some cloud service providers implement things different depending on the country of origin.
IDQ.40 What will the sole source limit be under this vehicle?	**IDA.40** The vehicle doesn't have an independent sole-source limit. Anyone doing a procurement over $40k through the vehicle would be required to have sole-source justification to direct to one company. Under $40k they would be able to direct to a specific company without sole-source justification. One other thing that's important to add when speaking to client departments on this, is that if they are doing the procurement under their delegated authority, they would not necessarily need to provide this justification to PSPC, but they would need to document it for their own internal files. If the procurement is above their delegated authority, or in any case where PSPC is doing the procurement on their behalf, they will need to provide PSPC with their sole-source justification, which would be reviewed and validated before proceeding with the procurement.
IDQ.41 If a break glass procedure is in place do we still have to go through the security clearance for support resources outside Canada?	**IDA.41** Security clearance for support resources outside of Canada would have to take place. If they already have security clearances, they will have to be verified.
IDQ.42 What is the future of on-premises software requirements? Will the Software Licensing Supply Arrangement (SLSA) remain in place?	**IDA.42** The SLSA is remaining in place and is independent of the RFSA, as on-premises software is going to be an ongoing requirement for the GC for the foreseeable future. Both vehicles will be available to client departments, and clients who require on-premises software will be able to use the SLSA, or complete procurements outside of the SLSA.
IDQ.43 For Protected B certification, is a Canadian CSO (person living in Canada) is required?	**IDA.43** For the Canadian organization to be cleared, the CSO must be a Canadian citizen or permanent resident, and must reside in Canada. For the organization that we're registering into the program, any super user or privileged user must also be employees of the organization that is being registered, not employees of a parent company.
IDQ.44 When is the next CCCS window after this one?	**IDA.44** At this time there is not an exact date set for the next window. CCCS will be working through the applications in Wave 2 before determining a date for the next window.
IDQ.45 Do you want to see vendors go through approvals for Protected A first, to reduce effort to evolve to Protected B later (e.g. if we have additional audits for ISO/SOC2 in progress now)? Or should we just wait and do Protected B from scratch later?	**IDA.45** This is up to suppliers to decide. If you do not have solutions for protected A data, then we would recommend to wait and do protected B when you are ready, as CCCS has limited capacity to assess solutions so we do not want them to be assessing at a Protected A level if this is not useful to clients.

INDUSTRY DAY QUESTIONS	INDUSTRY DAY ANSWERS
IDQ.46 If a department wants a SaaS for unclassified requirements, is it still required to achieve approval for Protected A?	**IDA.46** The lowest tier that we have available through the RFSA is Protected A, so it would be necessary to qualify for the RFSA under Protected A. Otherwise, the procurement for an unclassified solution would have to be done outside of the RFSA, but is important to note that there would still be security requirements that would have to be assessed in this scenario. It can be challenging for client departments to do a low level SCI assessment and IT security assessment on their own. The RFSA is in place to simplify that process for clients departments, and while they can do unclassified procurements outside of the RFSA, we are encouraging suppliers to qualify under the RFSA, and for client departments to procure through the RFSA as much as possible, as most client departments are still developing capacity to do those assessments on their own. CCCS is prioritizing the GC Cloud procurement vehicles, including this RFSA, so it is a preferred method for clients.
IDQ.47 Regarding the qualification requirements listed within RFSA Annex A, if a submission does not include full audit reports for all of the certifications listed, are they immediately disqualified for submission?	**IDA.47** If you only have the certifications and not the full audit reports, you will not be onboarded, as CCCS needs those reports in order to conduct the assessment. When submitting to the PSPC RFSA team, and not during a CCCS onboarding window, you could present us with all documentation and forms required without those certifications. It's only when you onboard with CCCS IT security assessment process that you will need to have all of those certifications and audit reports.

4.0 Annex A Tier 1 M5 and M7, and Tier 2 M8 and M11, are hereby deleted and replaced with the following:

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 1 (Up to and including Protected A Data)
M5	**Third Party Assurance**	The Software as a Service must be designed and developed to ensure the security of their proposed Commercially Available Public Software as a Service, including, implementing information security policies, procedures, and security controls. For suppliers that have already completed the security assessment by providing to CCCS their certifications and audit reports and have already entered into a Non-Disclosure Agreement (NDA) with them, must send their certifications and audit reports directly to CCCS client services at contact@cyber.gc.ca in order to meet this requirement. For suppliers that have not completed the security assessment, the onboarding process will commence once the Submission complies with the requirements of the Request for Supply Arrangements, meets all mandatory technical and financial evaluation criteria, and provides all of the mandatory certifications in order to be declared responsive. PSPC will then refer the Supplier to CCCS client services to begin the onboarding process to the IT Assessment and to enter into an NDA with them in order to receive a copy of the onboarding submission form and any additional information required to meet this requirement.	The Supplier must provide documentation to Canada that demonstrates how the Software as a Service Provider of the proposed Commercially Available Public Software as a Service complies with the requirements in the Third Party Assurance Requirements. Compliance must be demonstrated by providing one or more of the following industry certifications identified below, and validated through independent third party assessments. The Supplier must provide the following industry certifications and audit reports for the proposed Service to demonstrate compliance: (a) One of the following: (i) ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems – Requirements; or (ii) AICPA Service Organization Control (SOC) 2 Type II (b) Self-assessment of its services against the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) version 3.01 or subsequent version. Each provided certification and assessment report must: 1. Be valid as of the Submission date; 2. Identify the legal business name of the proposed Supplier, and applicable Supplier Sub-processor, including CSP;

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 1 (Up to and including Protected A Data)
			3. Identify the current certification date and/or status; 4. identify the list of Assets, Supplier Infrastructure, and Service Locations within the scope of the certification report. 5. The scope of the report must map to locations and services offered by the proposed Supplier. If the carved out method is used to exclude subservice organizations such as data centre hosting, the subservice organization's assessment report must be included; and 6. Be issued from an independent third party qualified under AICPA or CPA Canada, and/or ISO certification regime and that conforms to ISO/IEC 17020 quality management system standard. **Please note:** • Certifications must be provided for all portions of the proposed Service identified; • Certifications must be accompanied by assessment reports; and • Certifications must be valid and within the 12 months prior to the start of a contract.
M7	**Supply Chain Risk Management**	The Supplier of the proposed Commercially Available Public Software as a Service must implement safeguards to mitigate supply chain threats and vulnerabilities to IT services. This includes, but is not limited to designing and implementing controls to mitigate and contain data security risks through proper separation of duties,	The Supplier must demonstrate how the Software as a Service Provider of the proposed Commercially Available Public Software as a Service complies with the requirements in Supply Chain Risk Management Requirements as documented under the Software as a Service Provider Information Technology Security Assessment program.

