



Questions and Answer #4 – CIC-152202

New questions begin at Question #53

Question 1:	Would it be possible to obtain an Editable version (Unlocked) of the .xls files – not just the response column but the whole file so that we can copy and paste out various sections? Especially Appendix a – d.
Answer 1:	No. The versions of the .xls files will remain unchanged.

Question 2:	TBS and CSPS have deemed [name redacted] and the Learning Management System for the federal government. That service can either be either hosted in-house or Cloud based. Can I ask why the crown is going through this RFP process when the [name redacted] platform I thought was already a standard?
Answer 2:	There has been no statement from TBS or CSPS that defines a vendor as the Learning Management System for the Federal Government. A standard has not been developed as of yet.

Question 3:	<p>Section 1.2.1 states: For the purposes of this solicitation, Bidders must meet the security requirements identified under Tier 1 – Security Requirements for SaaS but may be asked to meet the Tier 2 – Security Requirements for SaaS following contract award.</p> <p>The SCRL (Security Requirement Checklist, P.54) very clearly shows only Protected A boxes checked. With that said, there is Appendix M which illustrates the requirements needed for Tier 2 at Protected B.</p> <p>Does Appendix M need to be met for the response of this RFP or is it here for reference only?</p>
Answer 3:	Bidders are required to meet the security requirements as specified in the SRCL as well as Appendix M – Tier 1 Security Requirements included within the RFP document. Appendix M – Tier 2 Security Requirement was included as an attachment for reference.

Question 4:	Section 1.2.1 states: For the purposes of this solicitation, Bidders must meet the security requirements identified under Tier 1 – Security Requirements for SaaS but may be asked to meet the Tier 2 – Security Requirements for SaaS following contract award.
--------------------	--



	<p>The SCRL (Security Requirement Checklist, P.54) very clearly shows only Protected A boxes checked. With that said, there is Appendix M which illustrates the requirements needed for Tier 2 at Protected B.</p> <p>If Protected B is not required for the initial project, what would the potential “triggers” be or timeframes in future to move from Protected A to Protected B status?</p>
Answer 4:	<p>The Contractor must demonstrate compliance with the security requirements selected in the GC Security Control Profile for Cloud-Based GC-IT Services for Protected B, Medium Integrity and Medium Availability (PBMM) within the initial contract period. The “trigger” will be the end of the initial contract period. IRCC would require the vendor to be assessed at the Protected B level by the Canadian Center for Cyber Security (CCCS) before the first option period is exercised. Amendment 001 of RFP CIC-152202.</p>

Question 5:	<p>Section 1.2.1 states: For the purposes of this solicitation, Bidders must meet the security requirements identified under Tier 1 – Security Requirements for SaaS but may be asked to meet the Tier 2 – Security Requirements for SaaS following contract award.</p> <p>The SCRL (Security Requirement Checklist, P.54) very clearly shows only Protected A boxes checked. With that said, there is Appendix M which illustrates the requirements needed for Tier 2 at Protected B.</p> <p>How is the vendor to identify pricing differentials between a Protected A solution and a Protected B solution? Should the vendor provide two pricing charts?</p>
Answer 5:	<p>Only one pricing chart should be submitted with a bid. All rates must be all inclusive of any expenditures required to fulfill the contract.</p>

Question 6:	<p>Part 3, Bid Preparation Instructions, Section 1: Technical Bid requires responses to both Appendix M and Appendix G. Are responses to both Appendices required?</p>
Answer 6:	<p>Yes. The technical bid must include a substantiation of compliance with Appendix M – Tier 1 – Security Requirements for SaaS and compliance with Appendix G – Security and Privacy Obligations.</p>

Question 7:	<p>Section 1.2.7, Accessibility states: Considering accessibility criteria and features is obligatory with this requirement. For additional information consult the Treasury Board Contracting Policy. Is this asking for written assurance that the vendor meets the accessibility requirements per the Treasury Board Contracting Policy or is this assumed with a bid submission and does not require a written response beyond what is required in ‘Annex A to Appendix D Statement of LMS Requirements’ in Section 11.0 Accessibility?</p>
--------------------	---



Answer 7:	IRCC does not require a formal written response beyond what is required in Annex A to Appendix D Statement of LMS Requirements.
------------------	---

Question 8:	APPENDIX N, PERIODIC USAGE REPORT indicates it is attached. C2.3 requires: The Contractor must provide this data in accordance with the reporting requirements detailed in Appendix N. Can you please provide Appendix N?
--------------------	---

Answer 8:	Appendix N is available for download as an attachment to the solicitation on BuyandSell.gc.ca.
------------------	--

Question 9:	<p>As per the pricing table found within the bid (page 49/117), the RFP suggests pricing based on 12,000 users. Page 40 of 117 (D4.2 c) suggests that the solution should <i>scale to at least 25,000 users</i> and in section 4.3 and B5.3 <i>that the number of users may be decreased</i> and Appendix E, 3. <i>The volumetric data included is provided for bid evaluation price determination purposes only. They are not to be used as a contract guarantee.</i></p> <p>Would IRCC consider amending the pricing Table 1 to reflect the table entirely to introduce an option for vendors to introduce minimum volume tiers to the pricing? (multiple lines for T1.2 based on volume tier). Or does Table 5 provide such option to show tiers?</p>
--------------------	--

