SHARED SERVICES CANADA

Amendment No. 007 to Invitation to Qualify for Government of Canada Cloud Service Procurement Vehicle (GC Cloud)

Solicitation No.	32099	Date	November 7, 2018
GCDocs File No.		GETS Reference No.	PW-18-00841719

This Amendment is issued to modify the ITQ solicitation documentation. Except as expressly amended by this document, all the terms and conditions of the ITQ remain unchanged.

THIS SOLICITATION AMENDMENT IS ISSUED TO:
1. Modify the Invitation To Qualify. 2. Provide a revised copy of Annex J NOTE: Respondents' clarification questions are numerically sequenced upon arrival at SSC. Respondents are hereby advised that questions and answers for this solicitation may be issued via BuyandSell.gc.ca out of sequence.

1. MODIFICATIONS TO THE INVITATION TO QUALIFY (ITQ)

The following modifications are applicable to the solicitation documents released in Amendment 005 on October 29, 2019. Please note the following:

- All modifications are shown in the highlighted text.
- All modifications shown in highlight with red strikethrough (~~xxxxx~~) should be considered redacted as part of the modification.
- Non highlighted text should not be considered as part of the modification.

Modification 1 – **On page of 14 the ITQ, Section 3.3 (e)**

DELETE

Please Note: Responses to **Annex A, Appendix 1 – Part A** and **Annex A, Appendix 2 –Part A** must be submitted to Shared Services Canada (SSC) at the following email address ~~ssc.cloudsolicitationsollicitationinfonuagiques.spc@canada.ca~~

INSERT

Please Note: Responses to **Annex A, Appendix 1 – Part A** and **Annex A, Appendix 2 –Part A** must be submitted to Shared Services Canada (SSC) at the following email address ssc.cloudsolicitation-sollicitationinfonuagiques.spc@canada.ca

Modification 2 – **On page of X the ITQ, Section 3.3 (g)**

DELETE

Please Note: Responses to ~~**Annex A, Appendix 1 –Part B** and **Annex A, Appendix 2 –Part B**~~ must be submitted to Shared Services Canada (SSC) at the following email address ~~ssc.cloudsolicitationsollicitationinfonuagiques.spc@canada.ca~~

INSERT

Please Note: Responses to **Annex A, Appendix 3** must be submitted to Shared Services Canada (SSC) at the following email address ssc.cloudsolicitationsollicitationinfonuagiques.spc@canada.ca

Modification 3 – **On page of 49 the ITQ, Annex J - ATTESTATION OF MANDATORY REQUIREMENT FOR PRICING IN CANADIAN DOLLARS**

DELETE

(_____), acknowledge Canada's mandatory requirement identified in ~~M5~~, which identifies a need for the proposed Commercially Available Public Cloud Service

INSERT

(_____), acknowledge Canada's mandatory requirement identified in Annex A (Appendix 1 – M6 | Appendix 2 – M4), which identifies a need for the proposed Commercially Available Public Cloud Service

Modification 4 – **On page 1 of the ITQ, Annex A, Appendix 1**

DELETE

Responses to **Annex A, Appendix 1 – Part A** must be submitted to Shared Services Canada (SSC) at the following email address by the solicitation closing date – ~~ssc.cloudsolicitationsollicitationinfonuagiques.spc@canada.ca~~

INSERT

Responses to **Annex A, Appendix 1 – Part A** must be submitted to Shared Services Canada (SSC) at the following email address by the solicitation closing date – ssc.cloudsolicitation-sollicitationinfonuagiques.spc@canada.ca

Modification 5 – **On page 4 of the ITQ, Annex A, Appendix 1**

DELETE - M5 in its entirety

INSERT

M5	General	The Cloud Service Provider (and if applicable the Alternative Service Provider)of the proposed Commercially Available Public Cloud Service must have the ability to protect the confidentiality, integrity and availability of GC Master Account information and credentials used to establish the GC cloud environment. This includes ensuring that credentials remain within the geographic boundaries of Canada.	The Respondent must demonstrate compliance by providing documentation outlining the Cloud Service Provider's (and if applicable the Alternative Service Provider) ability to protect the confidentiality, integrity and availability of GC Master Account information and credentials used to establish the GC cloud environment. To be considered compliant, the provided documentation must include: a) System documentation or white paper that outlines the policies, processes and procedures used to protect the confidentiality, integrity and availability of GC Master Account information and credentials used to establish the GC cloud environment. The substantiation required for M5 cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Cloud Service Provider of the proposed Commercially Available Public Cloud Service meets the requirement. Respondents can provide screen captures and technical or end-user documentation to supplement their responses. Where Canada determines that the substantiation is not complete, the Respondent will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Response, it is requested that Respondents indicate where in the Response the reference material can be found, including the title of the document, and the page and paragraph numbers.

