Public Works and Government Services Canada | Travaux publics et Services gouvernementaux Canada

RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:
Email to:
TPSGC.PADivisionQE-APQEDivision.PWGSC@tpsgc-pwgsc.gc.ca

SOLICITATION AMENDMENT
MODIFICATION DE L'INVITATION

The referenced document is hereby revised; unless otherwise indicated, all other terms and conditions of the Solicitation remain the same.

Ce document est par la présente révisé; sauf indication contraire, les modalités de l'invitation demeurent les mêmes.

Comments - Commentaires

Vendor/Firm Name and Address
Raison sociale et adresse du fournisseur/de l'entrepreneur

Issuing Office - Bureau de distribution
Security and Information Operations Division/Division de la securite et des operations d'information
11 Laurier St. / 11, rue Laurier
8C2, Place du Portage
Gatineau
Québec
K1A 0S5

Title - Sujet ITI in Sp of C2 Project	
Solicitation No. - N° de l'invitation W8474-18IT01/B	**Amendment No. - N° modif.** 013
Client Reference No. - N° de référence du client W8474-18IT01	**Date** 2020-04-29
GETS Reference No. - N° de référence de SEAG PW-$$QE-450-27248	
File No. - N° de dossier 059qe.W8474-18IT01	**CCC No./N° CCC - FMS No./N° VME**
Solicitation Closes - L'invitation prend fin **at - à 02:00 PM** **on - le 2021-03-31**	**Time Zone** **Fuseau horaire** Eastern Daylight Saving Time EDT
F.O.B. - F.A.B. **Plant-Usine:** ☐ **Destination:** ☑ **Other-Autre:** ☐	
Address Enquiries to: - Adresser toutes questions à: See herein	**Buyer Id - Id de l'acheteur** 059qe
Telephone No. - N° de téléphone (819) - ( )	**FAX No. - N° de FAX** (819) -
Destination - of Goods, Services, and Construction: **Destination - des biens, services et construction:**	

Instructions: See Herein

Instructions: Voir aux présentes

Delivery Required - Livraison exigée	**Delivery Offered - Livraison proposée**
Vendor/Firm Name and Address **Raison sociale et adresse du fournisseur/de l'entrepreneur** **Telephone No. - N° de téléphone** **Facsimile No. - N° de télécopieur**	
Name and title of person authorized to sign on behalf of Vendor/Firm (type or print) **Nom et titre de la personne autorisée à signer au nom du fournisseur/ de l'entrepreneur (taper ou écrire en caractères d'imprimerie)** **Signature** **Date**	

Canada

Amendment 013

This amendment is raised in order to:

I. Provide industry with the additional information on a possible cloud solution as described below;

Possible Secret-level Cloud Implementation

This section provides information regarding a possible Department of National Defence (DND) Secret-level cloud implementation. This information is provided for discussion and feedback purposes, with the assumption of beginning the implementation in a 2-4 year timeframe (before end 2024), and does not necessarily represent the proposed way ahead.

Data Centre Location Options for Secret Cloud

The data centres could be located in either Cloud Service Provider (CSP) or DND/Government of Canada (GC) facilities, depending on which approach would best meet DND effectiveness, efficiency, and operational requirements. Given the data centre geographic separation requirements associated with survivability criteria, as detailed in Annex B of the RFI, it is assumed that a single CSP geographic location would not be sufficient to achieve DND's objectives and that the implemented architecture would therefore include at least two fully independent data centres. This leads to the following options for selecting sites:

- Multiple CSP locations only;
- Mix of CSP and DND/GC locations; or
- Multiple DND/GC locations only.

In accordance with GC and DND data residency[1] and security policies, the data centres and all data, including backups, must be located in Canada or Canadian facilities (e.g. embassies, should such a case arise), and operated by Canadian citizens with a Canadian Secret security clearance.

Additionally, DND has a requirement to extend its Command and Control (C2) capabilities to the operational/tactical edge. If a cloud infrastructure is implemented as part of this project, that cloud and its services should be extendable to the operational/tactical edge, and be able to operate in both limited communications bandwidth environments and in extended autonomous mode during periods of loss of communications (with re-synching capabilities after communications restoral).