Answer 9:	IRCC will not be amending Appendix E to allow for tier pricing. A per user price is required in both Table 1 and Table 5.
------------------	---

Question 10:	<p>As per the pricing table found within the bid (page 49/117), the RFP suggests pricing based on 12,000 users. Page 40 of 117 (D4.2 c) suggests that the solution should <i>scale to at least 25,000 users</i> and in section 4.3 and B5.3 <i>that the number of users may be decreased</i> and Appendix E, 3. <i>The volumetric data included is provided for bid evaluation price determination purposes only. They are not to be used as a contract guarantee.</i></p> <p>Will IRCC consider the volume tier as shown in T1.2 in Table 1 the minimum contract guarantee?</p>
---------------------	--

Answer 10:	The volumetric data included is provided for bid evaluation price determination purposes only and are not to be used as a contract guarantee.
-------------------	---

Question 11:	As per the pricing table found within the bid (page 49/117), the RFP suggests pricing based on 12,000 users. Page 40 of 117 (D4.2 c) suggests that the solution should
---------------------	--



	<p><i>scale to at least 25,000 users and in section 4.3 and B5.3 that the number of users may be decreased and Appendix E, 3. The volumetric data included is provided for bid evaluation price determination purposes only. They are not to be used as a contract guarantee.</i></p> <p>May the vendor provide an explanatory narrative to the pricing table?</p>
Answer 11:	<p>Bidders must provide in their financial bid a price breakdown as detailed in Appendix E, Basis of Payment.</p>

Question 12:	<p>4.1.(d).a: Canada reserves the right to reject any SaaS Solution proposed by a Bidder and enter into negotiation related to any prices under Appendix E, Basis of Payment.</p> <p>In what scenario would Canada reject the SaaS Solution by a Bidder while continuing to proceed with pricing as listed in Appendix E, Basis of Payment from the same Bidder?</p>
Answer 12:	<p>Negotiations could be entered in the scenario that only one compliant bid is received. Refer to Amendment 001 of RFP CIC-152202</p>

Question 13:	<p>Does IRCC intend to have a “source of truth” authentication system in front of the LMS? (such as an HRIS) If yes, what is the name of that authentication system?</p>
Answer 13:	<p>No. IRCC does not intend to have a “source of truth” authentication system in front of the LMS.</p>

Question 14:	<p>Will user information from the HRIS be modified in any way before it reaches the LMS to protect the identity of the individual entering the LMS?</p>
Answer 14:	<p>No. The LMS will not receive data from an HRIS.</p>

Question 15:	<p>Will IRCC expect to provide access to the LMS for non-IRCC employees? General public, etc.? If yes, please explain.</p>
Answer 15:	<p>No. Access to the LMS will be provided to IRCC employees.</p>

Question 16:	<p>In Part 3, article 3.3.(b) viii, “Bidders may provide a web site URL containing information on the SaaS Solution. “ This statement conflicts with the requirements to</p>
---------------------	--



	not include URLs in the bid. Please confirm if URLs are allowed anywhere in the bid or if the URLs are allowed only in the Financial Bid section.
Answer 16:	<p>When submitting the Technical Documentation to support the Bidder's response to each requirement identified in Annex A to Appendix D, URLs or links to websites are not acceptable. (Refer to Part 3, article 3.2 (c)v.).</p> <p>When submitting a response to the other requirements identified in the solicitation, Bidders may include URLs as indicated in the respective sections. See Amendment 001 to RFP CIC-152202.</p>

Question 17:	C8. Subcontracts. The Bidder intends to be the front line of all subcontracts (and therefore subcontractors) of the Solution. Please confirm when C8 would be in effect (whereby subcontractors' invoices (at cost) would go directly to IRCC for payment).
Answer 17:	There is no scenario in which C8. Subcontracts would apply. Refer to Amendment 001 to RFP CIC-152202.

Question 18:	D4.2.a – re: "platform and device-agnostic,.. without the need for any additional software" installation. The Solution requires the most up to date browsers to be installed on each device using the Solution. What browsers does IRCC use currently?
Answer 18:	IRCC uses Internet Explorer 11 and the latest Chrome browser.

Question 19:	D5.1 c.i.2 – Data Migration – please explain the existing learning system used by IRCC and the expectations of what data is to be migrated into the new LMS.
Answer 19:	IRCC will be batch importing data through the use of the LMS' own import tools/capacity. There is no interoperability requirement for data migration.

Question 20:	D5.1 c.ii.1 – Please confirm your expectations for live vs online training for the following LMS roles a. Administrators b. Instructors c. Learners
Answer 20:	



	Instructor-led moderated training is required for the LMS System Administrators only. Non-moderated, asynchronous training is required for all other roles.
--	---

Question 21:	<p>Re: Table 2 - Definition of a Day/Proration: 1. <i>All proposed personnel must be available to work outside of normal office hours during the duration of the Contract.</i></p> <p>Please confirm the scenarios at which the Bidder would need to provide professional services resources outside of 8am-5pm ET Monday - Friday.</p>
Answer 21:	Some services may be required across the country, and in rare instances, abroad (virtual). Personnel may be asked to provide the necessary services to accommodate local time zones.

