Amendment 9 to the IaaS & Native PaaS Prequalification CBS

Solicitation No.	CS-IAAS-2024	Amd: 009

The purpose of this amendment is to:

1- Provide answers to questions received as detailed in section A.
2- Provide the latest version Attachment 1 - Prequalification Evaluation Grid, which includes any changes that have been made as detailed in section B.

Section A - Questions and Answers (set 7)

	Question	Answer
103	In response to a recent question, the Crown revised the requirement that respondents must meet three of five trust principles of AICPA SOC 2 Type II. The fifth requirement of Privacy was added with this recent change. While AICPA SOC 2 Type II requirements evaluate a broad range of controls relevant to data security which includes confidentiality and privacy, in this context, many Cloud vendors choose to adhere to and certify against ISO 27018 because it is a more rigorous standard specifically addressing cloud deployments. ISO 27018 is a specific standard for cloud service providers (CSPs) focusing on the protection of personally identifiable information (PII) in the cloud. It provides guidance, and controls for handling PII, addressing issues such as data handling, transparency,	At this stage of the prequalification process, Canada will not change the prequalification criteria, but will consider your proposal for a future stage of this procurement process.

	consent, and compliance with applicable privacy laws and regulations. Where SOC 2 Type II includes controls related to data protection and confidentiality, which indirectly address privacy concerns, ISO 27018 offers a set of specific controls tailored to cloud service providers for protecting PII in a cloud environment. It includes provisions for data encryption, access controls, data portability, transparency, and compliance with legal and regulatory requirements related to privacy. Respecting the Crown's desire to have qualified vendors to meet three of five trust principles related to securing Canada's data, as this prequalification process is specifically related to cloud-based solutions, will the Crown consider ISO 27018 certification as a satisfactory equivalent (if not a more rigorous standard) for meeting the privacy and confidentiality standard?	
104	Regarding Canada's responses to question number 93 in Amendment 008 – The response has led to some confusion about the scoring based on various stages of the CMVP process. We request Canada to confirm that full points will be awarded if the module is in "COORDINATION" phase of the CMVP process. The amendment states that full points will be awarded only if the module is in "In review" status (i.e., Step-3). However, "Coordination" status is in fact Step-4 of the process which is beyond "Step-3 In-review" status and thus should receive full points per our understanding.	As previously stated, the criteria remain unchanged after Amendment 8. The specific requirement is that the Bidder "has provided a module at or passed the status of 'In Review' for FIPS 140-3 validation in the Modules In Process List by the CMVP at the Prequalification CBS closing date." In accordance with the CMVP Validation Process Flow, the statuses that follow "In Review" are "Coordination" and "Finalization." Therefore, a module with a status of "In Review" or "Coordination" or "Finalization" would receive 3 points.

Section B

For your convenience, Canada is providing the latest version of Attachment 1—Prequalification Evaluation Grid, which includes any changes that have been made to date.

Part A – Mandatory Criteria

The following mandatory criteria must be met.

	Criteria	Information required by Bidders	Scoring Elements
M1	**Capacity of the Bidder to sell Commercially Available Infrastructure-as-a-Service (IaaS) AND Platform-as-a-Service (PaaS)** The Bidder must be a Cloud Service Provider (CSP) with Commercially Available Infrastructure-as-a-Service (IaaS) services **AND** Native Platform-as-a-Service (PaaS) services. For the purpose of this criterion, an instance type, in the context of cloud computing, refers to a virtual machine, serverless instance, or an add-on to a virtual machine offered by a cloud service provider.	1. The Bidder should provide the URL currently available to the public listing the Commercially Available IaaS and Native PaaS services of the following: services (instance types) that address each category of the following Commercially Available IaaS services: a. Category 1—General or Standard Purpose instances that are configurable to balance the amount of compute, memory, and networking resources based on the requirements of applications and workloads. b. Category 2—Compute Optimized instances for applications and workloads that require high computing power using high-performance processors. c. Category 3—Memory Optimized instances for applications and workloads that require fast processing of large data sets in memory. d. Category 4—Specialized instances for applications and workloads that require specific requirements, including any of the following sub-categories: i. High-Performance Computing (HPC) ii. Enhanced storage capabilities iii. GPU-supported processes iv. Machine learning-based systems e. Category 5—Block, Object and File storage capabilities that are scalable. f. Category 6—Cold storage for long-term storage of archived data. g. Category 7—High-Performance storage based on Solid-State Drives (SSD) technology.	To be compliant, the Bidder must demonstrate the following services through URLs currently available to the public: • A minimum of 5 Commercially Available IaaS services for each of the categories 1 to 4 evidenced by their publicly viewable product/service list (1a to 1d) • A minimum of 3 Commercially Available IaaS services for category 5 evidenced by their publicly viewable product/service list (1e) • A minimum of 1 Commercially Available IaaS service for each of the categories 6 and 7 evidenced by their publicly viewable product/service list (1f and 1g) • A minimum of 4 Commercially Available PaaS services for each of the categories 8 to 13 evidenced by their publicly viewable product/service list (2a to 2f) The Bidder must provide a publicly available URL which must present direct evidence of the requirement. Please not that Canada will not move past that provided URL in any way.