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 1 (Up to and including Protected A Data)
		role-based access, and least-privilege access for all personnel within the supply chain.	To be considered compliant, the provided documentation demonstrating compliance by providing at least one of the following three options: 1. ISO/IEC 27036 Information technology -- Security techniques -- Information security for supplier relationships (Parts 1 to 4); or 2. NIST Special Publication 800-161 - Supply Chain Risk Management Practices for Federal Information Systems and Organizations; or 3. ITSG-33 security control for SA-12 and SA-12(2) where the organized defined security safeguards is documented in a Supply Chain Risk Management (SCRM) plan. The SCRM Plan must describe the Software as a Service Provider's approach to SCRM and demonstrate how the Supplier of the proposed Commercially Available Public Software as a Service will reduce and mitigate supply chain risks; or 4. CSA STAR controls to support CSA CCM Supply Chain Management controls.

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

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 2 (Up to and including Protected B Data)
		demonstrate the compliance. For suppliers that have already completed the security assessment by providing to CCCS their certifications and audit reports and have already entered into a Non-Disclosure Agreement (NDA) with them, must send their certifications and audit reports directly to CCCS client services at contact@cyber.gc.ca in order to meet this requirement. For suppliers that have not completed the security assessment, the onboarding process will commence once the Submission complies with the requirements of the Request for Supply Arrangements, meets all mandatory technical and financial evaluation criteria, and provides all of the mandatory certifications in order to be declared responsive. PSPC will then refer the Supplier to CCCS client services to begin the onboarding process to the IT Assessment and to enter into an NDA with them in order to receive a copy of the onboarding submission form and any additional information required to meet this requirement.	(e) The scope of the report must map to locations and services offered by the proposed Commercially Available Software as a Service. If the carved-out method is used to exclude subservice organizations such as data centre hosting, the subservice organization's assessment report must be included; and (f) Be issued from an independent third party qualified under AICPA or CPA Canada, and/or ISO certification regime and that conforms to ISO/IEC 17020 quality system standard. The Supplier can provide additional supplementary evidence from system security plans, information system design, information system architecture, or documents that provide a comprehensive system description, such as assessment of its Services against the Cloud Security Alliance (CSA) Cloud Control's Matrix (CCM) version 3.01 or subsequent version, to support the claims from the above certifications, in order to demonstrate compliance to the GC Security Control Profile for Cloud-Based GC IT Services for Protected B, Medium Integrity and Medium Availability (PBMM). **Please note:** • Certifications must be provided for all portions of the proposed Service. • Certifications must be accompanied by assessment reports.
M11	**Supply Chain Risk Management**	The Supplier of the proposed Commercially Available Software as a Services must implement safeguards to mitigate supply chain threats and vulnerabilities to IT services in order to maintain confidence in the security of the sources of information systems and the IT components used to provide Services. This	The Supplier must demonstrate how the Supplier of the proposed Commercially Available Software as a Service complies with the requirements in the Supply Chain Risk Management Requirements as documented under the Supplier Information Technology Security Assessment program. To be considered compliant, the provided documentation must demonstrate that the Commercially Available Software as a

Mandatory ID	Sub-Category	Requirement	Required to demonstrate compliance for Tier 2 (Up to and including Protected B Data)
		includes, but is not limited to designing and implementing controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privilege access for all personnel within the supply chain.	Service supply chain risk management approach aligns with one of the following best practices: 1. ISO/IEC 27036 Information technology -- Security techniques -- Information security for supplier relationships (Parts 1 to 4); or 2. NIST Special Publication 800-161 - Supply Chain Risk Management Practices for Federal Information Systems and Organizations; or 3. ITSG-33 security control for SA-12 and SA-12(2) where the organized defined security safeguards is documented in a Supply Chain Risk Management (SCRM) plan. The SCRM Plan must describe the Supplier's approach to SCRM and demonstrate how the Suppliers of the proposed Commercially Available Software as a Service will reduce and mitigate supply chain risks; or 4. CSA STAR controls to support CSA CCM Supply Chain Management controls. The SCRM Plan must be independently assessed and validated by an independent third party certified under AICPA or CPA Canada, and/or ISO certification regime. The Suppliers must indicate where in response the reference material can be found, including the title of the document, and the page and paragraph numbers.

5.0 Annex C – SaaS Solutions and Professional Services and Ceiling Prices is hereby deleted in its entirety and replaced with the following:

ANNEX C – SaaS Solutions and professional Services Ceiling Prices

Option 1: Suppliers provide a link to their commercially-available SaaS catalogue and indicate the percentage discount offered to Canada.

URL:

OR

Option 2: Suppliers complete the table below.

