Citizenship and Immigration Canada | Citoyenneté et Immigration Canada

RETURN BIDS TO:

IRCC.BidsReceiving-Receptiondessoumissions.IRCC@cic.gc.ca

Attn: Jasdeep Jande

FOR ELECTRONIC BIDS:
The electronic mailbox is equipped to send an automatic reply to all messages received. If you do not receive an automatic response, please contact the Contracting Authority to ensure your bid was received. Please note that it is the bidder's sole responsibility to ensure that all bids submitted are received in their entirety by Citizenship and Immigration Canada by the closing date and time indicated in this RFP.

IMPORTANT NOTICE TO SUPPLIERS
The Government Electronic Tendering Service on buyandsell.gc.ca/tenders will be the sole authoritative source for Government of Canada tenders that are subject to trade agreements or subject to departmental policies that require public advertising of tenders.

REQUEST FOR PROPOSAL
Proposal To: Citizenship and Immigration Canada
We hereby offer to sell to Her Majesty the Queen in right of Canada, in accordance with the terms and conditions set out herein, referred to herein or attached hereto, the goods, services, and construction listed herein and on any attached sheets at the price(s) set out thereof.

THIS DOCUMENT CONTAINS A SECURITY REQUIREMENT

Instructions : See Herein
Instructions: Voir aux présentes
Issuing Office – Bureau de distribution
Citizenship and Immigration Canada
Procurement and Contracting Services
70 Crémazie
Gatineau, Québec K1A 1L1

Title – Sujet Cloud based Enterprise Learning Management System (LMS) for department wide use at Immigration, Refugees and Citizenship Canada	
Solicitation No. – N° de l'invitation **CIC-152202**	**Date** **June 24 2021**
Amendment No. – N° de modification **003**	
Solicitation Closes – L'invitation prend fin at – à *2:00* **PM** **on – July 6 2021**	**Time Zone** **Fuseau horaire** **EDT**
F.O.B. - F.A.B. **Plant-Usine:** ☐ **Destination:** ☐ **Other-Autre:** ☐	
Address Inquiries to: - Adresser toutes questions à : **IRCC.BidsReceiving-Receptiondessoumissions.IRCC@cic.gc.ca**	
Telephone No. – N° de téléphone : **343-574-4425**	
Destination – of Goods, Services, and Construction: **Destination – des biens, services et construction :** See Herein	
Delivery required - Livraison exigée ***See Herein***	
Vendor/firm Name and address **Raison sociale et adresse du fournisseur/de l'entrepreneur** **Facsimile No. – N° de télécopieur** **Telephone No. – N° de téléphone**	
Name and title of person authorized to sign on behalf of Vendor/firm **Nom et titre de la personne autorisée à signer au nom du fournisseur/de l'entrepreneur** _____ **(type or print)/ (taper ou écrire en caractères d'imprimerie)** _____ _____ **Signature** **Date**	

Canada

Amendment 003 – RFP CIC-152202

Amendment 003 is raised to:

1. **Update Part 3 – Bid Preparation Instructions;**
2. **Update Part 5 – Certifications and Additional Information;**
3. **Update Appendix B – Supplemental Terms and Conditions**
4. **Update Appendix D – Statement of Work;**
5. **Update Annex A to Appendix D – Statement of IRCC LMS Requirements**
6. **Update Appendix G – Security and Privacy Obligations;**
7. **Update Appendix H – Supply Chain Integrity Process;**
8. **Update Appendix K – Non-Disclosure Agreement**
9. **Update Appendix M – Tier 1 – Security Requirements for Saas;**
10. **Update Appendix M – Tier 2 – Security Requirements for SaaS; and**
11. **Update Appendix L – SaaS IT Security (ITS) Assessment Program: Onboarding Process**

1. PART 3 – BID PREPARATION INSTRUCTIONS

Sub article 3.2 c) vii Compliance with Appendix G – Security & Privacy Obligations is deleted in its entirety and replaced with:

vii **Compliance with Appendix G – Security & Privacy Obligations:** Bidders must comply with security and privacy obligations contained in Appendix G – Security & Privacy Obligations. Bidders must demonstrate that they meet the security and privacy obligations detailed under 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 Appendix G – Security & Privacy Obligations upon request throughout the period of the Contract.

2. PART 5 – CERTIFICATIONS AND ADDITIONAL INFORMATION

Sub article 5.2.4 *Confirmation of Registration for the SaaS IT Security (ITS) Assessment* is deleted in its entirety.

3. APPENDIX B, SUPPLEMENTAL TERMS AND CONDITIONS

Sub article B16.3 e) is deleted in its entirety.

4. APPENDIX D, STATEMENT OF WORK

Sub article D6. Limitations and Constraints is deleted in its entirety and replaced with:

D6. Limitations and Constraints

The Contractor must meet the security requirements outlined in the ***Government of Canada Security Control Profile for Cloud-Based GC Services****(https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/government-canada-security-control-profile-cloud-based-it-services.html)*, which is a comprehensive set of guidelines and controls based on ITSG-33. The Contractor's Solution must meet the *Government of Canada Security Control Profile for Cloud-Based GC Services* by providing one of the following:

a. A valid SOC-2 or SOC-3 report (ISAE-3402);
b. ISO-27001 Certification;
c. Compliance with U.S. National Institute of Standards and Technology (NIST) Publication 800-53;
d. Within the initial contract period, the Contractor must demonstrate compliance with Appendix M - Tier 2, Security Requirements for SaaS.

5. ANNEX A TO APPENDIX D – STATEMENT OF IRCC LMS REQUIREMENTS

Annex A to appendix D has been updated. Please refer to Amendment 001 of Annex A to appendix D, included as an attachment.