Modification 6 – **On page 5 of the ITQ, Annex A, Appendix 1**

DELETE – M6 in its entirety

INSERT

M6	General	The Respondent must confirm that the proposed Commercially Available Public Cloud Service will provide Canada's users the ability to obtain pricing for services, billing and support in Canadian dollars including but not limited to consumption reporting.	The Respondent must demonstrate compliance by providing **ONE** of the following: a) Documentation that includes either screen captures or system documentation detailing and outlining how the services will be priced, billed and supported in CDN dollars The substantiation required for ~~M5~~ M6 cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Commercially Available Public Cloud Service meets the requirement. Respondents can provide screen captures and technical or end-user documentation to supplement their responses. Where Canada determines that the substantiation is not complete, the Respondent will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Response, it is requested that Respondents indicate where in the Response the reference material can be found, including the title of the document, and the page and paragraph numbers. or b) If the Respondent's proposed Commercially Available Public Cloud Services does not currently provide the ability to obtain pricing for services, billing and support in Canadian dollars (including but not limited to consumption reporting), the Respondent must provide an attestation found in Annex J.

Modification 7 – **On page 5 of the ITQ, Annex A, Appendix 1**

DELETE – M7 in its entirety

INSERT

M7	General	The proposed Commercially Available Public Cloud Services must have published service level agreements (SLA) available to its customers. The service level commitments (detailed in the published service level agreements) must provide commercial clients support that includes, at the minimum, any published and Commercially Available support (i.e. warranty, maintenance and support services) typically provided to customers who provision the Respondent's proposed Services.	The Respondent must demonstrate compliance by providing documentation that ~~outline's~~ outlines the Respondent's published service level agreements and commitments for the proposed Services. To be considered compliant, the provided documentation must include: a) Screen shots or documentation of the published service level agreements detailing any published and Commercially Available support (i.e. warranty, maintenance and support services) typically provided to customers who provision the ~~Cloud Service Provider's~~ proposed Commercially Available Public Cloud Services including but not limited to the service commitment, credit process and monthly uptime percentage. The substantiation required for M7 cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Commercially Available Public Cloud Service meets the requirement. Respondents can provide screen captures and technical or end-user documentation to supplement their responses. Where Canada determines that the substantiation is not complete, the Respondent will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Response, it is requested that Respondents indicate where in the Response the reference material can be found, including the title of the document, and the page and paragraph numbers.

Modification 8 – **On page 6 of the ITQ, Annex A, Appendix 1**

DELETE – M8 in its entirety

INSERT

M8	General	The proposed Commercially Available Public Cloud Service must provide the ability for the consumer to choose the official language of their choice, French or English, when browsing, ordering and contacting the Cloud Service Provider.	The Respondent must demonstrate how the proposed Commercially Available Public Cloud Service provides the capability to allow consumers to choose which official language, French or English. To be considered compliant, the provided documentation needs to demonstrate the Service's ability to perform each of the following in ~~both~~ French or English: a) Browsing the service(s) on their website(s); b) Ordering services; c) Contacting the company for assistance via phone, email or chat. The substantiation required for M8 cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Commercially Available Public Cloud Service meets the requirement. Respondents can provide screen captures and technical or end-user documentation to supplement their responses. Where Canada determines that the substantiation is not complete, the Respondent will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Response, it is requested that Respondents indicate where in the Response the reference material can be found, including the title of the document, and the page and paragraph numbers.