TABLE 1 - PRODUCT LIST AND CEILING PRICES												
Item NO.	**SaaS Publisher's Part No. (A**	**SaaS Solution's Name (B)**	**SaaS Publisher's Name (C)**	**Cloud Service Provider's Name (D)**	**Ceiling Prices for SaaS Solutions (E)**	**Ceiling Prices for Optional Professional Services (F)**	**Unit of Measure (G)**	**Applicable Percentage Discount (H)**	**Language (s) available (I)**	**SaaS Solution Product Description (J)**	**SaaS Solution Information (K)**	**Keywords/tags (L)**
	(enter the Part Number that the SaaS Publisher uses to identify the SaaS Solution)	(enter the name that the SaaS Publisher uses to identify the SaaS Solution.	(enter the name of the SaaS Publisher that produces the SaaS Solution)	(enter the name of the Cloud Service Provider that hosts the SaaS)	(enter ceiling price for SaaS Solution per unit of measure in Canadian Dollars)	(enter ceiling price for professional services per per diem rates, hours, or package in Canadian Dollars for each category: Quick Start Guide ("QSG"), training and services, implementation services, training services, data cleansing, migration and transition services, and advisory services)	(enter the unit of measure for the SaaS, such as "per user", "per entity", etc. **and** subscription, term)	(enter the percentage discount that will be applied to the Ceiling Commercial Unit Prices for the duration for the SA)	(enter the language of the SaaS Solution, English and/or French)	(enter a brief description of the SaaS Solution – if applicable)	(enter a web site URL containing SaaS Solution information)	(enter keywords associated with the SaaS Solution that will help the Clients to easily search and find SaaS Solutions that meet their needs
1												
2												
3												

6.0 Part 6 – Supply Arrangement of solicitation EN578-191593/F is hereby deleted in its entirety and replaced with the editable version under the Attachments section of the Tender Notice page: RFSA - SaaS Method of Supply (GC Cloud) (EN578-191593/F).

7.0 Section 7.2 and 7.3 of Part 7 – Contractor Selection and Resulting Contract Clauses of solicitation EN578-191593/F are hereby deleted and replaced with the following:

7.2 Contractor Selection

(a) **Requirements valued at less than $40,000.00 CAD (GST/HST/QST included)**

(i) **Sole Source:** For requirements under **$40,000.00** CAD (applicable taxes included), Canada may choose, at its sole discretion, to direct contracts to a Supplier or to issue contracts following Bid Solicitations.

(b) **Requirements valued at $40,000.00 CAD (applicable taxes included) or greater**

(i) For requirements above **$40,000 CAD** (applicable taxes included) where there is only one source of supply, the Client must provide valid sole source limited tendering certification in accordance with the Government Contracting Regulations.

(ii) If only one source of supply exists for the required SaaS Solution, Canada may request that the Supplier submit price support prior to any contract award. Canada reserves the right to negotiate with the Supplier if it is determined that the prices being offered do not represent good value to Canada.

(iii) **Bid Solicitation:** For requirements valued at **$40,000 CAD** or above, if multiple SaaS Solutions are available from the GC SaaS Catalogue that can meet Canada's technical requirements, Canada will issue a bid solicitation to all Supply Arrangement holders who offer a Solution that meets the Client's technical requirements under their Supply Arrangement. If Canada determines that there is no sufficient capability under the GC SaaS Catalogue or it is a complex and/or specialized requirement, Canada may acquire the SaaS Solution outside the GC SaaS Catalogue and extend the competition to all firms by posting a formal bid solicitation document on the Government Electronic Tendering Service (GETS).

(c) **Set-Aside / Aboriginal Business**

(i) At the discretion of each Client, some solicitations against the resulting SAs may be set-aside for Aboriginal Business under the federal government's PSAB.

(ii) In the event that Canada wishes to issue a Contract under the PSAB, Canada may do so by utilizing the Aboriginal Suppliers' SAs. All the terms and conditions as stated in this SA apply to the Aboriginal Suppliers SAs.

Also note that the splitting of requirements, (i.e. the dividing of a requirement into several lower dollar value requirements) to avoid a higher approval authority is contrary to contracting policy.

7.3 Bid Solicitation Process

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

(b) The bid solicitation will be posted on GETS (www.buyandsell.gc.ca) and may be sent directly to Suppliers.

(c) Suppliers will have a minimum of 15 calendar days to respond to Canada or as specified by the Contracting Authority, whichever is longer.

(d) The bid solicitation will contain as a minimum the following:

(i) Additional or updated security requirements (*if applicable*);

(ii) a complete description of the SaaS Solution to be provided;

(iii) 2003, Standard Instructions - Goods or Services - Competitive Requirements;

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

"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."

(iv) bid preparation instructions;

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

(vi) evaluation procedures and basis of selection;

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

(viii) certifications*; and,*

(ix) conditions of the resulting contract.

(e) Annex E – SaaS Bid Solicitation Template may be used to conduct Bid Solicitations.

8.0 Annex F – SaaS Resulting Contract Clauses EN578-191593/F is hereby deleted in its entirety and replaced with the editable version under the Attachments section of the Tender Notice page: RFSA - SaaS Method of Supply (GC Cloud) (EN578-191593/F).

9.0 Annex H – Security Requirements for Foreign Suppliers EN578-191593/F is hereby deleted in its entirety and replaced with the following:

ANNEX H – Security Requirements for Foreign Contractor

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

The Designated Security Authority for Canada (Canadian DSA) is the Industrial Security Sector (ISS), Public Works and Government Services Canada (PWGSC), administered by International Industrial Security Directorate (IISD), PWGSC. The Canadian DSA is the authority for confirming **Contractor/Sub-processor/Subcontractor** compliance with the security requirements of this contract for foreign suppliers. The following security requirements apply to the foreign recipient **Contractor/Sub-processor/Subcontractor** incorporated or authorized to do business in a jurisdiction other than Canada and delivering/performing outside of Canada the Services and/or Work described in the Cloud Solutions, in addition to the Privacy and Security Requirements, detailed in Appendix C & Appendix D, respectively. These security requirements are in addition to those requirements identified in the Section entitled Protection and Security of Data Stored in Databases.

1. The Foreign recipient **Contractor/Sub-processor/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/Sub-processor/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/Sub-processor/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/Sub-processors/Subcontractors**, this will be the national Data Protection Authority (DPA).

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

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

   (b) The Foreign recipient **Contractor/Sub-processor/Subcontractor** must 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/Sub-processor/Subcontractor** in an Attestation Form, to provide confirmation of compliance and authorization for services to be performed.