Question 22:	If the Bidder does not have the required clearances at time of bid submission, will IRCC sponsor the Bidder to obtain such clearance?
Answer 22:	As indicated in Part 6, 6.1.1, The Security Requirements of the contract must be met before award of the contract. IRCC will not sponsor Bidders to obtain such clearance.

Question 23:	<p>Re: Data Isolation 8.a.ii.: The separation of customer resources in multi-tenant environments in order to prevent one malicious or compromised consumer from affecting the service or data of another;</p> <p>If a crypto key is used in order to separate IRCC's data from other tenants, would IRCC accept co-mingling IRCC data with other departments within the GoC that are also at Protected B using the same cryptographic key?</p>
Answer 23:	No, IRCC will not accept co-mingling data.

Question 24:	You have provided a table of delivery dates but there are no actual dates associated with this table. Does IRCC have a desired go-live date?
Answer 24:	IRCC requires Data and content integration to be delivered at 10 weeks following contract award. Closure of the project plan is expected at 20 weeks following contract award. Refer to Amendment 001 to RFP CIC-152202.



Question 25:	D.7 Official Languages: You have indicated that the Solution must be available and fully functional in both of Canada's official languages (English and French). All required documentation and support must also be available and provided upon request in both of Canada's official languages (English and French). Can IRCC confirm that this includes the provision of Administrator support in French?
Answer 25:	Yes. All required documentation and support must be available and provided upon request in both English and French.

Question 26:	<p>Regarding solicitation no. CIC-152202, "Cloud based Enterprise Learning Management System (LMS) for department wide use at Immigration, Refugees and Citizenship Canada", in the main RFP document,</p> <p>PART 7 - RESULTING CONTRACT CLAUSES, APPENDIX A, GENERAL TERMS AND CONDITIONS A3. General Conditions A3.1 General Conditions CIC-SI-001 (2016-05-26) Med/High Complexity Goods and Services Contract shall apply to and form part of this Contract.</p> <p>The link provided does not lead to the correct document. Can you provide the correct link so that we might review it?</p>
Answer 26:	<p>The link to <i>CIC-SI-001 (2016-05-26) Standard Instructions – Goods or Services Competitive Requirements</i>, can be found at the below address:</p> <p>https://www.canada.ca/en/immigration-refugees-citizenship/corporate/transparency/contract-terms-conditions/standard-instructions-goods-services-competitive-requirements-001-2016-05-26.html</p> <p>It is also referenced in Part 2 – Bidder Instructions, Section 2.1 – Standard Instructions, Clauses and Conditions within the Request for Proposal.</p> <p>The link to <i>CIC-GC-001 (2020-12-02) General Terms and Conditions – Medium/High Complexity Goods and Services Contracts</i> can be found at the below address:</p> <p>https://www.canada.ca/en/immigration-refugees-citizenship/corporate/transparency/contract-terms-conditions/general-terms-conditions-medium-high-complexity-goods-services-contracts-2020-12-02.html</p> <p>It is also referenced in Part 7 – Resulting Contract Clauses – Appendix A, General Terms and Conditions, section A3.1 within the Request for Proposal</p>

Question 27:	Section B.21 Liability: The proposed Resulting Contract Clauses included in Part 7 of the RFP contain no clause limiting the Contractor's liability for damages. A standard limitation of liability clause developed primarily by PWGSC is contained in contracts for IM/IT procurements. This limitation of liability clause reflects for the
---------------------	---



	<p>most part, a commercially reasonable allocation of risk between Canada and the Contractor in keeping with Treasury Board policy regarding Contractor liability in Crown procurements. Since this RFP describes an IM/IT procurement, we request that IRCC inserts the IM/IT limitation of liability SACC clause N0000C into the Articles of Agreement of the Contract which is available at the following web link: https://buyandsell.gc.ca/policy-and-guidelines/standard-acquisition-clauses-and-conditions-manual/5/N/N0000C/4</p>
Answer 27:	IRCC will not be including a limitation of liability clause within the RFP.

Question 28:	<p>B19.5 Price Certification - B19.6 Discretionary Audit and B3 - SACC Manual Clauses - C0705C 2010-01-11 - Discretionary Audit: A competitive RFP process that results in a comparison of rates proposed by more than one Bidder is the most fair, efficient, and effective means of determining the lowest price and best value to Canada, as the Bidder has to bid against competitors. Current policy in the Canadian Government for competitive RFPs indicates that clauses, such as the Price Certification and related Discretionary Audit provisions, apply only to non-competitive procurement process for goods and services over \$50,000. In this case, the RFP is competitive and has an evaluation methodology that establishes a competitive financial outcome.</p> <p>Canada is already protected by Section 14 Price Justification of the CIC-SI-001 (2016-05-26) Standard Instructions – Goods or Services - Competitive Requirements that governs the bid response. Therefore the price protection clause should not have been included in the Articles of Agreement. Given that this is a competitive process, inclusion of the Price Certification and Discretionary Audit clauses is inconsistent with the practice agreed to between Canada and Technation (previously known as ITAC) representing the IT community.</p> <p>As a result, the Price Certification and the related Discretionary clauses should not be required. Please remove Sections B19.5 Price Certification - B19.6 Discretionary Audit and B3 - SACC Manual Clauses - C0705C 2010-01-11 - Discretionary Audit from this RFP.</p>
Answer 28:	<p>Articles B19.5 and B19.6 will remain.</p> <p>SACC Manual Clauses C0705C has been removed from the solicitation. Refer to Amendment 001 to RFP CIC-152202.</p>

