

Amendment 5 to the IaaS & Native PaaS Prequalification CBS

Solicitation No.	CS-IAAS-2024	Amd: 005
------------------	--------------	----------

The purpose of this amendment is to:

- 1- Provide answers to questions received as detailed in section A.
- 2- Modify the Prequalification CBS as detailed in section B.

Section A - Questions and Answers (set 4)

NOTE: Questions related to the resulting contract will not be addressed at this time, as Bidders are not required to agree to be bound by the terms and conditions of the resulting contract at this point in the prequalification process. While these are provided for informational purposes and will be finalized in consultation with prequalified vendors later in the process (Stage 5), Bidders should understand that by submitting a bid, they are agreeing to be bound by the instructions, clauses, and terms of the Prequalification Challenge-Based Solicitation as currently written. However, agreement to the terms and conditions of the resulting contract will not be required until Stage 7 - Final Challenge-Based Solicitation. Sections 2.1 and 2.3 will be amended to clarify this distinction.

Please also note that due to operational requirements, Canada will not be able to accommodate a further extension of the Prequalification Closing Date.

	Question	Answer
37	<p>The executive summary states “Once the prequalified Bidders are identified, Canada will work with them to develop the selection process that will result in the award of 2 or 3 Task Authorization Contracts” but section 1.4 states “Up to two Contractors that will be invited to sign a Task Authorization Contract (TAC)”. Section 4.3.1 states “The 2 or 3 highest-ranking responsive Bid(s) (Total Score) will be recommended for Contract award.” Will Canada please provide definitive information regarding the number of Contractors that it intends to recommend for contract award?</p>	<p>Canada will clarify with the prequalified bidders the number of resulting contracts later in the process, as the decision is still pending.</p>
45	<p>With respect to “what” a bidder may have intended could be subjective in nature (e.g., a Bidder may not have intended to submit clauses contrary to the instructions and did not believe in good faith that it had done so).</p> <p>Could Canada please:</p> <p>a. Include as part of the Pre-Bid Compliance Check Process (section 3.2) a review of the bidder’s terms to identify if there are provisions that Canada views as “superseding” the Resulting Contract Clauses; or b. If Canada will not do so, will Canada please modify the provision of section 2.3 as follows:</p> <p>Bidders submitting a Bid containing statements implying that the Bid is conditional on modification to these Contract terms and conditions (including all documents incorporated into the Contract by reference) or containing terms and conditions that purport to supersede these Contract terms and conditions will be required to submit only those terms not already addressed in the resulting contract clauses that the Bidder would like Canada to consider considered non-responsive.</p>	<p>Canada will not include a review of the Bidder’s terms and conditions as part of the pre-bid compliance review process. Sections 2.1 and 2.3 will be modified.</p> <p>Canada will provide additional clarity in the forthcoming amendment.</p>
47	<p>In recognition of the CCCS CSP ITS Assessment’s identical objective to requirements M2’s aim of demonstrating the capacity of a CSP to secure Canada’s data, we request that Canada allow</p>	<p>To ensure a fair and equal opportunity for all Bidders, Canada will only require ISO and SOC information at the Prequalification stage.</p>

	<p>CSPs to satisfy requirements M2, in the alternative, by demonstrating a current assessment under the CCCS CSP ITS Assessment Process using the CCCS Cloud Control Profile – Medium.</p>	<p>As the procurement process moves beyond the Prequalification stage, Canada will require additional documentation in this area.</p>
<p>48</p>	<p>Because Canada has moved industry certifications and audit reports from a rated to a mandatory requirement, SOC 2 Type II certification is now mandatory for prequalification. As it is currently drafted, requirement M2 requires a SOC 2 certification which addresses the trust principles of “security, availability, processing integrity, and confidentiality.” Because the trust principle of “processing integrity” is concerned with the application layer of a service, it is not relevant for IaaS/PaaS services. By contrast, requirement M2 does not currently require a SOC 2 certification which addresses the trust principle of “privacy,” which is aligned with Canada’s draft Privacy Obligations (Appendix A – Schedule 2).</p> <p>Question: To address this misalignment, we request that Canada amend requirements M2 to require a SOC 2 certification that addresses the trust principles of “security, availability, confidentiality, and privacy”.</p>	<p>CCCS consistently requires SOC2 Type II for the trust principles of security, availability, processing integrity, and confidentiality. This is identified as a security requirement, not a privacy requirement, and the specified trust principles remain unchanged.</p>
<p>49</p>	<p>Once two CSPs are awarded a contract, what will be the post-award mechanism to have CSPs compete for workloads/projects? Will it be similar to what was the RCR process under the existing GCCFA or will there be no competition and CSPs will be informed which workloads they will be hosting?</p>	<p>In accordance with Section 1.4 Challenge-Based Solicitation Stages of the CBS – Prequalification, the Work Allocation Process will be discussed with prequalified bidders in ITR wave 5 of Stage 5.</p>
<p>51</p>	<p>The requirement for existing GC Cloud Framework Agreement (“current FA”) holders having to re-qualify for this Solicitation. We request that all existing FA holders be automatically qualified and moved past the Prequalification phase of this Solicitation.</p>	<p>No, existing FA holders will not be automatically qualified and will not move past the Prequalification phase of this Solicitation. The Cloud Framework Agreement and this solicitation or two distinct procurement processes, each with its own unique set of requirements and prequalification criteria. In order to uphold fairness, it is of the utmost importance that all Bidders undergo the same evaluation process. This ensures equal opportunities for</p>