   (c) The Foreign recipient **Contractor/Sub-processor/Subcontractor** must identify an authorized Contract Security Officer (CSO) and an Alternate Contract Security Officer (ACSO) (if applicable) to be responsible for the overseeing of the security requirements, as defined in this contract. This individual will be appointed by the proponent foreign recipient **Contractor's/Sub-processor'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.

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

      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/Sub-processor/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** information/assets to a foreign recipient **Contractor/Sub-processor/Subcontractor** for cause.

4. **CANADA PROTECTED/PERSONAL** information/assets, provided to the foreign recipient **Contractor/Sub-processor/Subcontractor** or produced by the Foreign recipient **Contractor/Sub-processor/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).

5. The Foreign recipient **Contractor/Sub-processor/Subcontractor** MUST NOT remove **CANADA PROTECTED** information/assets from the identified work site(s), and the foreign recipient **Contractor/Sub-processor/Subcontractor** must ensure that its personnel are made aware of and comply with this restriction.

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

7. The Foreign recipient **Contractor/Sub-processor/Subcontractor** must, at all times during the performance of the **Contractor/Sub-processor/Subcontractor** hold an equivalence to an approved Document Safeguarding Capability (DSC) at the level of **CANADA PROTECTED** A or B, as applicable.

All **CANADA PROTECTED** information/assets, furnished to the foreign recipient **Contractor/Sub-processor/Subcontractor** or produced by the foreign recipient **Contractor/Sub-processor/Subcontractor**, must also be safeguarded as follows:

8. The Foreign recipient **Contractor/Sub-processor/Subcontractor** must immediately report to the Canadian DSA all cases in which it is known or there is reason to suspect that **CANADA PROTECTED** information/ assets pursuant to this **contract/subcontract** has been compromised.

   OR

9. The Foreign recipient **Contractor/Sub-processor/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.

10. The Foreign recipient **Contractor/Sub-processor/Subcontractor** must not disclose **CANADA PROTECTED** information/assets to a third party government, person, firm or representative thereof, without the prior written consent of the Government of Canada. Such consent must be sought through the Canadian DSA.

11. The Foreign recipient **Contractor/Sub-processor/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.

12. Upon completion of the Services and/or Work, the foreign recipient **Contractor/Sub-processor/Subcontractor** must return to the Government of Canada, all **CANADA PROTECTED** information/assets furnished or produced pursuant to this **contract/subcontract**, including all **CANADA PROTECTED** information/assets released to and/or produced by its subcontractors.

13. The Foreign recipient **Contractor/Sub-processor/Subcontractor** requiring access to **CANADA PROTECTED** information/assets or Canadian restricted sites, under this contract, must submit a Request

for Site Access to the Departmental Security Officer of Department/Organization for which the Services and/or Work are performed under the Contract**.**

14. The Foreign recipient **Contractor/Sub-processor/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 until authorization to do so has been confirmed by the Canadian DSA.

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

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

17. All Subcontracts awarded to a third party foreign recipient are NOT to be awarded without the prior written permission of the Canadian DSA in order to confirm the security requirements to be imposed on the subcontractors.

18. All Subcontracts awarded by a third party foreign recipient are NOT to be awarded without the prior written permission of the Canadian DSA in order to confirm the security requirements to be imposed on the subcontractors.

19. The Foreign recipient **Contractor/Sub-processor/Subcontractor** must comply with the provisions of the Security Requirements Check List attached at Annex I.

20. Canada has the right to reject any request made separate and apart from the authorization in this Contract in connection with the Contractor delivering Services to electronically access, process, produce, transmit or store **CANADA PROTECTED** information/assets related to delivery of Services and/or the Work in any other country if there is any reason to be concerned about the security, privacy, or integrity of the information.

Protection and Security of Data Stored in Databases

1. The foreign recipient **Contractor/Sub-processor/Subcontractor** must ensure that all the databases used by organizations to provide the services described in the proposed Cloud Solutions containing any **CANADA PROTECTED B** Information, related to the Services and/or Work, are located in Canada.

2. The foreign recipient **Contractor/Sub-processor/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/Sub-processor/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/Sub-processor/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/Sub-processor/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/Sub-processor/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.

Personal Information

Interpretation

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;

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.

Ownership of Personal Information and Records

To perform the Services and/or Work, the foreign recipient **Contractor/Sub-processor/Subcontractor** will be provided with and/or will be collecting Personal Information from third parties. The foreign recipient **Contractor/Sub-processor/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/Sub-processor/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/Sub-processor/Subcontractor** agrees to create, collect, receive, manage, access, use, retain and dispose of the Personal Information and the Records only to perform the Services and/or Work in accordance with the **contract/subcontract**.

Collection of Personal Information

1. If the foreign recipient **Contractor/Sub-processor/Subcontractor** must collect Personal Information from a third party to perform the Services and/or Work, the foreign recipient **Contractor/Sub-processor/Subcontractor** must only collect Personal Information that is required to perform the Services and/or Work. The foreign recipient **Contractor/Sub-processor/Subcontractor** must collect the Personal Information from the individual to whom it relates and the foreign recipient **Contractor/Sub-processor/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/Sub-processor/Subcontractor**.

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

3. If requested by the Contracting Authority, the foreign recipient **Contractor/Sub-processor/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/Sub-processor/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/Sub-processor/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/Sub-processor/Subcontractor** must ask the Contracting Security Authority for instructions.

Maintaining the Accuracy, Privacy and Integrity of Personal Information

The foreign recipient **Contractor/Sub-processor/Subcontractor** must ensure that the Personal Information is as accurate, complete, and up to date as possible. The foreign recipient **Contractor/Sub-processor/Subcontractor** must protect the privacy of the Personal Information. To do so, at a minimum, the foreign recipient **Contractor/Sub-processor/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/Sub-processor'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 Services and/or Work (for example, by using passwords or biometric access controls);

d. provide training to anyone to whom the foreign recipient **Contractor/Sub-processor/Subcontractor** will provide access to the Personal Information regarding the obligation to keep it confidential and use it only to perform the Services and/or Work. The foreign recipient **Contractor/Sub-processor/Subcontractor** must provide this training before giving an individual access to any Personal Information and the foreign recipient **Contractor/Sub-processor/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/Sub-processor/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/Sub-processor/Subcontractor** has decided not to make the correction for any reason. Whenever this occurs, the foreign recipient **Contractor/Sub-processor/Subcontractor** must immediately advise the Contracting Authority of the details of the requested correction and the reasons for the foreign recipient **Contractor's/Sub-processor'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/Sub-processor/Subcontractor** and Canada at any time; and

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

Safeguarding Personal Information

The foreign recipient **Contractor/Sub-processor/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/Sub-processor/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 Services and/or 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.