Modification 9 – **On page 8 of the ITQ, Annex A, Appendix 1**

DELETE – M10 in its entirety

INSERT

M10	Personnel Security	The Cloud Service Provider (and if applicable the Alternative Service Provider) of the proposed Commercially Available Public Cloud Services must implement security measures that grant and maintain the required level of security screening for its respective personnel, as well as the personnel of any subcontractor personnel pursuant to their access privileges to information system assets on which Canada's Data is stored and processed. Screening measures must be applied in accordance with the definition and practices in the Treasury Board Standard on Security Screening (https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=28115), or use an acceptable equivalent agreed to by Canada. This includes, at a minimum: a) description of the employee and subcontractor positions that require access to Canada's Data or have the ability to affect the confidentiality, integrity or availability of the Services; b) process for ensuring that employees and contractors understand, are aware, and fulfil, their responsibilities for information security, and are suitable for the roles for which they are considered; c) process for security awareness and training as part of employment onboarding and when employee and subcontractor roles change; d) process that is enforced when an employee or subcontractor changes their role or when employment is terminated; and e) approach for detecting potential malicious insiders and controls implemented to mitigate the risk of access to GC data and/or affect on the reliability of cloud services hosting GC assets and data	The Respondent must provide documentation that demonstrates how the Cloud Service Provider (and if applicable the Alternative Service Provider) of the proposed Services complies with the requirements in M10. To be considered compliant, the provided documentation must include: a) system documentation or technical documentation outlining and detailing the security measures including the policies, processes and procedures that are used to grant and maintain the required level of security screening for the Cloud Service Provider's and subcontractor personnel pursuant to their access privileges to information system assets on which Canada's Data is stored and processed. The substantiation required for M10 cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Cloud Service Provider (and if applicable the Alternative Service Provider) of the proposed Commercially Available Public Cloud Service meets the requirement. Respondents can provide screen captures and technical or end-user documentation to supplement their responses. Where Canada determines that the substantiation is not complete, the Respondent will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Response, it is requested that Respondents indicate where in the Response the reference material can be found, including the title of the document, and the page and paragraph numbers.

Modification 10 – **On page 9 of the ITQ, Annex A, Appendix 1**

DELETE – M11 in its entirety

INSERT

M11	Data Protection	The Cloud Service Provider (and if applicable the Alternative Service Provider) of the proposed Commercially Available Public Cloud Services must have the ability for the GC to store and protect its information at rest, including data in backups or maintained for redundancy purposes within the geographic boundaries of Canada. This includes: a) Identifying and providing the GC with an up-to-date list of the physical locations including city which may contain Canada's data in Canada for each data centre that will be used to provide Services. b) Identifying which portions of the Services are delivered from outside of Canada including all locations where data is stored and processed and where they manage the service from. c) ensuring the infeasibility of finding a specific customer's data on physical media; and d) Employing encryption to ensure that no data is written to disk in an unencrypted form. **Respondents please note** Respondents are advised that subsequent procurement phases may require the Respondent and/or Cloud Service Provider of the proposed Commercially Available Public Cloud Service to notify Canada when there are updates to the list of physical locations which may contain Canada's data.	The Respondent must provide documentation that demonstrates how the Cloud Service Provider (and if applicable the Alternative Service Provider) of the proposed Commercially Available Public Cloud Service (identified in M1) meets the mandatory requirement outlined in M11. To be considered compliant, the provided documentation must include: a) system documentation or technical documentation outlining and detailing the policies, process and procedures that are used to store and protect its information at rest, including data in backups or maintained for redundancy purposes within the geographic boundaries of Canada; and b) For the portions of Services that could be delivered from outside of Canada, the Respondent must describe how Cloud Service Provider of the proposed Commercially Available Public Cloud Service will ensure Canada's data remains protected from unauthorized access, use, disclosure, modification, disposal, transmission, or destruction. The substantiation required for M11 cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Cloud Service Provider meets the requirement. Respondents can provide screen captures and technical or end-user documentation to supplement their responses. Where Canada determines that the substantiation is not complete, the Respondent will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Response, it is requested that Respondents indicate where in the Response the reference material can be found, including the title of the document, and the page and paragraph numbers.

Modification 11 – **On page 10 of the ITQ, Annex A, Appendix 1**

DELETE – M12 in its entirety

INSERT

M12	Third Party Assurance	The Cloud Service Provider (and if applicable the Alternative Service Provider) of the proposed Commercially Available Public Cloud Service must be designed and developed to ensure the security of their proposed Commercially Available Public Cloud Service, including, implementing information security policies, procedures, and security controls. The Cloud Service Provider (and if applicable the Alternative Service Provider) of the proposed Commercially Available Public Cloud 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 Public Cloud Service ~~provided by the Cloud Service Provider~~.	The Respondent must demonstrate how the Cloud Service Provider (and if applicable the Alternative Service Provider) of the proposed Commercially Available Public Cloud Service complies with the requirements in M12. 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 Respondent **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 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 solicitation closing date; b) Identify the legal business name of the proposed CSP or ASP; c) Identify the current certification date and/or status; d) The scope of the report must map to locations and services offered by the proposed Commercially Available Public Cloud 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 e) 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. The Respondent 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 FedRAMP Moderate Certification