	Criteria	Information required by Bidders	Scoring Elements
		2. services (instances type) that address each category of the following Native PaaS services: a. Category 8—Container services b. Category 9—Developer tools c. Category 10—Database services d. Category 11—Network and security services e. Category 12—Artificial Intelligence (AI) or Machine Learning (ML) f. Category 13—Analytics and Big Data services	
M2	**Capacity of the Bidder to secure Canada's Data** The Bidder must have the following current, latest version and valid industry certifications and audit reports: 1. ISO/IEC 27001: Information technology — Security techniques—Information security management systems — Requirements; 2. ISO/IEC 27017: Information technology — Security techniques—Code of practice for information security controls based on ISO/IEC 27002: for cloud services; 3. AICPA Service Organization Control (SOC) 2 Type II for a minimum of 3 of the 5 following trust principles: Security, availability, processing integrity, privacy and confidentiality. *Only certifications issued by an independent third party qualified under AICPA, CPA Canada, or conforming to the ISO/IEC 17020 quality system standard will be accepted.	The Bidder should provide the following evidence: a) For each certification: copies of the certifications and audit reports including the date of issuance and expiration (where applicable). Should a certification have expired or be due to expire prior to the Prequalification CBS closing date and the bidder is in the process of renewal, a verification letter or a statement from the issuing body confirming the certification's current and valid status should be provided. b) For SOC 2: copy of the audit reports, the trust principles, date of issuance and expiration (as applicable).	To be compliant the Bidder must demonstrate they have current: a) latest version and valid certifications and audit reports of the following: ISO/IEC 27001 and ISO/IEC 27017; b) AICPA Service Organization Control (SOC) 2 Type II that includes a minimum of 3 of the following trust principles: • Security; • Availability; • processing integrity; • privacy; • confidentiality.

Part B – Rated Criteria

The following criteria will be rated as per the scoring elements defined in the table.

Maximum total score = 77 points

	Criteria	Information to be provided by Bidders	Scoring Elements
R1	**Capacity to satisfy data residency requirements (maximum 15 points)** The Bidder should have a minimum of two data centres located in a single region in Canada. Canada uses the Uptime Institute's Tiered Classification System for the Data Centre definition. For the purpose of this solicitation: A Data Centre (DC) is a physical infrastructure that meets or exceeds the "Data Centre Tier III" requirements. A DC is part of a region. A region is defined as multiple DC's located within 100 km of each other within the same defined region. Data Centre is part of the Bidders' publicly available commercial cloud offering.	The Bidder should provide the physical address of two data centres located in a single region in Canada. If the Bidder chooses not to provide the physical address, they can provide: • the bidder public designation of each DC; • the complete postal code; and • the direct distance (in km) between the DCs.	Up to 15 points will be allocated. Points will be allocated as follows: **15 points:** the Bidder has provided the physical address or postal code of 2 data centres located in a single region in Canada. **10 points:** the Bidder has provided the physical address or postal code of 2 data centres located in Canada not within the same region. **5 points:** the Bidder has provided the physical address or postal code of one data centre located in Canada. **0 points:** the Bidder has not provided the physical address or postal code of any data centre located in Canada.
R2	**Capacity of the Bidder's Solution to protect Canada's data (maximum 12 points)** The Bidder should demonstrate that the Solution has the capability to encrypt data-in-transit and data-at-rest with Communications Security Establishment Canada (CSE) approved cryptography. The CSE approved cryptography can be found in the Cryptographic algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B Information—ITSP.40.111 (version 3 — March 18, 2024) (https://www.cyber.gc.ca/en/guidance/cryptographic-	**1. For Data-in-transit:** To demonstrate its capacity, the Bidder should provide one cryptographic mechanism used to prevent unauthorized disclosure of information and detect changes to information during transmission, and provide evidence for the following elements: a) Identify if the Cryptographic module has been tested and validated or is undergoing review under the Cryptographic Module Validation Program (CMVP) for compliance to FIPS 140-3: Security Requirements for Cryptographic Module as per Section 12 of ITSP 40.111	Up to 12 points will be allocated. **1. For Data-in-transit:** Points will be allocated as follows: a) Cryptographic module: **3 points:** The Bidder has provided a certificate number demonstrating that the module is FIPS 140-3 validated by the CMVP or has provided a module at or passed the status of "In review" for FIPS 140-3 validation in the Modules In Process List by the CMVP at the Prequalification CBS closing date.