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/Sub-processor/Subcontractor** must submit the following to the Contracting Authority:

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

d. a complete copy (in an electronic format agreed to by the Contracting Authority and the foreign recipient **Contractor/Sub-processor/Subcontractor**) of all the Personal Information stored electronically by the foreign recipient **Contractor/Sub-processor/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/Sub-processor/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/Sub-processor/Subcontractor** to collect Personal Information;

b. a list of the types of Personal Information used by the foreign recipient **Contractor/Sub-processor/Subcontractor** in connection with the Services and/or 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/Sub-processor/Subcontractor** has granted access to the Personal Information or the Records;

f. a list of all measures being taken by the foreign recipient **Contractor/Sub-processor/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/Sub-processor/Subcontractor** intends to implement to safeguard the Personal Information and the Records.

Audit and Compliance

Canada may audit the foreign recipient **Contractor's/Sub-processor's/Subcontractor's** compliance with these supplemental general conditions at any time. If requested by the Contracting Authority, the foreign recipient **Contractor/Sub-processor/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/Sub-processor/Subcontractor** must immediately correct the deficiencies at its own expense.

Statutory Obligations

1. The foreign recipient **Contractor/Sub-processor/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/Sub-processor/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/Sub-processor/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/Sub-processor/Subcontractor** believes that any obligations in the **contract/subcontract** prevent it from meeting its obligations under any of these laws, the foreign recipient **Contractor/Sub-processor/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/Sub-processor/Subcontractor** believes it conflicts.

Disposing of Records and Returning Records to Canada

The foreign recipient **Contractor/Sub-processor/Subcontractor** must not dispose of any Record, except as instructed by the Contracting Authority. On request by the Contracting Authority, or once the Services and/or 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/Sub-processor/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/Sub-processor/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/Sub-processor/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.

SECRET CLEARANCE

Secret clearance will be required for any Contractor/Sub-processor/Subcontractor personnel that has elevated privileges with unrestricted logical access to the GC assets hosted in the Contractor data centers, any sensitive system and security incident data.

The contractor and/or any and all subcontractors must be from a country with which Canada has an international bilateral industrial security instrument or will have such an instrument with Canada by the end of the bidding period. The Contract Security Program (CSP) has international bilateral industrial security instruments with the countries listed on the following PSPC website: http://www.tpsgc-pwgsc.gc.ca/esc-src/international-eng.html.

1. Subcontracts which contain security requirements are **NOT** to be awarded without the prior written permission of **their respective National Security Authority (NSA) or Designated Security Authority (DSA), in accordance with the National legislation, regulations and policies of the supplier's country / the Canadian DSA.**

2. The Foreign recipient **Contractor / Sub-processor / Subcontractor** MUST NOT utilize its Information Technology systems to electronically process, produce, or store on a computer system and transfer via an IT link any **CANADA PROTECTED / CLASSIFIED** information/assets until the

National Security Authority (NSA) or Designated Security Authority (DSA) of **the supplier's country** has granted approval to do so. After approval has been granted in writing to the Foreign recipient **Contractor / Sub-processor / Subcontractor**, these tasks may be performed up to the level of **SECRET.**

3. The Foreign recipient **Contractor / Sub-processor / Subcontractor** shall not use the **CANADA PROTECTED / CLASSIFIED** information/assets for any purpose other than for the performance of the **Contractor / Sub-processor / Subcontractor** without the prior written approval of the Government of Canada. This approval must be obtained from the Canadian DSA.

4. The Foreign recipient **Contractor / Sub-processor / Subcontractor** shall immediately report to the Canadian DSA all cases in which it is known or there is reason to suspect that **CANADA PROTECTED / CLASSIFIED** information/assets pursuant to this **Contractor / Sub-processor / Subcontractor** has been compromised.

5. The Foreign recipient **Contractor / Sub-processor / Subcontractor** shall not disclose **CANADA PROTECTED / CLASSIFIED** information/assets to a third party government, person, firm or representative thereof, without the prior written consent of the Government of Canada. Such consent shall be sought through the {recipient's National Security Authority/ Designated Security Authority (NSA/DSA) / Canadian DSA}.

6. The Foreign recipient **Contractor / Sub-processor / Subcontractor** must comply with the provisions of the Security Requirements Check List attached at Annex I.

10.0 **Protected SaaS RFSA Industry Day presentation:**

Serving GOVERNMENT, serving CANADIANS. Au service du GOUVERNEMENT, au service des CANADIENS.

Protected SaaS Request for Supply Arrangement (RFSA)

Welcome to the Industry Day

11 January 2021
9:00 AM a 12:00 PM

Software Procurement Directorate
Public Services and Procurement Canada

Welcome and Introduction

Protected SaaS RFSA - Industry Day

Agenda

Time	Description and Objectives
9:00 to 9:05	Welcome and Introduction – PSPC
9:05 to 9:15	Industry Day objectives – PSPC
9:15 to 9:45	Presentation of the Procurement Vehicle - PSPC
9:45 to 10:30	Security Requirements – PSPC, CCCS & CSP
10:30 to 11:00	Financial Requirements – PSPC
11:00 to 11:40	Questions and Answers – Industry
11:40 to 11:45	Closing remarks - PSPC

Objective

The intent of this presentation is to provide suppliers with information and guidance on how to participate under this procurement vehicle to meet GC business needs and requirements.