		<p>all parties involved and promotes transparency in the selection and decision-making process.</p>
<p>52</p>	<p>The award of only 2 or 3 Task Authorization Contracts. Specifically, we object to section 4.3 (Number of contracts and qualified vendors permanent list) of Section 4 (Evaluation Procedures and Basis of Selection) of the Prequalification document. We request that there be no limit on the number of Task Authorization Contracts awarded; all current FA holders should be awarded a TA Contract and be eligible to fairly compete for individual Task Authorizations. Other GC vehicles have qualified significantly higher numbers of suppliers to promote vigorous competition. This Solicitation seems to be designed to limit competition.</p>	<p>In many competitive procurement processes, Canada is awarding one contract. For this IaaS and Native PaaS solicitation, Canada expects to award two or three contracts. In establishing the number of selected vendors, Canada must balance the diversity of providers with the costs of maintaining multiple cloud environments.</p> <p>The decision to select two or three vendors under the IaaS and Native PaaS solicitation is informed by the necessity to put in place an ecosystem of contracts that optimizes performance for Canada and the best value for taxpayers. The IaaS and Native PaaS solicitation is only one of the procurement vehicles that will be put in place in the new ecosystem; other new procurement vehicles will be put in place for other cloud services offering.</p> <p>To ensure the fairness of the solicitation, SSC will develop the evaluation framework in collaboration with the prequalified vendors. SSC will also invite third parties to give input on the fairness of the procurement.</p> <p>Capping the number of resulting contracts does not aim to limit competition, it is aiming to optimize the procurement ecosystem. The current prequalification criteria are different from the ones that led to the selection of FA holders. Like any other bidder, current FA holders will need to submit their bids and undergo the same Prequalification process.</p>
<p>53</p>	<p>In Section 6 – Resulting Contract Clauses of the Prequalification document, we object to section 6.1.4 (“Other Jurisdictions: Canada reserves the right to allow other Canadian Jurisdictions to use the contract for Cloud Services requirements.”). This clause improperly limits competition not only within the Government of Canada but perpetuates the unfairness across the entirety of</p>	<p>This procurement process is designed to meet the needs of both the Government of Canada as a whole and potentially other jurisdictions. The practice of extending competitive contracts to other jurisdictions is intended to enhance the effectiveness of the public service ecosystem. There are several procurement vehicles within the Government of Canada that already provide access to contracts for other jurisdictions.</p>