Question 29:	<p>Page 40 of 117, D 5.1 Fully Functional Solution: You say: "The contractor must provide the implementation deliverables presented below a) i. an average of 5,000 active users each month nationwide. " However, you state on page 4 of 123 that the solution is for 12,000 departmental users. Please specify the number of monthly users and the number of annual users, please?</p>
Answer 29:	The average active users is identified at 5000 per month, with a total of 12000 active users annually.



Question 30:	Page 40 of 123, D4.2 Requirements, c) you say: "... the solution must extend to at least 25,000 authorized users". Please specify how many users is the LMS targeting on an annual basis? Do you plan to increase subscription services to 25,000 authorized users upon exercise of the last option year of the contract?
Answer 30:	The LMS must be equipped to provide for 12,000 active subscriptions, annually. Over the length of the contract, IRCC may require an increase of subscriptions, up to a total 25,000 active users.

Question 31:	Page 36 of 123, point C4.2: "Monthly subscription fees and professional services: Canada will pay the contractor each month for work completed during the month in question Will you pay the contractor every month? months only work relating to the professional services described in a Task Authorization? Rather, will subscription services not be paid in full and in advance on an annual basis as stipulated on page 52 of 123, Price schedule: for subscription services,.... The entrepreneur will be paid annually and in advance the firm prices specified in tables 1 and 3?
Answer 31:	Professional services described in a Task Authorisation will be paid monthly, in arrears as per Annex E – Basis of Payment, Table 2 – List of Professional Services “as and when requested” during the initial contract period. For subscription services, as specified in Appendix E – Basis of Payment, Pricing Schedule, the all-inclusive firm unit price includes the provision of Software Documentation, Warranty, Hosting and Maintenance and Support related to the Learning Management System and described in Annex A to Appendix D - Statement of requirements, the Contractor will be paid the firm all-inclusive rates indicated in the Tables 1 and 3, payable yearly in advance. Refer Amendment 002 of RFP CIC-152202.

Question 32:	We ask you to extend the period of preparation of the proposals and to postpone the date of their submission to July 13 2021?
Answer 32:	IRCC will be extending the solicitation period by an additional 2 weeks. The bid closing date is July 6 2021 at 2:00pm EDT. Refer to Amendment 002 of RFP CIC-152202.

Question 33:	B14.1.f.iv. The per user pricing is based on a commercially reasonable amount of storage per user with additional storage available at reasonable rates. Based on the number of users for IRCC would IRCC please indicate the amount of storage it expects to use for the following volumes of users 7500, 12000, 25000.
Answer 33:	IRCC would expect no more than 2.5TB in total.

Question 34:	In the event that our proposal exceeds the 10MB file size, what alternative submission method can we employ?
Answer 34:	IRCC would accept multiple emails, should a bidder’s proposal exceed the 10 MB file size. Bidders should expect to receive an auto-reply when submitting an e-mail to the Bids Receiving email as indicated on Page 1 of the RFP. Should Bidders not



	receive an auto-reply, please contact the contracting authority immediately to make alternate arrangements.
--	---

Question 35:	<p>In Annex A to Appendix D, <i>3.3.7 Ability to inform the manager of a resource of shortages or conflicts</i></p> <p>Does this requirement refer to classrooms/materials/etc. or do you include learner/participant schedules in your requirements?</p>
Answer 35:	Point 3.3.7 of Annex A to Appendix D refers to classrooms/materials/etc.

Question 36:	<p>In Annex A to Appendix D, <i>9.5.9 Ability to meet industry standard targets for optimal performance and scalability</i></p> <p>Please define what IRCC means by “industry standard targets”?</p>
Answer 36:	By industry standards IRCC is referring to best practices, more specifically commercial or professional procedures that are accepted or prescribed as being correct or most effective.

Question 37:	<p>In Annex A to Appendix D, <i>3.4.10 Ability to view, update and delete a waiting list in waiting list repository</i></p> <p>Please clarify what you mean by “waiting list repository”?</p>
Answer 37:	The wait listing for registrations must be able to be managed.

Question 38:	<p>B5.3 Change in Consumption</p> <p>“The Contractor grants to Canada the irrevocable option to increase or decrease their consumption of the SaaS products or services detailed in Appendix D. Where Canada’s consumption of the SaaS products or services is decreased, the Contractor agrees that no penalties or increase in pricing per unit shall apply as a result.”</p> <p>This term/scenario as described is not aligned with SaaS tiered pricing models and will not be agreed to by our Legal Dept. Respectfully request that this be stricken from the RFP or altered accordingly.</p>
Answer 38:	Article B5.3 will remain unchanged.