Presentation of the Protected SaaS Procurement Vehicle

Table of Contents

Protected SaaS RSFA benefits for the industry

- Increase sales leads within GC departments (Internal distribution list and online catalogue)

- Simplified qualification process and new collaborative approach with PSPC
- Flexible approach to provide products and price lists
- Contracting vehicle in place to sell up to Protected B SaaS to the GC
- New Limitation of Liability that is fair and reasonable adapted to SaaS

- Support the GC toward the new Digital Transformation objectives

1. GC Digital Transformation (1/2)

Business Driver #1: To Support the GC Cloud Adoption Strategy

The software industry is evolving rapidly toward a cloud-based ecosystem, therefore the GC is adopting a proactive measure to respond to this evolution.

“The GC’s cloud adoption strategy requires that CIOs consider the public cloud deployment model and the software-as-a-service (SaaS) delivery model first because they offer the greatest benefits to the GC” *

The “**Cloud-First”** adoption strategy is promoting cloud as the preferred option for delivering IT services, and public cloud is the preferred option for cloud deployment within departments.

* TBS :GC Cloud Adoption Strategy : 2018 update

1. GC Digital Transformation (2/2)

Business Driver #2: To achieve the following Goals and Objectives

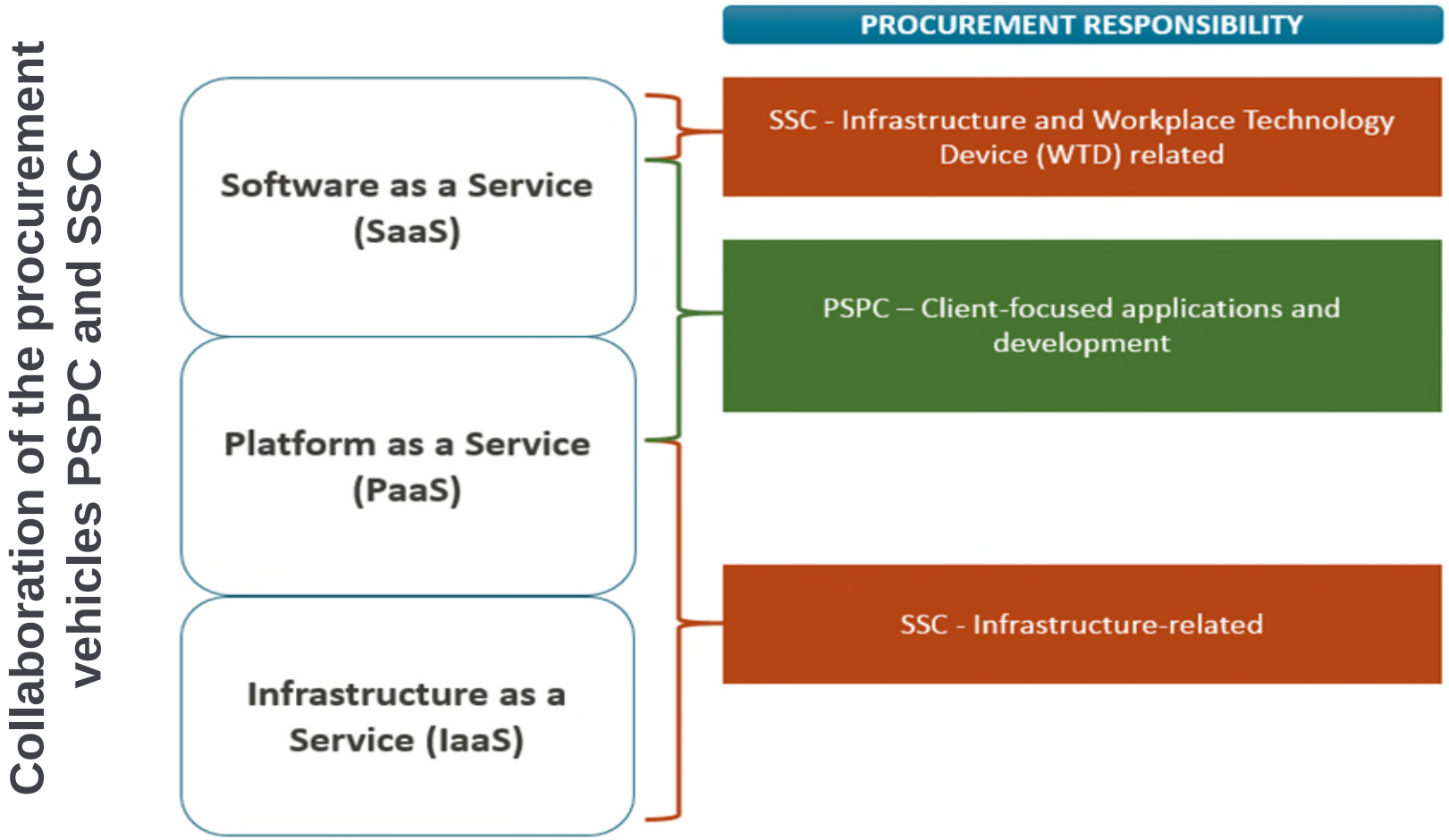
1. Provide GC Departments with a contracting vehicle to **simplify the procurement process** to acquire SaaS Solutions and Services

2. Establish a list of pre-qualified suppliers in order to **increase the number of solutions** available to the GC departments to access the latest SaaS

3. Allow GC departments to procure applications that are **accessible from various devices and do not require management of the infrastructure**

4. Qualify **Secure**, Unclassified, Protected A and Protected B, SaaS Solutions that ensure the protection of GC Assets.

2. GC Cloud Procurement Roles and Responsibilities



3. Protected SaaS RFSA Process

Innovation

- RFI issued to align GC requirements with industry standards.
- 40+ One-on-One sessions held.
- Incorporated feedback from the industry.
- Simplified contract terms and conditions.
- Built-in new Limitation of Liability clauses.

Evolving

- RFSA permanently published without closing date.
- Flexibility for suppliers to qualify.
- Enabling GC to procure SaaS Solutions on an ongoing basis.