	<p>Canada. We request that section 6.1.4 be deleted altogether, or that all current FA holders are awarded a TA Contract.</p>	<p>This approach ensures a fully competitive environment. Competition is upfront, allowing Bidders to assess the potential business opportunities from both the Government of Canada and potentially other jurisdictions. Bidders receive the same comprehensive information upfront, allowing them to make an informed decision about their interest and ability to perform the contract. This information forms the basis for their bid/no-bid decision, ensuring fairness and transparency throughout the procurement process. Therefore, Section 6.1.4 will not be deleted and all current FA holders will be required to participate in the competitive process as outlined in the solicitation documents.</p>
<p>54</p>	<p>The lack of a defined Contract Period of a Task Authorization Contract and Task Authorization Period of individual Task Authorizations. In the webinars, SSC communicated the intention to award exceedingly long contracts/task authorizations in the range of 20-25 years. We request that a time limit (e.g., 5 years) is placed on each Task Authorization Contract and an individual Task Authorization.</p>	<p>The intent is to conduct a comprehensive competition at the beginning and to establish long-term contracts. Throughout stage 5 of the process, the details of the task authorization process will be further developed and refined in collaboration with prequalified Bidders.</p>
<p>55</p>	<p>The Rated Criteria unduly favour the incumbent cloud service providers. The Criteria and Scoring Elements are weighted towards characteristics of preferred suppliers rather than the Government of Canada desired workloads or outcomes.</p>	<p>Canada has drafted prequalification criteria that align with the necessary capacities and capabilities a Contractor must possess in order to successfully execute the contract. The prequalification criteria have been tailored to mirror the specific requirements outlined in the resulting contract.</p>
<p>55a</p>	<p>In Rated Requirement 2 (R2), we request the addition FIPS140-2 as a satisfactory requirement worth 2 points.</p>	<p>For this Prequalification, Canada is limiting the security questions to a requirement that is representative of the capacity the Contractor will need to have to meet the requirement of the contract. FIPS 140-3 is the requirement in the published ITSP-40.111 standard. It is a requirement from CCCS as of March 18, 2024. The latest version of the Prequalification Evaluation Grid from Amendment 003, allows for FIPS 140-3 "undergoing review"</p>

		that may be worth 2 points. Consequently, FIPS 140-2 certifications will retain a value of 1 point. Prior to contract award, there will be more stringent security requirements that the Bidder must meet.
55b	In R3, under the heading “Duration of services rendered to the client,” we request the deletion of the first bullet “more than or equal to 7 years = 7 points.” This unduly restricts newcomer suppliers, restricts competition and hinders the Government of Canada’s ability to benefit from new technologies.	Newcomers still earn points as this rated criterion provides a progressive scale. The longevity of Bidder’s experience is a relevant and measurable indicator of the Bidders’ capacity/capabilities. Therefore, the criterion will remain unchanged.
55c	In R3, delete the whole section “Number of employees of the client.” The number of employees of the client is irrelevant to the scalability of the cloud services within a particular organization and also irrelevant to the ability of a cloud service provider to deliver cloud services to many different end clients. For example, the developer of a popular mobile application may have many times fewer employees than the number of end users that the application serves. Therefore, the number of employees of an organization is not a fair metric for assessing the ability of a cloud service provider to scale its cloud services.	The Contractor will be required to provide services to an organization with a large number of employees. Bidder’s experience in servicing large organizations is a relevant and measurable indicator of the Bidders’ capacity/capabilities. Therefore, the scoring element based on the number of employees will remain unchanged.
56	In Section 6 – Resulting Contract Clauses of the Prequalification document, section 6.6.1, we object to subsection (c) (which states, “Provided Canada respects the Task Authorization Work Allocation Process described in this document, the Contractor has no rights against Canada with respect to the way in which Canada administers the contracts with other contractors...”) We request the deletion of s. 6.6.1(c). The Government of Canada should always be accountable for improper actions.	Agree, your concern is noted and will be discussed with prequalified Bidders during stage 5.
57	At p. 8 of the Prequalification document, Stage 8: Demonstration and Feedback states that the demonstration is mandatory to bid and Stage 10: Pre-award states that the Bidder’s written Technical Bid are not to be provided at Bid Closing. Demonstrations highly	Demonstrations provide interactive opportunities for Bidders to demonstrate their capabilities. The selection process is only notional at this stage. It will be refined and discussed with prequalified Bidders in stage 5.