	Criteria	Information to be provided by Bidders	Scoring Elements
	algorithms-unclassified-protected-protected-b-information-itsp40111) and Guidance on securely configuring network protocols (ITSP.40.062) (revision 2—August 21, 2020) (www.cyber.gc.ca/en/guidance/guidance-securely-configuring-network-protocols-itsp40062) *Note to Bidders: This requirement is not mandatory for the prequalification stage. In subsequent procurement stages, we will require all cryptographic mechanisms and subsequent modules and algorithms used and they will be verified prior to contract award.*	For validated module: Bidder should provide the module name and the certificate number. For module undergoing review: Bidder should provide the module name and the status of validation for FIPS 140-3 in the Modules In Process List by the CMVP. b) Identify one implemented encryption algorithm that satisfies section 2 and 3 of ITSP 40.111 and is on one of the tables (Tables 1 to 21) of ITSP.40.062. Bidders should provide the algorithm name and the applicable table in the ITSP.40.062. c) Confirm whether Cryptographic algorithm implementations have been tested and validated under the Cryptographic Algorithm Validation Program (CAVP) as per Section 12 of ITSP 40.111. Bidders should provide the validation number **2. For Data-at-rest:** To demonstrate its capacity, the Bidder should provide one cryptographic mechanism used to prevent unauthorized disclosure and modification of the information at rest on information system components storing Canada's data and provide evidence for the following elements: a) Identify if the Cryptographic modules have been tested and validated or are undergoing review under the Cryptographic Module Validation Program (CMVP) for compliance to FIPS 140-3: Security Requirements for Cryptographic Modules as per Section 12 of ITSP 40.111 For validated modules: Bidder should provide the module name and the certificate number.	**1 point:** The Bidder has provided a certificate number demonstrating that the module is validated under FIPS 140-2 by the CMVP. **0 points**: Not CMVP validated. b) Encryption algorithm: **2 points:** The encryption algorithm implemented is on one of the tables (Tables 1 to 21) under the recommended column in the ITSP.40.062. **1 point:** The encryption algorithm implemented is on one of the tables (Tables 1 to 21) under the sufficient column in the ITSP.40.062. **0 points:** Any other algorithm not in one of the tables under recommended and sufficient columns in the ITSP.40. c) Cryptographic algorithm: **2 points:** The Bidder has provided a validation number demonstrating that the cryptographic algorithm is validated by the CAVP **0 points:** The Bidder has not provided a validation number demonstrating that the cryptographic algorithm is validated by the CAVP **2. For Data-at-rest:** Points will be allocated as follows: a) Cryptographic module: **3 points:** The Bidder has provided a certificate number demonstrating that the module is FIPS 140-3 validated by the CMVP or has provided a module at or passed the status of "In review" for FIPS 140-3 validation in the Modules In Process List by the CMVP at the Prequalification CBS closing date. **1 point:** The Bidder has provided a certificate number demonstrating that the module is validated under FIPS 140-2 by the CMVP. **0 points:** Not CMVP validated.