Question 39:	<p>B6. Termination on Thirty (30) Days' Notice</p> <p>"1. Canada reserves the right to terminate the Contract at any time in whole or in part by giving thirty (30) calendar days written notice to the Contractor.</p> <p>2. In the event of such termination, Canada will only pay for costs incurred for services rendered and accepted by Canada up to the date of the termination. Despite any other provision of the Contract, there will be no other costs that will be paid to the Contractor as a result of the termination."</p> <p>Our company does not agree to a Termination for 'Convenience' as described above in B6. SaaS subscription terms are typically 1 year, 3 years, or 5 years. Respectfully request that this be stricken from the RFP or altered accordingly.</p>
Answer 39:	Article B6. will remain unchanged.

Question 40:	<p>B13.1 Software as a Service.</p> <p>"The Contractor will deliver the Solution through a Software as a Service ("SaaS") delivery model, allowing Canada to access and use the Solution which is hosted by the Contractor."</p> <p>Does your definition of Contractor (in the 'hosted by the Contractor' above) include sub-contractors?</p>
Answer 40:	"Contractor" means the entity named in the Contract to provide the Services and/or the Work to Canada.

Question 41:	<p>B13.5 Downgrade.</p> <p>"If the Contractor is unable to provide the Services with no less favourable features and functionality, the Contractor will provide written Notice to Canada identifying the circumstance, and alternative options, specifically including a reduction in pricing. If no proposed alternative option is acceptable to Canada, the Contractor agrees to consent to a termination of the Contract, and pay all identifiable direct costs incurred by Canada to migrate and store Client's Data, and to procure equivalent replacement services."</p> <p>Our company will not agree to the highlighted section of this clause. Respectfully request that this be stricken from the RFP or altered accordingly.</p>
Answer 41:	Article B13.5 will remain, unchanged.



Question 42:	<p>B14.1 Solution Services</p> <p>“(a) Software as a Service. The Contractor will provide all Services required for Canada to access and use the Solution as specified in Appendix D – Statement of Work and Annex A to Appendix D Statement of Requirements.”</p> <p>Our software company does not provide solutions as a function of an SOW. Is it your understanding that this is the role of the SI, not the software provider?</p>
Answer 42:	IRCC requires a contractor that can provide access to a solution that satisfies the requirements outlined in Appendix D – Statement of Work and Annex A to Appendix D Statement of Requirements.

Question 43:	<p>B14.1 (k) Data Retrieval</p> <p>“The Contractor agrees to make Canada’s data available for a minimum of 90 days after the end of the Contract to allow the Client sufficient time to migrate their data to a new environment, at no additional cost to Canada.”</p> <p>Our company offers an extension of your contract for up to 6 months with the same Terms & Conditions if more time is needed to complete the migration – but we do not agree to this clause as it is written (agreeing to make data accessible at no cost after a contract is expired. Respectfully request this be stricken from the RFP or altered accordingly.</p>
Answer 43:	Article B14.1 (k) will remain unchanged.

Question 44:	<p>B. 21 Limitation of liability</p> <p>“The Contractor is liable for any damage caused by the Contractor, its employees, subcontractors, or agents to Canada or any third party. Canada is liable for any damage caused by Canada, its employees or agents to the Contractor or any third party. The Parties agree that no limitation of liability or indemnity provision applies to the damages unless it is specifically incorporated in full text in the Articles of Agreement. Damage means any injury to persons (including injury resulting in death) or loss of or damage to property (including real property) caused as a result of or during the performance of the Contract.”</p> <p>While our company offers unlimited liability for specific topics, our general liability must be capped. Respectfully request this be rewritten to propose a cap or stricken from the RFP.</p>
Answer 44:	Please refer to Question 27.

Question 45:	<p>APPENDIX G – Security and Privacy Obligations</p> <p>8. Data Isolation, a, iii:</p>
---------------------	---



	<p>iii. Ability for the GC to support isolation within GC-managed tenant environment.</p> <p>Our cloud-based SaaS application is delivered through a multi-tenant architecture managed by our Cloud Operations. Within the application we enforce strict segregation of customer data at both the database and application server ties. The application cannot be installed or operated outside of our managed environment.</p> <p>Q. Is the GC referring to the 'hyper-scaler' tenant or the instance that the GC has control over within our tenant managed environment?</p>
Answer 45:	<p>Yes, enforcing strict segregation of customer data in all applicable ways (e.g., database, application servers) is an acceptable approach from an isolation perspective.</p>

Question 46:	<p>APPENDIX M – Tier 1 Security Requirements</p> <p>M14 Cryptographic Protection</p> <p>(a) Configure any cryptography used to implement confidentiality or integrity safeguards, or used as part of an authentication mechanism (e.g., VPN solutions, TLS, software modules, PKI, and authentication tokens where applicable), in accordance with Communications Security Establishment (CSE)-approved cryptographic algorithms and cryptographic key sizes and crypto periods;</p> <p>Can you explain what specific cryptographic algorithms and key sizes are required?</p>
Answer 46:	<p>The Communications Security Establishment (CSE)-approved cryptographic algorithms and key sizes are outlined in the following two Government of Canada guideline documents:</p> <p>ITSP.40.111 - Cryptographic Algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B Information https://cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-and-protected-b-information-itsp40111</p> <p>ITSP.40.062 - Guidance on Securely Configuring Network Protocols https://cyber.gc.ca/en/guidance/guidance-securely-configuring-network-protocols-itsp40062</p>