Secure

- Selection and alignment with the GC Cloud Security Standards.
- Leveraging industrial security standards available on the market.

Collaboration

- Leveraging a collaborative procurement process approach to facilitate the submission and qualification process.
- Enabling Multi-departmental contracts.

4. Protected SaaS Supply Arrangement Overview

The first phase consists of **qualifying suppliers** through the SaaS RFSA continuously posted on Buy and Sell . Qualified suppliers will be granted a Supply Arrangement.

The second phase consists of **awarding contracts** to Supply Arrangement holders via simplified bid solicitation or by issuing sole source contracts when all the mandatory justifications are met.

5. Standardized Evaluation Criteria (1/5)

The RFSA applies various standardized criteria to assess suppliers' ability to meet Canada's requirements, including:

Technical Criteria

- Qualification requirements
- Security & Privacy obligations
- Supplier's Service Level Agreement
- Submission Forms

Financial Criteria

- Indicative pricing + applicable discount rate
- Unit of Measure (e.g. 'per user', 'per usage' etc.)

Security & IT Certification Requirements

- Industrial Security Certifications (depending on Tiers)
- IT Assessment and Supply Chain Integrity Process

5. Standardized Evaluation Criteria (2/5)

Detailed Submission Process for the Financial Proposal

- ✓ Suppliers must submit Annex C - SaaS Solutions and Professional Services Ceiling Prices :
  - including applicable percentage discount
  - by completing the table in Annex C or by providing a link to commercially available SaaS catalogue
- ✓ Suppliers must provide a price support to demonstrate that their proposed prices are fair and reasonable.
- ✓ Suppliers now have the ability to leverage their own online price and products list with PSPC for review.

The intent is to minimize changes and accept companies' price and product lists.

5. Standardized Evaluation Criteria (3/5)

Annex C - SaaS Solutions and Professional Services Ceiling Prices

Option 1: Suppliers provide a link to their commercially-available SaaS Catalogue and indicate the percentage discount offered to the GC.

Option 2: Suppliers complete a table that includes product list and ceiling prices for SaaS solutions and professional services with other information such as units measures and applicable percentage discount.

5. Standardized Evaluation Criteria (4/5)

Collaborative Evaluation Process

1

The assessment process for RFSA Submissions will be a **collaborative process between PSPC and Suppliers**. Suppliers who do not meet all of the criteria to qualify will be contacted in order to request additional documentation or clarification.

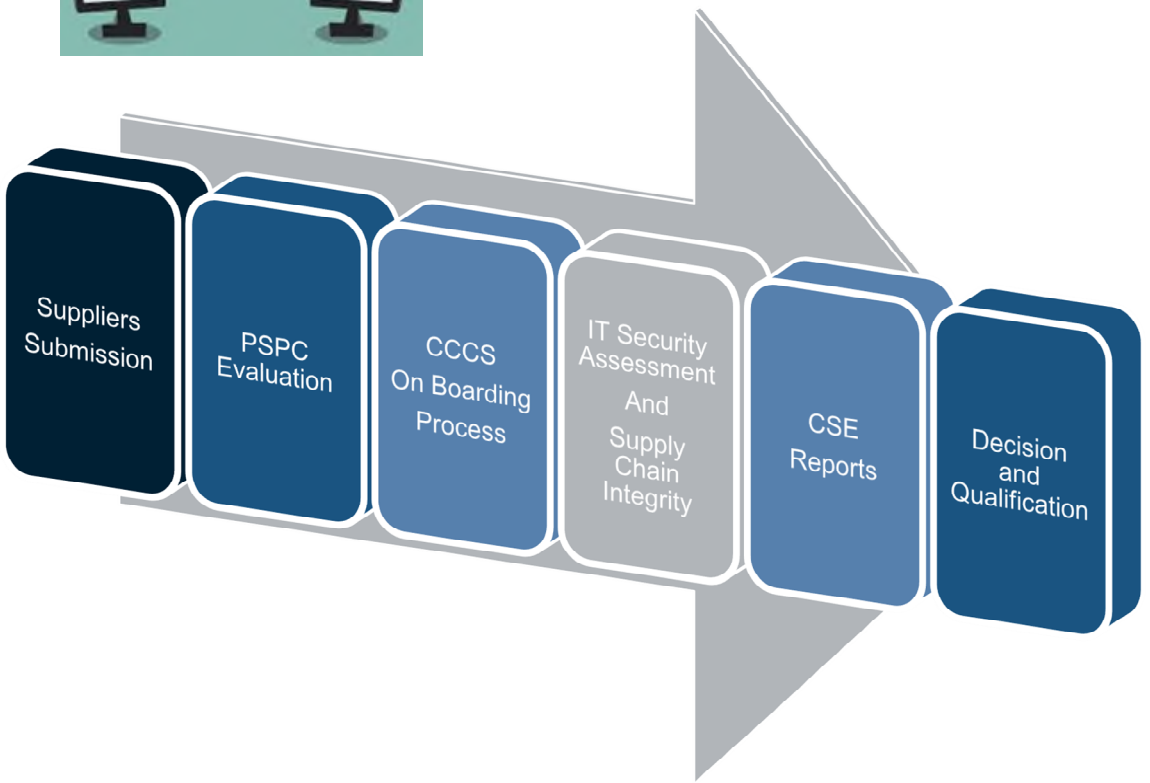
2

PSPC will review the documentation to ensure that the Supplier has submitted all the required documents and information. **The goal is to qualify as many Suppliers** as possible.

3

PSPC will assess the Submission against the defined evaluation qualification criteria.

PSPC has an arrangement with the Canadian Centre for Cyber Security to process **SCI assessment in parallel with the IT Security Assessment.**



5. Standardized Evaluation Criteria (5/5)

QUESTIONS? CONTACT US RIGHT NOW!

Collaborative process to support your submission and application.