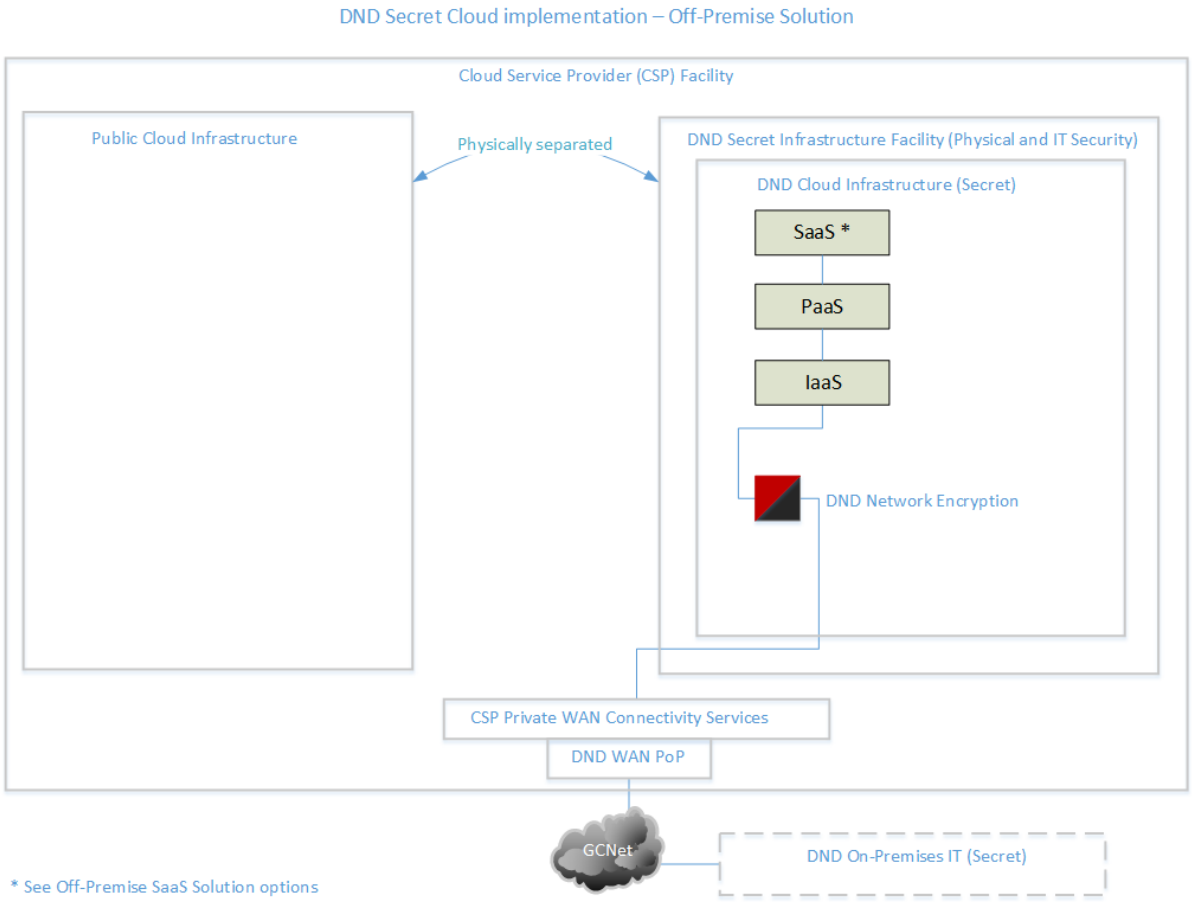
[1] Government of Canada IT Policy Implementation Notice (ITPIN) 2017-02 - Direction for Electronic Data Residency

Cloud Infrastructure

Under current policy, a Secret cloud infrastructure would need to be physically and securely separated from any CSP's commercial cloud infrastructures (up to and including the abstraction layer), as depicted in Diagram 1. Should DND implement a Secret cloud infrastructure in CSP facilities, this would require space and infrastructure that are physically separated from their commercial infrastructure, with physical and Information Technology (IT) security safeguards implemented in accordance with DND policies and standards. The implementation of those safeguards would be a combined CSP/DND effort, but final approval of the implemented security safeguards would remain solely with DND. Should a supplier implement a Secret cloud infrastructure in DND/GC facilities, DND would be solely responsible for provisioning and securing the physical space.

