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

RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:

Bid Receiving - PWGSC / Réception des soumissions - TPSGC
11 Laurier St. / 11, rue Laurier
Place du Portage , Phase III
Core 0B2 / Noyau 0B2
Gatineau
Québec
K1A 0S5

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 CD-DAR - ITQ Invitation to Qualify: Cyber Defence – Decision Analysis and Response	
Solicitation No. - N° de l'invitation W6369-20CY06/C	**Amendment No. - N° modif.** 009
Client Reference No. - N° de référence du client W6369-20CY06	**Date** 2021-07-16
GETS Reference No. - N° de référence de SEAG PW-$$QE-049-28197	
File No. - N° de dossier 049qe.W6369-20CY06	**CCC No./N° CCC - FMS No./N° VME**

Solicitation Closes - L'invitation prend fin
at - à 02:00 PM Eastern Daylight Saving Time EDT
on - le 2021-07-28 Heure Avancée de l'Est HAE

F.O.B. - F.A.B.
Plant-Usine: ☐ **Destination:** ☑ **Other-Autre:** ☐

Address Enquiries to: - Adresser toutes questions à: Wight, Patti	**Buyer Id - Id de l'acheteur** 049qe
Telephone No. - N° de téléphone (873) 355-3543 ( )	**FAX No. - N° de FAX** ( ) -

Destination - of Goods, Services, and Construction:
Destination - des biens, services et construction:
See Herein

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

THIS SOLICITATION AMENDMENT 009 IS ISSUED TO:

1. Provide answers to Bidders' questions on the Invitation to Qualify.
2. Amend the Invitation to Qualify as detailed below:

Amendment 009-1

REFER: Table 2 – Point Rated Technical Evaluation Criteria – R3

DELETE: In its entirety

INSERT:

R3		The Respondent has Successfully Implemented one (1) Complex IM/IT Project in the last seven (7) years, which included the design, development, integration, implementation, and delivery of Cyber Security and Cyber Decision Analysis and Response COTS/GOTS/MOTS integrated solutions and re-synchronization within FVEY nations and provision of at least 12 months of Stabilization Support for all of the following in a given network: (a) within a globally distributed network components on two (2) or more continents with a minimum of ten (10) separate operating nodes, (b) interconnected at disadvantaged speed (less than 1.544 Mbps links) remoted in austere environments to a High speed (100Mbps or above) central network, and (c) for Cyber Security related data or information a network of: i) 2001 to 4000 endpoints; ii) 4001 to 6000 endpoints; iii) 6001 to 8000 endpoints; and iv) More than 8000 endpoints For R3 (c), the Respondent project must include a minimum of 5 of 9 of the examples listed below of Cyber security related data and information. 1. The identification and tracking of authorized and non-authorized IM/IT assets; 2. Information related to each of the assessment of vulnerabilities, configuration, risk and patch compliance;	**Points will be awarded based on the number of endpoints for the project.** **Maximum: Twenty (20) points** 5 points 10 points 15 points **20 points**		The Respondent must provide a maximum of one (1) reference project in the last seven (7) years for which the Respondent has Successfully Implemented Cyber Security and Cyber Decision Analysis and Response COTS/GOTS/MOTS integrated solutions within FVEY nations for the Rated Criteria R3

	3. The analysis of cyber threat information; 4. Detection and assessment logs for suspicious activity; 5. The execution of prevention and response to threats and remediation actions in near real time; 6. Data feeds of cyber threat and analysis information from multiple sources; 7. Threat intelligence information; 8. Integrated Cyber Security incident, data analysis and security alerts; 9. The processing of structured and unstructured data related to cyber security.			

All other Terms and Conditions remain unchanged.