Question 47:	<p>Considering the magnitude and complexity of the RFP and our current workload, we request an extension, this will enable us to submit a response.</p>
Answer 47:	<p>Please refer to Question 32.</p>

Question 48:	<p>On page 9 as part of the Substantiation of Technical Compliance, the RFP states: "The Technical Bid must substantiate the compliance of the Bidder's LMS Service with Annex A to Appendix D - Statement of Requirements." Our confusion is with the</p>
---------------------	---



	<p>wording of this; it appears that only the Excel spreadsheet should be used to demonstrate compliance along with documentation/substantiation to items in the spreadsheet.</p> <p>There are items in Appendix D Statement of Work (starting on page 38) that are not specifically covered in the Annex A to Appendix D – Statement of Requirements spreadsheet (for example, D.5.1 (b), including but not limited to implementation plan, communication plan, training, support, etc.)</p> <p>Do you want written responses to items D4.2 Requirements to item D.9 Availability of Personnel (noting D.10 Diversity is included in Annex A to Appendix D - Statement of Requirements)?</p>
Answer 48:	Bidders are to provide responses to substantiate compliance with “Annex A to Appendix D Statement of Requirements” and not Appendix D Statement of Work.

Question 49:	Regarding section B21. Liability, we respectfully request the inclusion of a mutually-acceptable limitation of liability in the contract documents, as is customary in our industry. Would it be possible to agree in advance that such a clause may be included?
Answer 49:	Please refer to Question 27.

Question 50:	<p>Related to PART 7 - RESULTING CONTRACT CLAUSES, APPENDIX A, GENERAL TERMS AND CONDITIONS: You reference in A1.1 the SACC Manual and in A1.2 you reference the Contract Terms and Conditions on the IRCC Website. Then, in A3. General Conditions, A3.1 General Conditions you reference CIC-GC-001 (2020-12-02), Med/High Complexity Goods and Services Contract. Can you please specify the exact Terms and Conditions that will apply to this contract? Is it just CIC-GC-001 (2020-12-02), Med/High Complexity Goods and Services Contract?</p> <p>Alternatively, if any of the terms from the SACC or IRCC website apply, can you please specify exactly which ones would form part of the contract?</p>
Answer 50:	<p>In Part 7, articles A1.1 and A1.2 have been provided for reference purposes. The general terms, conditions that apply to the contract are A3.1 General Conditions CIC-GC-001 (2020-12-02), Med/High Complexity Goods and Services Contract.</p> <p>Supplemental clauses, either from the SACC Manual or the IRCC Website, are identified and referenced in Appendix B.</p>

Question 51:	Does IRCC have a number you can share of total the annual sessions that will require Resource Management components/functionality (e.g. in person seminars requiring rooms and equipment or virtual seminars requiring instructors to be assigned)?
Answer 51:	This information is not available at this time.



Question 52:	In Annex A to Appendix D Requirements spreadsheet, regarding requirement 3.2.17 (Table A), "Ability for various roles to override scheduling conflicts for a class/session," are you referring to overriding a learner scheduling conflict or a conflict with a resource (e.g. classroom)?
Answer 52:	This is in reference to a conflict with a resource.

Question 53:	Page 106 of 117, Mandatory Requirement ID M7, Supply Chain Risk Management: You say, "To be found compliant, the documentation provided must demonstrate the supplier's compliance with one of the three following standards: 1. ISO 27036 2. NIST Special Publication 800-161 or 3. ITSG-33 Security Controls Catalog. Is it absolutely mandatory to have one of the three standards mentioned when submitting a proposal? Is it possible for a supplier to present only one of the listed standards to you within 12 to 18 months of contract award?"
Answer 53:	No. In order to be deemed compliant, prior to contract award, the bidder must provide documentation to demonstrate compliance with one of three standards as mentioned Appendix M – Tier 1 Security Requirements for SaaS, M7. It cannot be submitted after contract award.

Question 54:	Page 104 of 117, Mandatory Requirement ID M5, Third Party Assurance: You say, "The supplier must present the following industry certifications to demonstrate compliance of the service offered: 1. i. ISO 27001: 2013, ii. SOC 2 type II, 2. Self-assessment of its services against version 3.01 (or later) of the Cloud Security Alliance (CSA) Cloud Controls Matrix (MC) ": Is it possible for a provider to present only one of the three certifications mentioned here? Is it possible for a supplier to present one of the listed standards to you within 12 to 18 months of contract award?"
Answer 54:	The bidder must submit either ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems – Requirements; or AICPA Service Organization Control (SOC) 2 Type II, as well as a Self-assessment of its services against the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) version 3.01 or subsequent version. Bidders must submit the certifications prior to contract award in order to be deemed compliant.