	<p>favour the Government of Canada’s incumbent providers because GC’s technical resources are more knowledgeable about these suppliers; consequently, scoring a demonstration instead of a technical bid will invariably favour the incumbents.</p>	
58	<p>At p. 9, Stage 11: Incremental Contract Award, we request that all Task Authorization Contracts be awarded simultaneously to avoid providing one or two suppliers the advantage of a headstart. The impacts of this incremental award process can be seen in the current FA.</p>	<p>Your concern is noted and will be discussed with prequalified Bidders during stage 5.</p>
59	<p>Sections 1e. and 1g. are very similar and have overlapping product responses, will Canada accept a response with the same products answering both requirements?</p>	<p>These categories assess different capabilities and technologies of the publicly available Commercially Available IaaS. It is critical to the evaluation process that Bidders demonstrate how their offerings clearly meet the criteria for each specific category. It is at the Bidder’s discretion to propose the same service, but they must be confident that the service meets the criteria for both capabilities and technologies in order for Canada to distinguish this distinction in the technical evaluation.</p>
60	<p>For M2, the wording of the question implies that the bidder should submit both a certificate and a letter or audit report. In the case of ISO, no such letter exists, for SOC no such certificate exists. Can Canada please clarify that EITHER a certificate or letter is required?</p>	<p>Canada confirms that for M2 will require either a copy of the certifications and audit reports, including the date of issuance and expiration, OR a letter of verification or a statement from the issuing body confirming the current and valid status of the certification, but not both. M2 and the Prequalification Submission Form will be modified accordingly.</p>
66	<p>Requirement R2, as amended on 6 May (Amd 003), refers to ITSP.40.062 in the context of data-at-rest. However, ITSP.40.062 addresses only data-in-transit. To ensure that compliance with this requirement can be demonstrated, we request that references to ITSP.40.062 be removed in favour of ITSP.40.111.</p>	<p>Canada recognizes that ITSP.40.062 does not pertain to data-at-rest requirements. Consequently, due to the complexity of the requirement for prequalification, Canada has decided to remove element 2b) in its entirety and to revise the scoring element of 1a) and 2a). R2 and the Prequalification Submission Form will be amended accordingly.</p>
67	<p>In alignment with the guidance provided by the US FedRAMP program (https://www.fedramp.gov/blog/2022-12-22-crypto-</p>	<p>Canada has reviewed the evidence requirements for R2 and agrees to use the CMVP Modules in Process List as evidence. However, to</p>

	<p>modules-historical-status/), we request that requirement R2 be amended such that modules included on the CMVP Modules in Process List (https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Modules-In-Process/Modules-In-Process-List) are awarded 2 points.</p>	<p>be awarded for full points, the status of the module will remain "In Review" as per the CMVP process. The R2 criterion and the Prequalification Submission Form will be amended to reflect this update.</p>
<p>69</p>	<p>We strongly recommend that Canada amend requirement R1 to require the metropolitan area of data centers rather than the precise location.</p>	<p>In response to numerous requests, Canada has agreed to accept the postal code for requirement R1. However, Bidders are reminded that the complete physical address is required and will be subject to validation at Stage 10 of the procurement process.</p>
<p>72</p>	<p>The scoring methodology for this section (Part B - Rated Criteria R4) using a “comparative assessment isn’t as clear or explicit as other rated criteria such as R3. Considering this, will SSC update the question to provide more clarity into the specific number of points allocated and how this will contribute to the overall score of up to 29 points?</p>	<p>Canada will provide an illustrative example for the assessment of R4 using five bidders: A, B, C, D, and E. For the purposes of this example, let’s consider their respective number of regions for element 1: Bidder A has 8 regions. Bidder B has 1 region. Bidder C has 5 regions. Bidder D has 5 regions. Bidder E has 3 regions. The bidders are ranked from the highest to the lowest number of regions. The ranking and corresponding points would be as follows for element 1: Bidder A, with the most regions, is ranked first and receives 3 points. Bidders C and D, who have the same number of regions, will each be ranked second and receive 2 points each. Bidder E is ranked third and receives 1 point. Bidder B, with the lowest number of regions, will receive 0 points. This scoring approach will be applied to elements 1 through 9. The total score for each bidder will be the sum of all points accumulated for each element, plus the sum of elements 10 and 11. For example, if Bidder A received 3 points for element 1, 2</p>

		<p>points for element 2, and 0 points for element 3, and so on, its total score would be calculated as $3 + 2 + 0 + \text{etc.}$</p> <p>To achieve the maximum score of 29 points, a bidder would need to rank highest for each element from 1 to 9, thereby receiving 3 points for each, and also receive 1 point each for elements 10 and 11. This cumulative score across all elements would result in the full 29 points.</p>
--	--	--

Note: The numbering of the questions below is not chronological due to the presence of duplicates. These duplicates have been removed from the table to avoid confusion.

Section B – Modifications to the Solicitation

1-In Section – Instructions to Bidders

At Section 2.1

Delete: ‘Bidders who submit a Bid agree to be bound by the instructions, clauses and conditions of the Challenge-Based Solicitation and accept the clauses and conditions of the resulting Contract “in its entirety

Replace with: “Bidders who submit a Bid agree to be bound by the instructions, clauses and conditions of the Prequalification Challenge-Based Solicitation. “

At Section 2.3

Delete: “Acceptance by Bidders of SSC – RESULTING CONTRACT CLAUSES (Section 6), including the Annex A – Cloud General Terms and Conditions, is a mandatory requirement of this Solicitation”

Replace with: “Acceptance by Bidders of SSC – RESULTING CONTRACT CLAUSES (Section 6), including the Annex A – Cloud General Terms and Conditions, is a mandatory requirement of the Final CBS Solicitation.”