DND is open to a multi-tenancy, government-only, dedicated classified cloud infrastructure meeting DND confidentiality, integrity and availability requirements.

Diagram 1



Project Cloud Scope

Keeping within the National Institute of Standards and Technology (NIST) Definition of Cloud Computing terminology (Special Publication 800-145), the project's cloud scope is limited to Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) capabilities only, with the following potential exceptions for Software as a Service (SaaS) capabilities:

- A cloud-enabled office automation package, if adopted by DND at large;
- SaaS capabilities addressing IaaS and PaaS capability gaps (e.g. SaaS services required to meet DND security requirements)

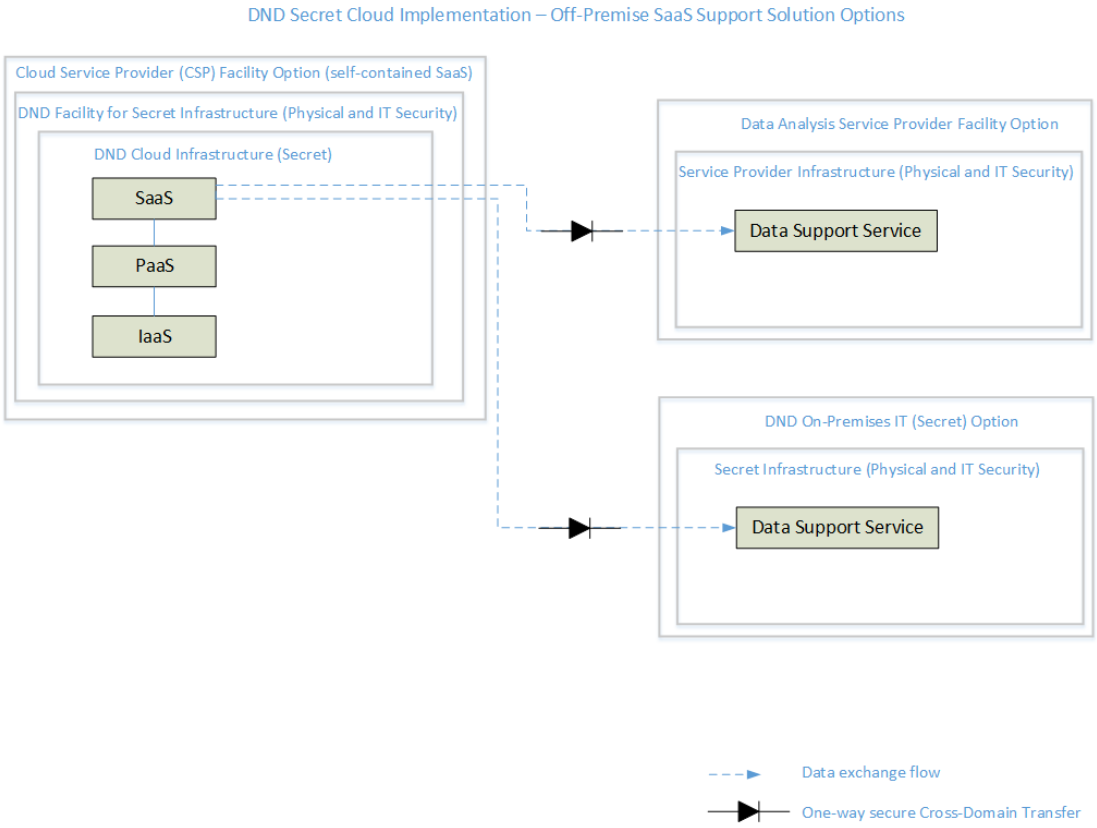
a. Applications Migration to a Cloud Environment