Table of ITQ Questions and Answers

Questions and Answers in Amendment 002		
No.	**Question**	**Answer**
1	Ref: 1.2.3 Scope of Anticipated Procurement: It is Canada's intention to have an iterative and phased approach to the implementation." Does this infer that Canada will require a development and project management approach to implementing CD-DAR (in the same approach used for Net C2 ISAC) rather than Canada procuring COTS/MOTS/GOTS security tools as a complete solution?	The CD-DAR Project's intention is to request a design and delivery of the capability based on COTS/MOTS/GOTS solutions. The solution(s) will be integrated through an iterative and phased approach by a Prime Integrator into a full and complete solution for the CD-DAR Project.
2	Does Canada anticipate that DND will act as the integrator for the CD-DAR solutions procured under contract or will industry be required to integrate them to CFNOC?	The CD-DAR capability integration within DND/CAF will be undertaken by the Prime Integrator, in coordination/direction of the PM Team.
3	Ref: Annex A, Table 1 – M1 – "FVEY Nations". Does this reference a military or government customer within US, UK, Australia, NZ or CAN or can the project reference come from a non-government entity within those FVEY nations?	"FVEY Nations" does not refer to military or government customer, but any customer within AUS, CAN, NZ, UK or US so the project reference may come from a non-government entity within one of the FVEY nations.
4	Will the Government release the documents in Word version for easier transcription for responses?	Canada will not release the documents in MS Word. Suppliers are directed to use the features of PDF software to convert the documents into editable text.
Questions and Answers in Amendment 003		
5	Ref: Annex A, Table 1 and 2. Can Canada please clarify that project references with COTS solutions within the commercial environment are acceptable as references for CD-DAR?	Canada will accept project references with COTS solutions within FVEY nations' commercial environment.
6	Can Canada address a recommendation that the scope of the project references be expanded to include NATO countries as well as FVEY nations?	Canada will only consider references covering experience within FVEY nations.
7	We would like to know potential partners we should be approaching with our solution. Is it possible to provide the names of which integrators or resellers bid in the initial phase of this process? Does Canada have a list of preferred integrators that could be provided?	As this is the first phase of the CD-DAR procurement PSPC currently has no list of interested suppliers nor a list of preferred integrators to provide. This ITQ will create the source list of qualified suppliers. Suppliers who are looking for partnering opportunities are invited self identify and put their name on the List of Interested Suppliers (LIS) linked to the ITQ posting on buyandsell. Instructions for joining the list are provided on the right side of the posting under the title "Find out who is interested in this tender"
Questions and Answers in Amendment 004		
8	Can Canada please clarify the purpose of the currently posted CD-DAR RFI No W6369-20CY06/B?	The RFI W6369-20CY06/B is not currently requesting any supplier responses. This RFI will remain open after the ITQ has closed and will be used to continuously inform industry of the CD-DAR procurement process.

9	Canada has mentioned that the ITB Policy will apply to the Cyber Defence – Decision Analysis and Response project. Can Canada provide any information on the potential terms and conditions related to the ITB Policy at this time?	The Industrial and Technological Benefits (ITB) Policy will apply to the Cyber Defence – Decision Analysis and Response project. The ITB Terms and Conditions (T&Cs) are provided at this time for informational purposes only and are subject to change. These T&Cs form the foundation on which any ITB requirement in a future CD-DAR contract may be based. ITB requirements for CD-DAR will be developed with any subsequently Qualified Suppliers, in conjunction with the ITQ engagement process. Any finalized ITB requirements specific to the CD-DAR project will be captured in a Request for Proposal for CD-DAR. Information on the ITB Policy, including Value Proposition can be Found at www.canada.ca/itb.
Questions and Answers in Amendment 005		
No.	**Question**	**Answer**
10	In order to protect the Crown and the procurement, we would like to clarify whether the definition of "entity" in section 2.2.2 of 2.2 Teaming Terminology's reference to "association" is intended to be a reference to the defined term "association of entities". "Entity" refers to any individual, corporation, partnership, firm, Joint Venture, syndicate, association, trust or other form of legal entity. (2.2.2 of 2.2 Teaming Terminology) "Association of Entities" means separate legal entities within a formally organized professional services network, where all members of the network operate using a common brand, with shared access to intellectual property, talent resources, integrated technology, methodology, strategies and policies across the network. It does not include unrelated affiliates of the Respondent with whom the Respondent is partnering through a Respondent Core Team or Joint Venture (as applicable). (2.2.1 of 2.2 Teaming Terminology) We believe and are hoping Canada's intent was to refer to "association of entities", as defined in section 2.2.1 of 2.2 Teaming Terminology, as this would ensure that firms with global qualifications within the Five Eyes (FVEY) Nations, which operate as separate legal entities within a formally organized professional services network, would be able to use projects to substantiate the mandatory	Section 3.4 of the ITQ explains how the experience of a Respondent Core Team will be evaluated for the purposes of the ITQ. "Association of entities" can submit a response to the ITQ. However, unless such response is submitted as a joint venture, one team member will need to be the "Prime Respondent". The other members of the "association of entities" will need to be submitted as "Core Team members".