			Evidence or assessment of its Services against the Cloud Security Alliance (CSA) Cloud Controls 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 identified in M1.** • **Certifications must be accompanied by assessment reports.**

Modification 12 – **On page 11 of the ITQ, Annex A, Appendix 1**

DELETE – M13 in its entirety

INSERT

M13	Supply Chain Management	The Respondent must provide a third party supplier list containing information on any third parties (e.g. subsidiaries, subcontractors, etc.) that would provide Canada with the proposed Commercially Available Public Cloud Service. For the purposes of this requirement, a company who is merely a supplier of goods to the Cloud Service Provider (and if applicable the Alternative Service Provider) of the proposed Commercially Available Public Cloud Service, but who does not perform any portion of the supply chain that could provide Canada with the proposed Commercially Available Public Cloud Service, is not considered to be a third party. Third party examples would include, for example, technicians who might be deployed or maintain the Commercially Available Public Cloud Services of the Cloud Service Provider that have been proposed by the Respondent in M1. **Please note:** Respondents are advised that subsequent procurement phases may require the Respondent to notify Canada regularly when there are updates to the list of third party suppliers.	The Respondent must provide documentation that lists information on any third parties that could be used to perform any part of the supply chain that would provide Canada with the proposed Commercially Available Public Cloud Service whether they would be (i) subcontractors to the Cloud Service Provider (and if applicable the Alternative Service Provider), or (ii) subcontractors to subcontractors of the Cloud Service Provider (and if applicable the Alternative Service Provider) down the chain, **OR** (iii) any subsidiaries. The list must include at a minimum: a) The name of the third party; b) The address of the third party headquarters; c) The portion of the Work that would be performed by the third party; d) The location(s) where the third-party would provide Canada with the proposed Commercially Available Public Cloud Service. e) Any third party that could have access to Canada's data in the proposed Commercially Available Public Cloud Service. If the ~~Cloud Service Provider~~ CSP or ASP does not use any third parties to perform any part of the supply chain that could provide Canada with the proposed Commercially Available Public Cloud Service, the Respondent is requested to indicate this in their response to this requirement.

Modification 13 – **On page 12 of the ITQ, Annex A, Appendix 1**

DELETE – M14 in its entirety

INSERT

M14	Supply Chain Risk Management	The Cloud Service Provider (and if applicable the Alternative Service Provider) of the proposed Commercially Available Public Cloud 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 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.	The Respondent must demonstrate how the Cloud Service Provider (and if applicable the Alternative Service Provider) of the proposed Commercially Available Public Cloud Service complies with the requirements in M14 as documented under the Cloud Service Provider Information Technology Security Assessment program. To be considered compliant, the provided documentation must demonstrate that the CSP's (and if applicable the ASP's) 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 Cloud Service Provider's approach to SCRM and demonstrate how the Cloud Service Provider (and if applicable the Alternative Service Provider) of the proposed Commercially Available Public Cloud Service will reduce and mitigate supply chain risks.

Modification 14 – **On page 12 of the ITQ, Annex A, Appendix 1**

DELETE – M15 in its entirety

INSERT

M15	Privacy	The Cloud Service Provider (and if applicable the Alternative Service Provider) of the proposed Commercially Available Public Cloud Service must demonstrate that it is compliant with the privacy policies, procedures, and provisions that meet the following industry certification: a) ISO/IEC 27018:2014 Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors. **Please note:** Respondents are advised that subsequent procurement phases may require the Respondent to confirm to Canada on a regular basis that the proposed Commercially Available Public Cloud Service meets the above certification, and that the certification is valid for the full term of the procurement vehicle.	To demonstrate compliance to the certification, the Respondent must provide: a) A copy of the Cloud Service Provider's (and if applicable the Alternative Service Provider) most recent and ISO 27018 certification documents, which must have been issued within the 12 months prior to the solicitation closing date; and b) A copy of the ISO 27018 assessment report for their current Commercially Available Public Cloud Services.