For questions or to suggest revisions to the RFSA, suppliers can submit their feedback or questions to the RFSA email inbox: TPSGC.LENQS-SAAS.PWGSC@tpsgc-pwgsc.gc.ca

6. IT Security Assessment and SCI (1/2)

ITS Assessment Program :

The SaaS ITS assessment program examines all available evidence to satisfy the security controls and enhancements selected by the GC with toward an acceptable level of assurance for storing GC data.

The assessments may also rely on CSE's existing guidance, standards and reports from the GC and allied agencies, industry best practices, and commercial certifications. The use of these different resources will encourage SaaS providers to interact with the GC, third party auditors, and other assessment agencies to understand the IT security capabilities and the residual risks of cloud services used by the client departments.

Supply Chain Integrity (SCI) :

The supply chain integrity process is performed using the information requested in Form 6 by CSE. CSE will review, assess and evaluate the available information under a non-disclosure agreement. CSE will contact the Supplier directly if they have questions related to the assessment.

At the end of the process, a security report will be generated and the result shared with the consuming department.

6. IT Security Assessment and SCI (2/2)

Security Certification Requirements

Canada has taken the business decision to select the following combinations of industrial certifications to protect Canada's data and assets.

*Information Categorization - Up to **Protected B** (SaaS Publisher only)*

Security requirements (RFSA annex A)

- ISO/IEC 27001:2013
- ISO/IEC 27017:2015
- ISO/IEC 27018:2014
- Report (SOC) 2 Type II
- SCI - Evidence from ISO/IEC 27036, **or** NIST Special Publication 800-161, **or** ITSG-33 security, **or** CSA STAR controls to support CSA CCM Supply Chain Management controls.
- List of all sub-processors.
- PSPC CSP Inspection/Screening

*Information Categorization - Up to **Protected A** (SaaS Publisher and VARs)*

Security requirements (RFSA annex A)

- ISO/IEC 27001:2013 **or**
- SOC 2 Type II
- SCI - Evidence from ISO/IEC 27036, **or** NIST Special Publication 800-161, **or** ITSG-33 security, **or** CSA STAR controls to support CSA CCM Supply Chain Management controls.
- List of all sub-processors.
- PSPC CSP Inspection/Screening

***Suppliers are also required to meet the mandatory criteria within the RFSA and are required to provide other artefacts.**

7. Submission of Documents by Tiers

Documents	Tier 2 (SaaS Publisher Protected B)	Tier 1 (SaaS Publisher up to Protected A)	Tier 1 (Value-added Resellers up to Protected A Only)
Form 1- RFSA Submission Form	X	X	X
Form 2 – SaaS Publisher Certification Form	X	X	
Form 3 – SaaS Publisher Autorisation Form			X
OPTIONAL - Form – 4 Certification requirement for the Set-Aside Programs for Aboriginal business	X	X	X
Form 5 – Submission Completeness Review Check List	X	X	X
Form 6 – SCI Submission Template	X	X	
Annex A – Qualification Requirements Tier 1		X	X
Annex A – Qualification Requirements Tier 2	X		
Annex C – SaaS Solutions and Professional Services Ceiling Prices and Price support	X	X	X
If required: Financial Viability	X	X	X
Annex D – SaaS Solution Service Level Agreements (SLA)	X	X	X
If required: Forms for the Integrity - Declaration of Convicted Offences	X	X	X

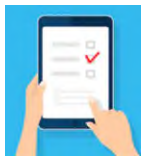
8. How to Participate? (1/2)

Step 1.Download the RFSA, amendments and associated documentation:

- https://buyandsell.gc.ca/procurement-data/tender-notice/PW-EEM-003-35660

Step 2.Select the stream under which you wish to participate

- SaaS Publisher Up to Protected B
- SaaS Publisher Up to Protected A
- Valued added Reseller Up to Protected A



Step 3.Complete your submission (details in slide 15)

- Providing artifacts demonstrating how you meet the mandatory technical, financial, security and Supply Chain Integrity requirements
- Ensure you have the latest SOC and ISO certifications and audit reports (within the last year).
- The submission process also involves completing multiple forms required by the RFSA.

Step 4.Send your submission

- Option 1 :E-Post Connect : https://www.canadapost.ca/cpc/en/business/postal-services/digital-mail/epost-connect.page
- Option 2 : Email: TPSGC.LENQS-SAAS.PWGSC@tpsgc-pwgsc.gc.ca

Having troubles? contact us at TPSGC.LENQS-SAAS.PWGSC@tpsgc-pwgsc.gc.ca

8. How to Participate? (2/2)

Outcomes of Awarding of Supply Arrangement

Supplier will be notified on the qualification result via email.

Supplier will be authorized to sell the SaaS products via the online Supply Arrangement to the client departments quickly and easily

Supplier will be added to the list of qualified suppliers, accessible by all client departments

Supplier will be able to update products list and pricing by notifying PSPC

Looking for help or update contact us at TPSGC.LENQS-SAAS.PWGSC@tpsgc-pwgsc.gc.ca

9. How Client Departments Procure Protected SaaS from SAs?

Step 1:

SaaS Solution(s) Identification

- Identify the applicable SaaS Solution(s) and Services through GC Catalogue or otherwise
- Establish the Statement of Requirements (SOR), if applicable

Step 2:

Issuance of simplified Bid Solicitation or justified sole source

- The Client or PSPC contracting authority will issue a simplified Bid Solicitation among qualified SA holders or sole source contracts if it is justified.
- Suppliers' submissions will be evaluated (if applicable).

Step 3:

Contract Award and Management

- Contract is signed with the Supplier Arrangement holder.
- SaaS usage & payment managed by client department.

10. Summary of the Presentation

- This is the way forward
- Get involve in the GC Digital Transformation
- Increase your GC Market presence
- Easy qualification process
- Leverage PSPC knowledge to qualify
- Flexible and business oriented
- Departments are eager to buy
- Accessible to municipal, provincial, academic, etc

END OF THE PRESENTATION

QUESTIONS AND ANSWERS

FEEDBACK

Supplemental information

New Limited Liability Clauses

First Party Liability:

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

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

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

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

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

(b) any breach of warranty obligations.

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