6. APPENDIX G – SECURITY AND PRIVACY OBLIGATIONS

Appendix G, sub article 6 – Cloud Service Provider (CSP) IT Security Assessment program is deleted in its entirety and replaced with:

6. Cloud Service Provider (CSP) IT Security Assessment Program

a Within the initial contract period, the Contractor must demonstrate compliance with the security requirements selected in the GC Security Control Profile for Cloud-Based GC IT Services for Protected B, Medium Integrity and Medium Availability (PBMM) (https://www.canada.ca/en/government/system/digital-government/modern-emergingtechnologies/cloud-computing/government-canada-security-control-profile-cloud-based-itservices.html) for the scope of the Cloud Services provided by the Contractor. Compliance must be demonstrated through the mapping of security controls to the applicable industry certifications identified below, and validated through independent third party assessments.

b Compliance will be assessed and validated by IRCC.in accordance with CCCS guidelines for localized IT security Assessments. https://cyber.gc.ca/en/guidance/cloud-service-provider-information-technology-security-assessment-process-itsm50100).

It is the continuous obligation of the Contractor of the proposed Cloud Services to notify IRCC when there are significant changes to its delivery of the IT Security services supporting the Contractor offering.

Certifications identified below, and validated through independent third party assessments.

c In the situation where the Contractor is a SaaS provider using a GC-approved IaaS Provider that already complies with Section 4 - Third-Party Assurance and Section 6 - Cloud Service Provider (CSP) IT Security Assessment Program, sub-sections (1) and (2) the SaaS provider must provide Canada with a copy of an email provided by the Canadian Centre for Cyber Security (CCCS) confirming that the Contractor has completed the CCCS CSP ITS Assessment Program. The email must state that the CSP has been assessed by the CSP ITS Assessment Program and that the CSP has received a final report with regards to the assessment.

7. APPENDIX H – SUPPLY CHAIN INTEGRITY PROCESS

Appendix H sub article 1.1 is deleted in its entirety and replaced with:

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

1.1.1. **IT Product List:** Contractors must identify the SaaS Solution over which Canada's Data would be transmitted and/or stored that will be used and/or installed to perform any part of the Work and/or Services described in the resulting contract. In regards to the SaaS Solution, by completing the Form 3 - SCI Submission Template as provided in the RFP, which includes following information :

a. **OEM Name:** Enter the name of the original equipment manufacturer (OEM) of the product that is being ordered.
b. **OEM DUNS Number:** Enter the DUNS number of the OEM. The Data Universal Numbering System (DUNS) is a unique nine-digit number assigned to each physical location of a businesses. It is a worldwide standard and is used to determine the credit score of a company. If the company does not have a DUNS number, or you are unable to find one, please fill out the requested information on "C – Ownership Information". ownership information consists of the top 5, by percentage, investors and owners of the company. The names provided for investors and owners should be those found in investment or ownership documents for the company in question.
c. **Product Name:** Enter the OEM's name for the product.
d. **Model Number:** Enter the OEM's model and/or version number of the product.
e. **Product URL:** Enter the URL of the OEM's webpage for the product.
f. **Vulnerability Information:** Enter information concerning the last 5 security issues that were reported about the product. If the OEM posts this information to the CVE website, list the CVE numbers separated by semi-colons (;). If the OEM does not post this information to the CVE website, you will need to ask the OEM directly for security vulnerability information and **provide this information to IRCC**. If this is the case for a particular product, enter "see attached information" in the Vulnerability Information field, and include the filename(s) in the additional information column which provide the required vulnerability information.

8. APPENDIX K – NON-DISCLOSURE AGREEMENT

Appendix K – Non-Disclosure Agreement is hereby deleted in its entirety and replaced with:

APPENDIX K, Non-Disclosure Agreement

Note to Contractors: Please note that this Non-Disclosure Agreement only covers Supply Chain Integrity requirements under Article 3.6, Section IV Supply Chain Integrity Requirements.

Non-Disclosure Agreement

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

1. The Contractor agrees to keep confidential any information it receives from Canada regarding Canada's assessment of the Contractor's Supply Chain Security Information (the "**Sensitive Information**")

including, but not limited to, which aspect of the Supply Chain Security Information is subject to concern, and the reasons for Canada's concerns.

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

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

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

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

9. APPENDIX M – TIER 1 SECURITY REQUIREMENTS FOR SAAS

Appendix M Mandatory ID M5 – Third Party Assurance is deleted in its entirety and replaced with:

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	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 for the proposed Service to demonstrate compliance: 1) 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 2) Self-assessment, or assessments by external auditors, 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: a) Be valid as of the Submission date; b) Identify the legal business name of the proposed Supplier, and applicable Supplier Sub-processor, including CSP; 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. e) 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 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 management system standard. Please note: • Certifications must be provided for all portions of the proposed Service identified • Certifications must be accompanied by assessment reports. • Certifications must be valid and within the 12 months prior to the start of a contract

10. APPENDIX M – TIER 2 SECURITY REQUIREMENTS FOR SAAS

Appendix M Mandatory ID M8 – Third Party Assurance is deleted in its entirety and replaced with:

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,	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 to demonstrate compliance: 1) ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems – Requirements; and

		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 in accordance with CCCS gudelines for localized IT security Assessments. 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 demonstrate the compliance	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 or 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. 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.

11. APPENDIX L – SAAS IT SECURITY (ITS) ASSESSMENT PROGRAM: ONBOARDING PROCESS

Appendix L – SaaS IT Security (ITS) Assessment Program: Onboarding Process is deleted in its entirety.

ALL OTHER TERMS AND CONDITIONS REMAIN THE SAME.