Modification 15 – **On page 1 of the ITQ, Annex A, Appendix 2**

DELETE

Responses to **Annex A, Appendix 2 – Part A** must be submitted to Shared Services Canada (SSC) at the following email address by the solicitation closing date – ~~ssc.cloudsolicitationsollicitationinfonuagiques.spc@canada.ca~~

INSERT

Responses to **Annex A, Appendix 2 – Part A** must be submitted to Shared Services Canada (SSC) at the following email address by the solicitation closing date – ssc.cloudsolicitation-sollicitationinfonuagiques.spc@canada.ca

Modification 16 – **On page 4 of the ITQ, Annex A, Appendix 2**

DELETE – M5 in its entirety

INSERT

M5	General	The proposed Commercially Available Public Cloud Services must have published service level agreements (SLA) available to its customers. The service level commitments (detailed in the published service level agreements) must provide commercial clients support that includes, at the minimum, any published and Commercially Available support (i.e. warranty, maintenance and support services) typically provided to customers who provision the Respondent's proposed Services.	The Respondent must demonstrate compliance by providing documentation that ~~outline's~~ outlines the Respondent's published service level agreements and commitments for the proposed Services. To be considered compliant, the provided documentation must include: b) Screen shots or documentation of the published service level agreements detailing any published and Commercially Available support (i.e. warranty, maintenance and support services) typically provided to customers who provision the ~~Cloud Service Provider's~~ proposed Commercially Available Public Cloud Services including but not limited to the service commitment, credit process and monthly uptime percentage. The substantiation required for M5 cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Commercially Available Public Cloud Service meets the requirement. Respondents can provide screen captures and technical or end-user documentation to supplement their responses. Where Canada determines that the substantiation is not complete, the Respondent will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Response, it is requested that Respondents indicate where in the Response the reference material can be found, including the title of the document, and the page and paragraph numbers.

Modification 17 – **On page 5 of the ITQ, Annex A, Appendix 2**

DELETE – M6 in its entirety

INSERT

M6	General	The proposed Commercially Available Public Cloud Service must provide the ability for the consumer to choose the official language of their choice, French or English, when browsing, ordering and contacting the Cloud Service Provider.	The Respondent must demonstrate how the proposed Commercially Available Cloud Service provides the capability to allow consumers to choose which official language, French or English. To be considered compliant, the provided documentation needs to demonstrate the Service's ability to perform each of the following in ~~both~~ French or English: d) Browsing the service(s) on their website(s); e) Ordering services; f) Contacting the company for assistance via phone, email or chat. The substantiation required for M6 cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Commercially Available Public Cloud Service meets the requirement. Respondents can provide screen captures and technical or end-user documentation to supplement their responses. Where Canada determines that the substantiation is not complete, the Respondent will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Response, it is requested that Respondents indicate where in the Response the reference material can be found, including the title of the document, and the page and paragraph numbers.

Modification 18 – **On page 7 of the ITQ, Annex A, Appendix 2**

DELETE – M8 in its entirety

INSERT

M6	General	The proposed Commercially Available Public Cloud Service must provide the ability for the consumer to choose the official language of their choice, French or English, when browsing, ordering and contacting the Cloud Service Provider.	The Respondent must demonstrate how the proposed Commercially Available Cloud Service provides the capability to allow consumers to choose which official language, French or English. To be considered compliant, the provided documentation needs to demonstrate the Service's ability to perform each of the following in ~~both~~ French or English: g) Browsing the service(s) on their website(s); h) Ordering services; i) Contacting the company for assistance via phone, email or chat. The substantiation required for M6 cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Commercially Available Public Cloud Service meets the requirement. Respondents can provide screen captures and technical or end-user documentation to supplement their responses. Where Canada determines that the substantiation is not complete, the Respondent will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Response, it is requested that Respondents indicate where in the Response the reference material can be found, including the title of the document, and the page and paragraph numbers.