Generally, the Information Technology Infrastructure in Support of Command and Control (ITI in Sp of C2) project will support DND's Life-Cycle Application Managers (LCAM) in preparing their applications for migration ahead of time to the maximum extent possible, but will not control the process as this will be a DND at-large responsibility. Accordingly, it is possible that the delivered Secret IT infrastructure will retain some legacy IT infrastructure components in order to operate specialized applications that can't be migrated in any fashion to the modernized environment. In a cloud-centered infrastructure, this would lead to a hybrid environment composed of cloud and traditional data centre capabilities (either co- or separately-located).

b. Third Party Service Provider SaaS Management Capability

Should any third party provided SaaS real-time/near-real-time support capabilities be required (e.g. value-added data analytics), the data needed to enable those capabilities would also need to comply with the GC data residency restrictions defined in ITPIN 2017-02, and the same physical and IT security requirements as those applicable to a DND Secret cloud infrastructure (as shown in Diagram 1). Third Party Service Provider SaaS Support Capability options are depicted in Diagram 2.

Diagram 2



II. Issue the supplemental cloud-related questions below to industry; and

2. Pricing and Services

e. Do you provide edge computing capabilities and services that could be used to support deployed Canadian Armed Forces (CAF) missions and other special requirements (e.g. mission-critical low latency requirements services)?

f. Do you support Bring Your Own License (BYOL) (e.g. Microsoft Windows)? If so, could you provide a list of BYOL applications/software that your cloud solution supports?

g. What type of cost savings could the Government of Canada (GC) expect from using its own licenses?

h. What would your process be for implementing changes to the service catalog implemented on the Secret DND/CAF cloud?

i. Could you please provide your technical support structure, Terms of Reference (TORs), and Service Level Agreements (SLAs) response times, and describe how you would ensure that only authorized personnel perform support? Please note that support personnel requiring access to DND classified data and infrastructure to perform their functions must have Canadian citizenship and a Canadian Secret clearance.

4. Data Security and Availability

h. Could you implement a classified, physically separated cloud infrastructure (up to and including the abstraction layer) on DND/GC premises?

i. Could you implement a physically separated classified cloud infrastructure (up to and including the abstraction layer) within your own facilities, which could be accessed by DND personnel at any time?

j. Could DND place its own specialized hardware within your data centres?

5. Cloud Migration

f. At the end of the contract period, how would you support DND in migrating its data onto another environment?

6. DND Governance Requirements

b. Based on your experience, could you please provide recommendations regarding the optimal size of a DND in-house team responsible for managing its classified cloud operations?

8. Procurement

a. How much time would you require to:

i. Review and provide feedback on a draft ITQ?

ii. Respond to an ITQ?

iii. Review and provide feedback on a draft RFP?

iv. Respond to an RFP?

b. Based on your experience, how much would it cost the GC to sponsor the development of an initial high-level architecture to guide DND’s development of an RFP (e.g. competitive dialogue)? What deliverables would you propose be included with high-level architectures to validate their technical feasibility

(e.g. proofs of concept), and what would be the associated level of effort for each deliverables?

c. Based on your experience, could you provide recommendations on how proof of concept comparisons could be carried out?

9. Feedback on the additional information provided in this RFI amendment

a. Could you please provide feedback on the feasibility of the cloud implementations described in this amendment?

b. Could you please provide information on the main challenges associated with the cloud implementations described in this amendment?

c. Could you please provide alternative implementation descriptions that you believe would provide the same/similar capabilities?

d. Could you please advise of the additional costs associated with the implementation of the requirements described in this amendment?