	and point rated criteria which were not delivered in Canada. Not only us, but the entire industry would benefit from this modification, as it would allow respondents to leverage a broader range of global qualifications from their firm network within the FVEY nations. This also benefits Canada by enabling a more competitive process, which includes global experience of firms that operate as an association of entities in their ITQ responses, providing Canada with the best representation of respondents' qualifications and experience. We do not believe that Canada's intent was to be unnecessarily restrictive and that the intent was to include the term "association of entities" in the definition of "entity". Since the term "association" is not included in the list of definitions under section 2.2 Teaming Terminology and the term "association of entities" is defined under section 2.2 Teaming Terminology, but appears nowhere else in the ITQ, it our belief that the intention was to include "association of entities" in the definition of "entity". Can Canada please confirm that an association of entities qualifies as an entity by releasing an updated version of the ITQ with this correction?	
11	Can the Crown confirm that a project reference to substantiate the mandatory and point rated criteria in which the Respondent acted as both the client and the supplier is acceptable?	A project reference to substantiate the mandatory and point rated requirements in which the Respondent acted as both the client and the supplier would not be acceptable.
12	In order to help the Crown evaluate the experience and ability of the Respondents in successfully designing, developing, integrating, implementing, and delivering previous Cyber Security and Cyber Decision Analysis and Response integrated solutions, can the Crown confirm that a project reference to substantiate the mandatory and point rated criteria in which the location of work performed was within the FVEY nations, but the client contact resides outside the FVEY nations is acceptable?	A client contact for the referenced project may reside outside of the FVEY nations but as per the mandatory and point rated criteria, the project must have been completed within a FVEY nation for a FVEY customer. Interested respondents are reminded to review the security requirements in section 1.2 Security Requirements for Phase 3 – Due Diligence, Phase 4 – RFP and section 1.3 Security Requirements for Phase 5 - Contract. These Security Requirements include limiting, to varying degrees, the Draft RFP/RFP and Contract to citizens of Canada, United States, United Kingdom, Australia, or New Zealand.
13	Ref: Annex A, Table 1, Table 2. Please confirm that projects successfully implemented onto the CSNI would be compliant to the requirements that reference "within Complex IM/IT Networks of 8,000 or more Endpoints", within FVEY nations.	At this time, we can not confirm if the referenced project completed on CSNI would be compliant. As part of the submission, the Respondent must clearly demonstrate that the referenced project was completed on a large enough area of the network to meet the 8000 node requirement.
14	Pursuant to Annex B: Security Requirements, Company A (USA) individually meets all of the requisite security requirements. Company B (Canada) meets several, but not all of the requisite security requirements. Company C is the legal entity which owns both Company A and Company B. Is it acceptable to	Respondents are not required to meet the security requirements of the next phases of the procurement in order to responds to this ITQ. The required clearances may be obtained after the ITQ process. For further procurement phases any legal entity that is participating in the process must itself hold the