Question 55:	<p>In Annex A to Appendix D, <i>3.2.15 Ability for wait-listed learner to accept an offered seat within a specified time limit</i></p> <p>Our system automatically either accepts wait-listed users once a spot becomes available, or once an admin has accepted them. If IRCC manages the waitlist with admin intervention, then this requirement can be met. Is this acceptable to IRCC?</p>
Answer 55:	<p>Yes, an automatically controlled wait-list is acceptable. Refer to Amendment 001 to Annex A to Appendix D, Table A.</p>

Question 56:	<p>In Annex A to Appendix D, <i>3.3.7 Ability to inform the manager of a resource of shortages or conflicts</i></p> <p>Do you mean “Ability to inform the manager of a resource shortage or conflict”?</p>
Answer 56:	<p>Yes. Table A, point 3.3.7 of Annex A to Appendix D refers to the ability to inform the manager of a resource shortage or conflict. Refer to Amendment 001 to Annex A to Appendix D.</p>

Question 57:	<p>In Annex A to Appendix D, <i>3.2.8 Ability to capture a user's accommodation requirement at registration (for delivery of learning)</i></p> <p>Does this have to be done automatically via the registration process or is it sufficient that this can be done in the user profile?</p>
Answer 57:	<p>The ability to capture a user’s accommodation requirement in the user profile is sufficient. Refer to Amendment 001 to Annex A to Appendix D, Table B.</p>

Question 58:	<p>APPENDIX G – Security and Privacy Obligations</p> <p>13. Key Management</p> <p>e. Ability to securely import GC generated keys from GC-managed on-premise hardware security module (HSM) without exposure of key plaintext during the import process;</p> <p>f. Ability to prevent the Cloud Service Provider to recover plaintext copies of the GC generated keys;</p> <p>Our company encrypts all Data at Rest with AES 256-bit encryption by default. We manage the encryption keys as part of the service and our key management system has passed the FIPS 140-2 certification testing. We request that any reference to “GC generated and managed keys” be removed from the RFP.</p>
Answer 58:	<p>Appendix G, Article 13 – Key management will remain unchanged.</p>



Question 59:	<p>APPENDIX G – Security and Privacy Obligations</p> <p>21. Logging and Auditing</p> <p>b. The Contractor must provide the ability for Canada to export security event logs using standardized reporting interfaces, protocols, and data formats (e.g. Common Event Format (CEF), syslog, or other common log formats) and APIs that support log data remote retrieval (e.g. via a database interface using SQL, etc.), for the Cloud Services it consumes, in support of GC operations including monitoring of the Cloud Services and for e-discovery and legal holds.</p> <p>All critical systems and infrastructure components within our Cloud need to log relevant data. This is enabled via the security configuration compliance checks and event monitoring. General security monitoring is performed 24x7 for all activities. We do not share the infrastructure logs, or provide the ability to export security event logs, with our customers. We respectfully request that this be stricken from the RFP.</p>
Answer 59:	Appendix G, Article 21 – Logging and Auditing will remain unchanged.

Question 60:	<p>APPENDIX M – Tier 1 Security Requirements</p> <p>M13 Information Spillage</p> <p>2) The Supplier must provide an up-to-date information spillage process to Canada on an annual basis, or promptly following any Change to the Supplier’s information spillage process.</p> <p>Our internal processes are confidential and not released to customers. We respectfully request that this be stricken from the RFP.</p>
Answer 60:	Appendix M, Article M13 – Information spillage will remain unchanged.

Question 61:	<p>APPENDIX M – Tier 1 Security Requirements</p> <p>M13 Information Spillage</p> <p>a) System documentation or technical documentation outlining and detailing the security measures including policies, processes and procedures that are implemented for the protection of Information Spillage.</p> <p>Our policies, processes and procedures are confidential and proprietary and will not be released. We respectfully request that this be stricken from the RFP.</p>
Answer 61:	Appendix M, Article M13 – Information spillage will remain unchanged.

Question 62:	Annex A to Appendix D, Table A - relating to item: 2.2.2 (Two-factor authentication): Can you please confirm (yes or no) that IRCC has its own authentication system that users must sign into first prior to launching the LMS?
Answer 62:	No, IRCC does not have its own authentication system that users must sign into first prior to launching the LMS.



Question 63:	Substantiating our ability to meet Protected A and B requires information we will only share under NDA. Please confirm how we may respond to all items in Appendix M in lieu of NDA not being in place at time of RFP submission.
Answer 63:	If a bidder requires an NDA in order to provide a response to Appendix M, the bidder should notify the contracting authority in writing prior to bid closing. The contracting authority will then provide the bidder with a signed NDA.

Question 64:	In APPENDIX G, p.71 of 117, point 4, b): you say: “The contractor must demonstrate that the measurements comply with the stated requirements.... Including: i) ISO / IEC 27001: 2013, ii) ISO / IEC 27017: 2015 based on ISO / IEC 27002 and (SOC) 2 type II carried out 12 months before the contract accompanied by the evaluation report prepared to validate compliance with ISO certification... the Contractor must maintain ISO 27001, ISO 27017 and SOC 2 Type II certifications for the duration of the contract. Are these three certifications absolutely necessary for a supplier to be able to respond to the request for proposal mentioned in the subject? Is it possible for a supplier to present you with only one of the three mentioned certifications, for example ISO 27001: 2013, and be authorized to respond to the request for proposal in question?
Answer 64:	As per Section 3.2 – Section I: Technical Bid, sub-article c) vii. Compliance with Appendix G – Security & Privacy Obligations , Bidders must demonstrate that they meet the security and privacy obligations detailed in Appendix G by responding to the mandatory requirements detailed in Appendix M – Tier 1 Security Requirements for SaaS. Suppliers may be requested to demonstrate their ongoing compliance with Annex G – Security and Privacy Obligations upon request through the period of the contract. Refer to Amendment 003 to RFP CIC-152202.