III. Publish the Questions and Answers from the Cloud one-on-one meetings.

Question Number	Question	Answer
164	What are the next steps in this procurement process? Are there any planned future engagements or opportunities for industry to work with Canada?	At this time, there are no planned additional industry engagements for the current Options Analysis Phase. Suppliers are encouraged to continue to monitor for amendments to the RFI on the Buyandsell.gc.ca website. Going forward, an Invitation to Qualify (ITQ) may be used for some of the project's requirements, including cloud services.
165	Where should suppliers send their questions, responses and additional information?	Suppliers must submit all questions, RFI responses and additional information directly to Public Services and Procurement Canada (PSPC) at the following email address: TPSGC.PADivisionQE-APQEDivision.PWGSC@tpsgc-pwgsc.gc.ca Note that questions and any additional information can be submitted at any time (until the RFI closing date).

166	Does the process include proofs of concept and/or demonstrations prior to a Request for Proposal (RFP)?	DND is considering whether or not to conduct proofs of concept and/or demonstrations during Definition Phase, but has not yet determined if, when and how they could be conducted. One possibility being evaluated would be to conduct proofs of concept and/or demonstrations after an ITQ. Suppliers demonstrating proposed solutions at events such as CANSEC or other public events may wish to inform PSPC at TPSGC.PADivisionQE-APQEDivision.PWGSC@tpsgc-pwgsc.gc.ca, so that project team members can consider attending. Suppliers that have suggestions on how DND should conduct the procurement process are encouraged to include that information in their RFI response.
167	Has Canada engaged with its counterparts in the United States (US) regarding the Joint Enterprise Defense Infrastructure (JEDI) requirement?	Canada is planning to exchange information with some US counterparts regarding the Joint Enterprise Defense Infrastructure (JEDI) in the near future, in order to obtain some insight and lessons learned.
168	Are suppliers able to use some of the content provided in their previous RFI response for this requested RFI response?	Yes.
169	Has Canada asked for pricing information from all the Cloud Service Providers (CSP)?	Canada included pricing questions in the RFI and is hoping that all interested suppliers will provide as much pricing information as they can. Pricing information provided by suppliers will be used solely for Canada’s internal approval process.
170	How does DND plan to procure services for public cloud, and what contract model would DND consider	The project is still in the RFI stage and DND is gathering information to better determine whether a commercially-provided public or private cloud would best serve its requirements (including security). According to

	taking for the product lifecycle?	DND's current assessment, any cloud services purchased from a CSP would need to be a physically separated, private infrastructure. Given the above, no decision has been made yet on how this requirement will be procured. Suppliers that have suggestions on how DND should procure a potential cloud solution are encouraged to include that information in their RFI response.
171	What is the RFI requested response date?	The RFI requested response date is 14 May 2020. However, Canada will continue to accept RFI responses up until the RFI closes.
172	Can Canada ask additional questions to suppliers?	Yes. Canada, via PSPC, can ask suppliers questions and seek clarifications or additional information.
173	What are the timelines for Canada's decision on the way forward for the ITI in Sp of C2 Project?	The ITI in Sp of C2 Project is currently in the Options Analysis Phase and is expected to enter Definition Phase in Spring 2021. Once in Definition Phase, the project team will identify clear project requirements and specifications, which will determine the scope of activities to implement the modernized Secret IT infrastructure.
174	Can suppliers connect their clients with DND to allow direct engagement between the two?	Yes. Suppliers can either provide the contact information for their clients or provide their clients with PSPC's contact information so that they may reach out to the Project team (through PSPC). The contact information for PSPC is TPSGC.PADivisionQE-APQEDivision.PWGSC@tpsgc-pwgsc.gc.ca. The decision on whether or not to engage with any suppliers' client(s) is at DND's sole discretion.
175	Does DND's current vendor engagement plan include demonstrations, workshops and discussions on various types of service level agreements?	Various options are still on the table. DND is open to industry advice on this topic. Please provide some recommended vendor engagement activities for DND's consideration in your RFI response.