	Canada for the purpose of this ITQ that Company C can be identified as the Prime Respondent and the security credentials of its abovementioned holdings will be recognized in determining its compliance to the Annex B Security Requirements?	required security clearances in order access to classified information and for the legal entity to be awarded a contract. Security clearances of separate legal entities cannot be combined to meet the required security clearances.
15	We are interested in responding to the ITQ but do not currently meet the security requirements of the RFP or Contract phases. Will PSPC or DND sponsor our company to obtain the required security clearances?	Canada will only assist suppliers that have qualified under this ITQ in obtaining the required security clearances for the next phases of the procurement.
16	The ITQ asks for "Open Source Intelligence (OSINT) for multi-source and multi-caveat analysis... rapid and sustained intelligence collection, and conduct deception activities. External Threat Intelligence DND/CAF should use proactive quantitative type feeds including darkweb analysis. The system must ingest reputable, sustainable and adjustable cyber Open Source Intelligence (OSINT) service feed(s)." This would suggest that bidders should have a demonstrable capability to produce cyber threat intelligence timely and actionable products tailored to DND. They should demonstrate knowledge of adversary and particularly attacks and compromises of DND.	Experience with the capability to produce cyber threat intelligence and knowledge of adversary attacks is not limited to DND.
17	Past Performance References: Under each Mandatory Criteria from Table 1 (Mandatory Technical Evaluation Criteria) and each Point Rated Evaluation Criteria from Table 2 (Point Rated Technical Evaluation Criteria), the ITQ requests the supplier to provide a reference where similar work has been successfully implemented that includes details of the networks characteristics themselves (e.g., endpoints). This kind of detail is often considered extremely sensitive, oftentimes classified, even amongst FVEYs nations because it reveals the extent and scale of network infrastructure and operations. Hence, while we are interested in preparing a response, securing permission from our existing FVEYs customers to disclose such information presents a considerable challenge. Would DND/CAF consider making official requests via the appropriate channels to the corresponding FVEYs partner agencies with similar capabilities to disclose (at their discretion) the current vendor landscape and associated capabilities?	As part of this ITQ process, DND/CAF is not considering requesting FVEY partners to provide a list of suppliers capable of meeting the requirements of CD-DAR. Respondents are advised to refer to Annex A: Mandatory Evaluation Criteria, Section 2 Work on Classified Projects of the ITQ. This outlines the procedure to identify the Project experience as classified, and how the evaluation team, including Contract Authority with appropriate security clearance, will verify the work completed as specified in the criteria.
18	We notice that NATO country references were included in the draft ITQ, but removed from the issued ITQ. Is the DND/CAF able to share the reasons for removing NATO country references?	After further analysis and multiple consultations with various stakeholders, DND has decided to remove the requirement for NATO country references as it did not meet DND's requirement.

19	Would the DND/CAF consider receiving references from governments other than FVEYs or NATO participating countries?	References from non-FVEY governments will not be considered as they do not meet the ITQ requirements.
20	Reducing program risk by reducing complexity: CD-DAR will require a well-integrated "amalgam" of solutions from multiple providers as stated in section 4.3 of the SOR. To increase the ability to maintain a complex and comprehensive solution such as CD-DAR, we suggest that Canada rely on fewer components that need to be integrated from separate providers. By breaking down the project in smaller lots, the smaller projects can be met by well-designed, integrated solutions that carry less risk of not delivering. We believe it is important for Canada to consider that an amalgamated solution is extremely complex to integrate and deploy where the risk of delays and failure increases as the number of integrated parts increases. Is the quantity of individual component parts of the amalgamated solution also a consideration that DND/CAF will introduced into the Point Rated Evaluation Criteria?	The quantity of individual component parts of the amalgamated solution will not be introduced into the Point Rated Evaluation Criteria. Points will be allocated in accordance with the scoring criteria detailed in Table 2 of Annex A.
Questions and Answers in Amendment 006		
No.	**Question**	**Answer**
21	Please confirm that the requirement "within/for FVEY nations" includes projects deployed into both commercial and government entities, with the exception of R4, which requires deployment in a military environment.	FVEY Nations does not refer to military or government customer, but any customer within AUS, CAN, NZ, UK or US so project references may come from a deployment on a non-government entity within one of the FVEY nations. R4 however requires deployment only in a military environment.
22	ITQ states: "Cyber Threat Hunting consists in proactively and iteratively searching through networks to detect and isolate threats that evade existing security solutions and establish persistence in networks. There is a stated requirement to be able to monitor and control its cyberspace so it remains defensible and hunt for Advanced Persistent Threats (APTs). Also: The system must provide features and data supporting the hunt for Advanced Persistent Threats (APTs), insider threats, and indicators. Threat Hunting must Empower Cyber Operators to proactively search for malicious or anomalous activity that has not yet been identified by DND/CAF automated security tools hunting analysts need to be offensively trained." Threat hunting, advanced persistent threats (APT) and offensive cyber operations are defined in doctrine. We suggest that CAF request explicit proof that the bidder possesses these capabilities as defined by joint military doctrine	Threat hunting is not unique to military and government agencies. In order to encourage competition from different sectors of industry with cybersecurity experience, the ITQ is designed to encourage respondents from outside the military and government agencies to participate in the ITQ and earn points based on their experiences delivering cyber defense capabilities in other sectors.