Modification 19 – **On page 8 of the ITQ, Annex A, Appendix 2**

DELETE – M9 in its entirety

INSERT

M9	Data Protection	The physical locations of the proposed Commercially Available Public Cloud Service (which may contain Canada's data) must be located in either: a) A country within the North Atlantic Treaty Organization (NATO); b) A country within the European Union (EU); or c) A country with which Canada has an international bilateral industrial security instrument **Respondents please note** Additional information on countries within NATO can be located at the following link: https://www.nato.int/cps/en/natohq/nato_countries.htm Additional information on countries within the EU can be located at the following link: https://europa.eu/european-union/about-eu/countries_en 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 and as updated from time to time.	The Respondent must provide documentation that demonstrates how the proposed Commercially Available Public Cloud Service (identified in M1) meets the mandatory requirement outlined in M9. To be considered compliant, the provided documentation must include: a) an up-to-date (as of the ITQ closing date) list of the physical locations (including city and country) for each data centre that may contain Canada's data including in backups or for redundancy purposes. The substantiation required for M9 cannot simply be a repetition of the mandatory requirement but must explain and demonstrate how the Cloud Service Provider (and if applicable the Alternative Service Provider) meets the requirement. Respondents can provide screen captures and technical or end-user documentation to supplement their responses. Where Canada determines that the substantiation is not complete, the Respondent will be declared non-compliant. The substantiation may refer to additional documentation submitted with the Response, it is requested that Respondents indicate where in the Response the reference material can be found, including the title of the document, and the page and paragraph numbers.

Modification 20 – **On page 9 of the ITQ, Annex A, Appendix 2**

DELETE – M10 in its entirety

INSERT

M10	Third Party Assurance	The Cloud Service Provider (and if applicable the Alternative Service Provider) must be designed and developed to ensure the security of their proposed Commercially Available Public Cloud Service, including, implementing information security policies, procedures, and security controls.	The Respondent must provide documentation to Canada that demonstrates how the Cloud Service Provider (and if applicable the Alternative Service Provider) of the proposed Commercially Available Public Cloud Service complies with the requirements in M10. Compliance must be demonstrated by providing one or more of the following industry certifications identified below, and validated through independent third party assessments. The Respondent 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 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 solicitation closing date; b) Identify the legal business name of the proposed CSP or ASP; c) Identify the current certification date and/or status; d) The scope of the report must map to locations and services offered by the proposed Commercially Available Public Cloud 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 e) 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 in M1.** • **Certifications must be accompanied by assessment reports.**

Modification 20 – **On page 10 of the ITQ, Annex A, Appendix 2**

DELETE – M11 in its entirety

INSERT

M11	Supply Chain Management	The Respondent must provide a third party supplier list containing information on any third parties (e.g. subsidiaries, subcontractors, etc.) that would provide Canada with the proposed Commercially Available Public Cloud Service. For the purposes of this requirement, a company who is merely a supplier of goods to the Cloud Service Provider (and if applicable the Alternative Service Provider) of the proposed Commercially Available Public Cloud Service, but who does not perform any portion of the supply chain that could provide Canada with the proposed Commercially Available Public Cloud Service, is not considered to be a third party. Third party examples would include, for example, technicians who might be deployed or maintain the Commercially Available Public Cloud Services of the Cloud Service Provider that have been proposed by the Respondent in M1. **Please note** Respondents are advised that subsequent procurement phases may require the Respondent to notify Canada regularly when there are updates to the list of third party suppliers.	The Respondent must provide documentation that lists information on any third parties that could be used to perform any part of the supply chain that would provide Canada with the proposed Commercially Available Public Cloud Service whether they would be (i) subcontractors to the Respondent or Cloud Service Provider, or (ii) subcontractors to subcontractors of the Respondent or Cloud Service Provider down the chain, or (iii) any subsidiaries. The list must include at a minimum: a) The name of the third party; b) The address of the third party headquarters; c) The portion of the Work that would be performed by the third party; d) The location(s) where the third-party would provide Canada with the proposed Commercially Available Public Cloud Service. e) Any third party that could have access to Canada's data in the proposed Commercially Available Public Cloud Service. If the CSP or ASP of the proposed Commercially Available Public Cloud Service does not use any third parties to perform any part of the supply chain that could provide Canada with the proposed Commercially Available Public Cloud Service, the Respondent is requested to indicate this in their response to this requirement.