176	Is DND engaging with France and Germany?	Not at this time. DND's focus thus far has been on engaging with stakeholders within Canada and with the US.
177	Is it possible to issue a Request for Proposal (RFP) before an ITQ?	No. If DND decides to conduct an ITQ, it would occur before the issuance of an RFP. However, an ITQ is not a prerequisite to an RFP.
178	Can a supplier provide more than one RFI response?	Yes, a supplier can provide any information that becomes available after the submission of their initial response, until the RFI closes.
179	How would any enhancements be funded over the course of the contract?	Canada is still considering various contracting options to allow for potential enhancements and innovation. One option would be to secure funding for Additional Work Requests (AWRs) that could then be used to cover any enhancements and upgrades not originally included in the contract.
180	Is there an advantage to having a Federal Risk and Authorization Management Program (FedRAMP) certification?	FedRAMP is not something that DND is currently considering asking for as part of its assessment process. DND is typically looking for ISO certifications, System and Organization Controls (SOC) 2 reports and Canadian Standards Association (CSA) group certifications. While this wouldn't provide suppliers any advantages, it may be easier for DND to assess/approve solutions that are already FedRAMP certified.
181	Is there an opportunity for a supplier to provide service integration?	Canada has yet to determine the procurement approach for the project, as this will be dependent on the type of solution(s) selected. Once the types of solution(s) and service(s) have been determined, Canada will then determine how best to procure them. Suppliers that have suggestions on how Canada should procure potential cloud solutions and services are encouraged to include that information in their RFI response.

182	Does DND currently use VMware?	Yes.
183	Is DND looking at a totally disconnected cloud for its secret infrastructure?	Yes. DND's current intent is to implement a private physically separated cloud infrastructure, which would also include cloud components supporting CAF missions. These components would be required to provide services to deployed CAF members relying on high latency, low bandwidth networks that are partially connected or completely disconnected from the enduring cloud infrastructure.
184	Would DND consider using the Shared Services Canada (SSC) data centre in Borden?	That option is being considered by DND. DND is seeking industry's advice and recommendations on the advantages and disadvantages of using a Government of Canada (GC) data centre to host a commercially provided cloud infrastructure.
185	Has DND considered leveraging existing investments in VMware to accelerate adoption?	It is too early in the process to make that determination. DND is seeking industry's advice and recommendations on the advantages and disadvantages of doing so.
186	Is DND looking at a hybrid solution?	DND expects that the solution will likely be a hybrid environment comprised of both cloud and traditional IT infrastructures, as some current specialized applications can't operate in a virtualized environment.
187	Is Software Defined-Wide Area Network (SD-WAN) in scope for this project?	Yes. DND is looking at all technologies of potential value for its solution(s), including SD-WAN.
188	Is DND planning to leverage Commercial Solutions for Classified (CSfC)?	Yes, DND is seeking to leverage CSfC wherever appropriate. For example, but not limited to: encryption of Local Area Network (LAN) connections to the desktop; and, data at rest encryption.

189	Is DND employing Kubernetes in its environment?	No, as DND doesn't currently have any workloads operating in a cloud environment at the Secret-level (to the best of the project team's knowledge). Suppliers are encouraged to include information on the advantages, disadvantages, and potential use cases of Kubernetes in their RFI response.
190	Does DND have any workloads operating in containers?	Not at the Secret level, to the best of the project team's knowledge. However, the project team is developing a cloud strategy, which could entail the use of containers. Suppliers are encouraged to include information on the advantages, disadvantages, and potential use cases of containers in their RFI response.
191	Do the CAF envision deploying on missions with their entire applications load or just a subset?	The CAF rely on a variety of applications, including mission critical applications that include legacy software. Some of the environments that the CAF operate in are austere with limited or no local communications. As a result, IT deployments are often limited to a subset of applications to optimize their operation over low bandwidth and high latency network segments.
192	Is DND considering a multi-cloud infrastructure?	A multi-cloud infrastructure may not be affordable within DND's current budget, as each cloud infrastructure would need to be physically separated to meet security requirements. Notwithstanding the above, DND is seeking industry's advice and recommendations on the advantages and disadvantages of using a multi-cloud infrastructure.
193	What are the relationships between the Cyber Defence Decision Analysis and Response (CD-DAR), the Network Command and Control Integrated Situational	The networks in-scope for each of the projects are not the same. The scopes of the CD-DAR and Net C2 ISAC projects are not solely limited to Secret networks, whereas the ITI in Sp of C2 Project's scope is limited to only Secret networks. Additionally, the ITI in Sp of