Question 65:	Page 105 of 117, Mandatory Requirement ID M6, Supply Chain Management: You say, “For SaaS, the contractor must demonstrate that IaaS / PaaS is leveraged by these services: a) the suppliers' sub-processors have been assessed in accordance with the CCCS program, and b) the supplier complies with the security obligations of the sub-processors... ”. To be eligible to submit a proposal with respect to the above mentioned request for proposal, is it required at the time of submission of the proposal to demonstrate that the sub-processors have been evaluated in accordance with the CCCS program? Is it possible to demonstrate this requirement after contract award?
Answer 65:	To be deemed compliant with Appendix M – Tier 1 – Security Requirements for SaaS, M6, prior to contract award, the Bidder must demonstrate the supplier sub-processors have been assessed by the CCCS program in order to be deemed compliant with this requirement. This cannot be submitted after contract award.



Question 66:	<p>APPENDIX M – Tier 1 Security Requirements M6 Supply Chain Management</p> <p>(1) For SaaS, the Contractor must demonstrate that the IaaS/PaaS leveraged by the Services: (a) Supplier Sub-processors have been assessed by the CCCS Program as per; and</p> <p>The software vendor does not control the CCCS program on behalf of its sub-processors (of which there can be multiple pages of entries) — it is the responsibility of the sub-processor to engage in the process, as the information required is extremely sensitive, proprietary, and confidential.</p> <p>Please clarify the expectation on the successful bidder in regards to the CCCS audit program as it relates to sub-processors? Because the clause referenced above mentions ‘have been assessed’ (implying that all sub-processors will have already been assessed at time of bid) – is this interpretation correct?</p>
Answer 66:	Please refer to Question and Answer #65

Question 67:	<p>In Annex A to Appendix D, <i>9.5.9 Ability to meet industry standard targets for optimal performance and scalability</i> How are these measured to determine ‘meet/does not meet’?</p>
Answer 67:	Bidders will be deemed compliant with 9.5.9 if they can demonstrate that they perform regular (at a minimum once a year) load testing that includes response rates to ensure their solution supports an increase in the number of users/transactions without impacting performance.

Question 68:	<p>B16.3 Notifications Required for Tier 1 (Protected A) and Tier 2 (Protected B) requirements.</p> <p>Please explain why security levels are connected to SLA’s?</p>
Answer 68:	Security levels are not connected to SLA’s. Refer to Amendment 003 to RFP CIC-152202.

Question 69:	<p>APPENDIX M – Tier 1 Security Requirements M5 Third Party Assurance</p> <p>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</p> <p>2) Self-assessment of its services against the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) version 3.01 or subsequent version.</p> <p>We are audited to ISO27001, ISO27017, ISO27018 and SSAE18 Trust Services Criteria. We are certified according to ISO 27001, ISO27017, ISO27018, ISO 22301,</p>
---------------------	---



	and BS 10012. We utilize independent external auditors and industry accepted standards instead of self-certification. Self-certification approaches have proven to be inadequate in the past. For example, the recent Schrems II decision by The Court of Justice of the European Union ("CJEU") that invalidated EU-US Privacy Shield. Are the audits and certifications that we maintain acceptable to GC? If so, we request that the self-assessment requirement described in 2) be stricken from the RFP.
Answer 69:	Yes, utilizing independent external auditors is acceptable. Refer to Amendment 003 to RFP CIC-152202.

Question 70:	B12.2.e and B14.1f2: providing incidental and additionally required information technology infrastructure services In what scenario would IRCC need additional cloud services beyond the cloud services needed for the hosting of the Solution being provided by the Bidder?
Answer 70:	<p>With regards to B12.2 (e), <i>Providing incidental and additional required information technology infrastructure services</i> IRCC requires details on what IT infrastructure is needed by the vendor, whether IRCC has that setup in our PBMM Cloud environment or internally and if they are a potential for SA&A non-compliance.</p> <p>With regards to B14.1 (f) ii., provision of all incidental and additional required information technology infrastructure services in compliance with all required security standards. Without this, it can take up to two years for a vendor to obtain GC certification on secure:</p> <ul style="list-style-type: none"> i. Partitioning of network, protocols, bandwidth, and channels, ii. Infrastructure - Data Center for IaaS, PaaS, or SaaS configuration, iii. Secure zone classification of Data Center Zones, iv. Data Center security classification through evidence and visits v. Various ISO certifications, vi. Data and application residency in Canada only, vii. Evidence of all vendor's developers, application support, and engagement managers are eligible for confidential or in some cases Secret clearances.

Question 71:	We respectfully request a 4 week extension to provide enough time to prepare a fulsome proposal response.
Answer 71:	Refer to Question and Answer #32.