Modification 21 – **On page 10 of the ITQ, Annex A, Appendix 2**

DELETE – M12 in its entirety

INSERT

M12	Supply Chain Risk Management	The Cloud Service Provider (and if applicable the Alternative Service Provider) of the proposed Commercially Available Public Cloud Service (identified in M1) 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, role-based access, and least-privilege access for all personnel within the supply chain.	The Respondent must demonstrate how the Cloud Service Provider (and if applicable the Alternative Service Provider) of the proposed Commercially Available Public Cloud Service complies with the requirements in M12 as documented under the Cloud Service Provider Information Technology Security Assessment program. 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 Cloud Service Provider's approach to SCRM and demonstrate how the Cloud Service Provider (and if applicable the Alternative Service Provider) of the proposed Commercially Available Public Cloud Service will reduce and mitigate supply chain risks

Modification 22 – **On page 1 of the ITQ, Annex A, Appendix 3**

DELETE

Respondents are reminded of that Responses to **Annex A, Appendix 3** must be submitted to Shared Services Canada (SSC) at the following email address by the solicitation closing date – ~~ssc.cloudsolicitationsollicitationinfonuagiques.spc@canada.ca~~

INSERT

Respondents are reminded of that Responses to **Annex A, Appendix 3** must be submitted to Shared Services Canada (SSC) at the following email address by the solicitation closing date – ssc.cloudsolicitation-sollicitationinfonuagiques.spc@canada.ca

2. REVISED COPY OF ANNEX J

A revised version of Annex J has been included as an attachment to Amendment 006 with the modifications in Modification 3 applied.

==========

The following is a summary of Attachments/Amendments issued to date for this solicitation:

Document	Distribution	Date	Description
ITQ	Buyandsell.gc.ca	September 7, 2018	**PDF Version** 1. 32099 - GC Cloud Vehicle - ITQ - ENGLISH 2. 32099 - ITQ Annex A Appendix 1 - ENGLISH 3. 32099 - ITQ Annex A Appendix 2 - ENGLISH 4. 32099 - ITQ Annex B - CSP ITS Assessment Program Onboarding Process - ENGLISH 5. SSC Standard Instructions for Procurement Documents - ENGLISH 6. 32099 - GC Cloud Vehicle - ITQ - FRENCH 7. 32099 - ITQ Annex A Appendix 1 - FRENCH 8. 32099 - ITQ Annex A Appendix 2 - FRENCH 9. 32099 - ITQ Annex B - CSP ITS Assessment Program Onboarding Process - FRENCH 10. SSC Standard Instructions for Procurement Documents - FRENCH
Amendment 1	Buyandsell.gc.ca	October 5, 2018	1. Extend qualification period for Stream 1 and Stream 2. 2. Provide information on when Canada's responses will be published. 3. Provide information on when Annex C & Annex D will be published.
Amendment 2	Buyandsell.gc.ca	October 5, 2018	1. Provide updated information on when Canada's responses will be published. 2. Provide updated information on when Annex C & Annex D will be published.
Amendment 3	Buyandsell.gc.ca	October 23, 2018	1. Extend qualification period for Stream 1. 2. Provide updated information on when Canada's responses will be published. 3. Provide updated information on when Annex C & Annex D will be published.
Amendment 4	Buyandsell.gc.ca	October 26, 2018	1. Provide updated information on when Canada's responses will be published. 2. Provide updated information on when a revised copy of the ITQ (including Annex C & Annex D) will be published.

Document	Distribution	Date	Description
Amendment 5	Buyandsell.gc.ca	October 29, 2018	a) Publish Canada's Response for Questions 1 to 185 b) Publish Annex C and Annex D c) Publish Modifications to the ITQ d) Key reminders to suppliers **PDF Version (Clean and Mark-up versions)** a) 32099 - GC Cloud ITQ – (EN) - Amend 005 b) 32099 - GC Cloud ITQ – Annex A App 1 (EN) - Amend 005 c) 32099 - GC Cloud ITQ – Annex A App 2 (EN) - Amend 005 d) 32099 - GC Cloud ITQ – Annex A App 3 (EN) - Amend 005 **MS-Word Version (Clean and Mark-up versions)** a) 32099 - GC Cloud ITQ – (EN) - Amend 005 b) 32099 - GC Cloud ITQ – Annex A App 1 (EN) - Amend 005 c) 32099 - GC Cloud ITQ – Annex A App 2 (EN) - Amend 005 d) 32099 - GC Cloud ITQ – Annex A App 3 (EN) - Amend 005
Amendment 6	Buyandsell.gc.ca	November 6, 2018	a) Extend qualification period for Stream 1. b) Key reminders to suppliers
Amendment 7	Buyandsell.gc.ca	November 7, 2018	a) Publish Modifications to the ITQ b) Provide a revised version of Annex J. **PDF Version** a) 32099 - GC Cloud ITQ – Revised Annex J – (EN) - Amend 007 **MS-Word Version** a) 32099 - GC Cloud ITQ – Revised Annex J – (EN) - Amend 007