	Awareness Capability (Net C2 ISAC) and the ITI in Sp of C2 projects?	C2 Project doesn't include Cyber Defence within its scope, as it is planning to leverage the solutions delivered by the other two projects. Furthermore, these Cyber projects might provide some IT Service Management (ITSM) related functions, but only within the scope of their projects; on the other hand, the ITI in Sp of C2 Project must deliver an enterprise solution. Further information can be found in RFI Amendment 005, Question and Answer #69.
194	Is DND considering the option of adopting a commercial cloud through the Cyber Security Procurement Vehicle (CSPV) and Shared Services Canada (SSC)?	Not at this time. DND's requirement under this project is for a high integrity, high availability, and physically separate cloud infrastructure. DND's understanding is that these requirements can't be addressed through the CSPV and SSC at this time.
195	How does the Secure Cloud Enabled/Enabling Defence (SCED) Project align with this project?	At this time, the SCED Project's scope is limited to public cloud connectivity for environments up to Protected B. As such, there is no direct linkage between the SCED Project and the ITI in Sp of C2 Project.
196	Is DND considering the use of a system integrator to implement the new infrastructure?	DND is considering various options. DND is seeking industry's advice and recommendations on the advantages and disadvantages of using system integrators for the purpose of implementing a cloud solution.
197	Will there be a requirement to employ professional services to help with the definition and implementation of the solution?	DND is considering various options. DND is seeking industry's advice and recommendations on the advantages and disadvantages of using professional services for the purpose of implementing a cloud solution.
198	When DND refers to "air-gapped", is DND looking at a dedicated connection to the CSP?	"Air-gapped", "dedicated" and "physically separated" are terms being used to describe that any commercial cloud infrastructure procured by this project must be completely separated from the CSP infrastructure used to serve other customers.

		As for connectivity, DND is considering extending its government Wide Area Network (WAN) to CSP data centre facilities, as required, in order to meet its service capability requirements.
199	Could DND define what is meant by tactical edge?	Tactical edge generally refers to providing services at deployed mission headquarters and interfacing with lower-level mission networks (e.g. Canadian Deployable Mission Network, Federated Mission Networking, etc.). This applies both domestically and abroad, and is intended to provide a subset of services in support of missions where the CAF may or may not have robust reach-back capabilities.
200	Will DND implement confidentiality data labelling for all data?	Yes. DND is planning to apply confidentiality data labels to all data in the modernized Secret-level infrastructure, both structured and non-structured, in accordance with National Defence Security Orders and Directives (NDSOD) Technical Standard 6, Allied Data Publication (ADatP) 4774 – Confidentiality Metadata Label Syntax, and ADatP 4778 – Metadata Binding Mechanism.
201	Is DND willing to share total system responsibility with a supplier?	No. The DND/CAF will retain total system responsibility of the entire Secret IT infrastructure through appropriate mechanisms, including contractual service level agreement obligations for outsourced services. However, responsibilities will be shared between the DND/CAF and suppliers as required to best meet the objectives of the project. This includes potentially outsourcing the provision of services (e.g. storage, email, etc.) where deemed in the best interests of DND/CAF.
202	Are North Atlantic Treaty Organization (NATO) work references acceptable to DND?	At this time, DND is considering accepting NATO references.