	Criteria	Information to be provided by Bidders	Scoring Elements
		For module undergoing review: Bidder should provide the module name and the status of validation for FIPS 140-3 in the Modules In Process List by the CMVP. b) Confirm whether Cryptographic algorithm implementations have been tested and validated under the Cryptographic Algorithm Validation Program (CAVP) as per Section 12 of ITSP 40.111. Bidders should provide the validation number.	b) Cryptographic algorithm: **2 points:** The Bidder has provided a validation number demonstrating that the cryptographic algorithm is validated by the CAVP. **0 points:** The Bidder has not provided a validation number demonstrating that the cryptographic algorithm is validated by the CAVP.
R3	**Experience of the Bidder to provide IaaS and Native PaaS services to large organizations (maximum 21 points)** The Bidder should demonstrate its experience in providing both IaaS and Native PaaS services to large government organizations or large external private corporations. *"external" refers to organizations or corporations that are not part of the Bidder's own corporate structure or its parent organization.* For the purpose of this criterion "unique services" means a specific element of the commercially and publicly available cloud services catalog. This specifically excludes non-public cloud services such as private cloud services and data centre hosting services.	To demonstrate its experience, the Bidder should provide a list of three clients to whom both IaaS and Native PaaS services were provided. For each client, the following information should be provided: 1) Client business name 2) Duration of services including service start date and end date (if applicable) (month and year) 3) Number of employees of the client 4) Number of unique services provided and used by the client within the duration of services.	Up to 21 points will be allocated using the average of the three clients' total points. Points will be allocated as follows: **Duration of services rendered to the client** **7 points:** more than or equal to 7 years **5 points:** more than or equal to 5 years and less than 7 years **3 points:** more than or equal to 3 years and less than 5 years **0 points:** less than 3 years **Number of employees of the client** **7 points:** 50,000 employees and more **5 points:** between 29,999 and 50,000 employees **3 points:** between 9,999 and 30,000 employees **0 points:** fewer than 10,000 employees **Unique services provided and used** **7 points:** 200 services and more **5 points:** between 149 and 200 services **3 points:** between 99 and 150 services **0 points:** fewer than 100 services If more than three clients are submitted, only the first three clients listed in the submission will be assessed.

	Criteria	Information to be provided by Bidders	Scoring Elements
R4	**Capacity of the Bidder to address Canada's needs (maximum of 29 points)** The Bidder should demonstrate its capacity to address Canada's needs	The Bidder should provide the following information to demonstrate its capacity to address Canada's needs for each element listed below: **Elements of comparison** 1. Number of Regions in Canada. 2. Number of Regions in the World. 3. Number of Data Centres (DC) in Canada. The Bidder should provide the city of each DC associated with the region. 4. Total number of Data Centres deployed and in service in the World. 5. Number of internet exchange points in Canada. The Bidder should provide the name of the corporations of each internet exchange point providers they are with. 6. Number of internet exchange points globally. 7. Internet bandwidth capacity in gigabits per second in Canada. The Bidder should provide the gigabits per second. 8. Daily average number of physical cores deployed in the Data centres identified in element 3 from February 1, 2024 to February 29, 2024. 9. Percentage of available capacity in terms of physical cores. The Bidder should provide the data associated with the following calculation: The percentage of available capacity in terms of physical cores is calculated by [1- daily average number of physical cores in use in the Data centres identified in element 3 from February 1, 2024 to February 29, 2024/by the daily average number of physical cores deployed in the Data centres identified in element 3 from February 1, 2024 to February 29, 2024 (item 8)]*100.	Up to 29 points will be allocated using the sum of the comparative assessment and direct scoring of the elements (1 to 11). Each element (1 to 11) will individually be assigned points. **Comparative assessment of elements** For elements 1 to 9: A. **Establishing the ranking**: Bidder will be ranked from the highest number to the lowest number. B. **Allocating the points:** points will be allocated based on the Bidder's ranking in each element, from highest to the lowest. Points will be allocated for each element of comparison as follows: **3 points:** Top rank Bidder **2 points:** Second rank Bidder **1 point:** Third rank Bidder **0 points:** Remaining ranked Bidder (4+) In the event of a tie in the ranking order for a particular element of comparison, all Bidders with equal rankings will receive the same score. **Direct scoring of the elements** For elements 10 and 11, points will be allocated as follows: **1 point:** Yes **0 points:** No

	Criteria	Information to be provided by Bidders	Scoring Elements
		Direct scoring 10. The Bidder has documentation that defines latency and performance metrics between their Canadian regions: yes or no 11. The Bidder offers a Marketplace for 3rd party apps: yes or no For elements 10 and 11: The Bidder should provide the hyperlinks.	

All other terms and conditions remain unchanged.