2- In Attachment 1—Prequalification Evaluation Grid

In M2

Delete: The information required by Bidder in its entirety

Replace with:

“The Bidder should provide the following evidence:

- 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.
- For SOC 2: copy of the audit reports, date of issuance and expiration (as applicable).”

In R1

Delete: R1 in its entirety

Replace with:

R1	<p>Capacity to satisfy data residency requirements (maximum 15 points)</p> <p>The Bidder should have a minimum of two data centres located in a single region in Canada.</p> <p>Canada uses the Uptime Institute’s Tiered Classification System for the Data Centre definition. For the purpose of this solicitation:</p>	<p>The Bidder should provide the physical address of two data centres located in a single region in Canada.</p> <p>If the Bidder chooses not to provide the physical address, they can provide:</p> <ul style="list-style-type: none"> • the bidder public designation of each DC; • the complete postal code; and 	<p>Up to 15 points will be allocated. Points will be allocated as follows:</p> <p>15 points: the Bidder has provided the physical address or postal code of 2 data centres located in a single region in Canada.</p> <p>10 points: the Bidder has provided the physical address or postal code of 2 data centres located in Canada not within the same region.</p>
----	--	--	--

<p>A Data Centre (DC) is a physical infrastructure that meets or exceeds the “Data Centre Tier III” requirements.</p> <p>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.</p>	<ul style="list-style-type: none"> the direct distance (in km) between the DCs. 	<p>5 points: the Bidder has provided the physical address or postal code of one data centre located in Canada.</p> <p>0 points: the Bidder has not provided the physical address or postal code of any data centre located in Canada.</p>
---	--	---

In R2

Delete: R2 in its entirety

Replace with:

<p>R2 Capacity of the Bidder’s Solution to protect Canada’s data (maximum 12 points)</p> <p>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.</p> <p>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-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)</p> <p><i>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.</i></p>	<p>1. For Data-in-transit:</p> <p>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:</p> <p>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</p> <p><u>For validated module:</u> Bidder should provide the module name and the certificate number. <u>For module undergoing review:</u> Bidder should provide the module name and the status of validation for FIPS 140-3 in the Modules In Process List by the CMVP.</p> <p>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.</p> <p>Bidders should provide the algorithm name and the applicable table in the ITSP.40.062.</p> <p>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.</p> <p>Bidders should provide the validation number</p> <p>2. For Data-at-rest:</p>	<p>Up to 12 points will be allocated.</p> <p>1. For Data-in-transit:</p> <p>Points will be allocated as follows:</p> <p>a) Cryptographic module:</p> <p>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.</p> <p>1 point: The Bidder has provided a certificate number demonstrating that the module is validated under FIPS 140-2 by the CMVP.</p> <p>0 points: Not CMVP validated.</p> <p>b) Encryption algorithm:</p> <p>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.</p> <p>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.</p> <p>0 points: Any other algorithm not in one of the tables under recommended and sufficient columns in the ITSP.40.</p> <p>c) Cryptographic algorithm:</p> <p>2 points: The Bidder has provided a validation number demonstrating that the cryptographic algorithm is validated by the CAVP</p>
--	---	---

		<p>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:</p> <p>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</p> <p><u>For validated modules:</u> Bidder should provide the module name and the certificate number.</p> <p><u>For module undergoing review:</u> Bidder should provide the module name and the status of validation for FIPS 140-3 in the Modules In Process List by the CMVP.</p> <p>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.</p> <p>Bidders should provide the validation number.</p>	<p>0 points: The Bidder has not provided a validation number demonstrating that the cryptographic algorithm is validated by the CAVP</p> <p>2. For Data-at-rest:</p> <p>Points will be allocated as follows:</p> <p>a) Cryptographic module:</p> <p>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.</p> <p>1 point: The Bidder has provided a certificate number demonstrating that the module is validated under FIPS 140-2 by the CMVP.</p> <p>0 points: Not CMVP validated.</p> <p>b) Cryptographic algorithm:</p> <p>2 points: The Bidder has provided a validation number demonstrating that the cryptographic algorithm is validated by the CAVP.</p> <p>0 points: The Bidder has not provided a validation number demonstrating that the cryptographic algorithm is validated by the CAVP.</p>
--	--	--	--

3 - In the Prequalification Documents

Delete: Bid Document 1—Prequalification Bidding Form, in its entirety

Insert: New version of the Prequalification Bidding Form V1.2.

All other terms and conditions remain unchanged.