203	The original RFI refers to core services and infrastructure. Is the implication that those are part of what needs to be delivered or that the infrastructure needs to be able to host those types of services?	DND may request that all or some of the core services be delivered along with the infrastructure. Options in that regard are still being assessed. For example, DND might decide to provide some of the core services itself, such as under a Bring Your Own License (BYOL) environment, if this better meets its overall objectives. DND is seeking industry's advice and recommendations on the advantages and disadvantages of this approach.
204	Annex B, section 2.1 of the RFI states that the system must use Commercial-Off-The-Shelf (COTS), Government-Off-The-Shelf (GOTS) or Military-Off-The-Shelf (MOTS) components. Is there a list of acceptable GOTS and MOTS applications/components?	Not at this time. However, during the Definition Phase, DND is planning on finalizing and providing a list of applications that must be migrated to the modernized Secret infrastructure, along with relevant application migration information. Otherwise, it is expected that it will be the Contractor's responsibility to ensure that applications/components, regardless of whether they are COTS, GOTS or MOTS, meet DND's requirements, as documented in Annex B of the RFI. It should be noted that the intent of that specific design and concept guidance is to minimize the usage of customized IT infrastructure solutions.
205	Could the provision of conference call services be outsourced to a third party vendor?	Yes, this would be possible, as long as the implemented solution meets DND's security requirements.
206	Could DND's existing teleconference bridge be leveraged to provide teleconference services?	Yes, this would be possible, as long as the implemented solution meets all the project requirements.
207	Will the project follow the Communications Security Establishment's (CSE) IT Security Risk Management: A	Yes. The project team will follow the principles of ITSG-33 and, more specifically, implement a Secret/High Integrity/High Availability (S/H/H) Security Control Profile. The specifics of the S/H/H Security Control Profile will be clarified in Definition Phase.

	Lifecycle Approach (ITSG-33)?	
208	Is the Consolidated Secret Network Infrastructure (CSNI) in scope for this project?	Yes.
209	Is DND looking for industry's input on how best to consolidate networks?	Yes. DND is seeking industry's advice and recommendations on how best to consolidate the (in-scope) networks.
210	In Annex B of the RFI (at section 4.1), DND states that they must maintain sovereignty over computing resources. Could you please clarify the requirement?	This is a requirement for all data to be processed and stored in Canada. However, data in transit can travel, if encrypted, outside of Canada. In this context, Canada is deemed to also include Canadian controlled facilities located outside the geographic boundaries of the country, such as deployed CAF headquarters and Canadian embassies (e.g. to meet edge support requirements).
211	In Annex A of the RFI (at section 1.3), there is a statement in the Secure IT Infrastructure business outcome that a security framework will be established. Could DND please clarify the meaning of that statement?	The security framework consists of a series of documented processes used to define policies and procedures around the implementation and on-going operations and management of information security controls in the IT environment. However, this is a business outcome sought by DND/CAF, and should not be perceived as a requirement. Project requirements, including security, are specifically defined in Annex B of the RFI.
212	Is DND open to suppliers making recommendations on the security architecture?	Yes. DND is actively seeking industry's advice and recommendations on the security architecture.
213	Is the purpose of this exercise to understand what is available from a cloud security perspective for solutions at the classified level?	Yes, DND is looking at implementing a cloud solution for its Secret-level environment. The purpose of this exercise is to give advance notice to industry that DND is interested in implementing cloud, and to seek advice and recommendations from industry on multiple aspects, including cloud security solutions.
214	Could Software as a Service (SaaS) solution(s) be	DND is currently investigating Infrastructure as a Service (IaaS) and Platform as a Service

	included in the future for this requirement?	(PaaS) solutions as it pertains to its project scope. The following areas are potential for exception: - A cloud-enabled office automation package, if adopted by DND at large; - SaaS capabilities addressing IaaS and PaaS capability gaps (e.g. SaaS services required to meet DND security requirements) DND is seeking industry's advice and recommendations on the usage of any specific SaaS solutions.
215	Does DND want to develop a better understanding of network infrastructure virtualization?	Yes, DND is interested in understanding various technologies that pertain to the project scope, including network infrastructure virtualization. Note that the WAN is outside the project's scope. DND is also interested in identifying ways to leverage technological innovation to improve agility. One of the biggest drivers for this requirement is to ensure the modernized Secret IT infrastructure can support Artificial Intelligence (AI) and big data capabilities.

ALL OTHER TERMS AND CONDITIONS REMAIN UNCHANGED.