	and that points are awarded to those who have experience delivering to 5 eyes militaries, security and intelligence agencies and particularly to those who have delivered to DND/CAF.	
23	There is a stated requirement for "Threat Hunting and vulnerability Discovery using artificial intelligence." We suggest allocating rated points to those who are using AI in Threat Hunting systems delivered to DND/CAF.	As detailed in Table 2 of Annex A rated points are allocated to companies that have experience in employing AI across multiple domains of cybersecurity.
24	The ITQ asks for "DDOS Protection CD-DAR will seek to provide the ability to repudiate malicious traffic targeted at an entity." Given that DDoS protection can only be implemented at a carrier level provider using upstream security and Intelligence. Does CAF intend that bidders have partnership agreements with the CAF's telecoms providers?	Partnership agreements with DND/CAF telecom providers is not required for the ITQ.
25	The ITQ Requires the "ability to attribute Advanced Persistent Threats and assess the actions and potential motives and intentions of an adversary operating on constituency networks." We infer that only bidders who have successfully demonstrated attribution of APT operating against the CAF/DND would receive full rated points.	Points will be allocated in accordance with the scoring criteria in Table 2 of Annex A. CAF/DND experience is not required to receive full points for any given rated criteria.
26	The ITQ requires bidders to have practiced "real-time Active Cyber Defence (ACD) which is the process of personnel taking an active and involved role in identifying and countering threats to systems." Active Cyber Defence and Active Cyber operations are explicitly defined in CAF doctrine and legislation as: "carry out activities on or through the global information infrastructure to degrade, disrupt, influence, respond to or interfere with the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group as they relate to international affairs, defence or security." Is it CAFs intention that Bidders demonstrate this operational capability and operations?	Respondents must demonstrate that they have the experience required in order to meet the mandatory and rated criteria detailed in Annex A.
27	The ITQ requires the capability to "conduct deception activities." The Communication Security Establishment (CSE) has provided cyber security guidance to departments on the matter of cyber deception, concealment and misdirection. Cyber deception is mandatory under ITSG33. What cyber deception activities does CAF require?	The draft Statement of Requirements (SOR) provided with the ITQ contains the information regarding the conduct of cyber deception activities.

28	Security Assessment and Authorization (SA&A) is the process by which departments ensure that only authorized software and hardware are implemented in their information technology (IT) environment. Will CD-DAR be subject to all security controls within ITSG33?	CD-DAR will be subject to all SA&A requirements, including ITSG33 security controls.
29	Will points be awarded to bidders who have successfully deployed protected B and classified cloud environments for Canada?	Points will be allocated in accordance with the scoring criteria detailed in Table 2 of Annex A.
30	The ITQ requires that "The system must provide an Endpoint Detection and Response (EDR) capability to identify the installation of malware in the form of APT on an endpoint device." Does this include mobile systems? Will full points be provided to bidders who have demonstrated detection of APT on CAF/DND endpoints?	Points will be allocated in accordance with the scoring criteria detailed in Table 2 of Annex A. Endpoint devices will include only laptop and desktop workstations. Mobile systems will not be included.
31	How will the RFP require prime contractors to invest in Key Industrial Capabilities (KICs), such as Cyber Resilience and Artificial Intelligence?	The Value Proposition (VP) and bid evaluation scoring mechanisms are designed to be a flexible framework and are adjusted on a procurement-by-procurement basis. Canada will consider competitive scoring incentives in cases where opportunities exist to leverage significant benefits for Canadians. For example, Canada may use point multipliers in the VP bid evaluation to incentivize bidder commitments for work in specific Key Industrial Capabilities (KICs). At this time, Canada is determining the best approach for leveraging economic activities related to relevant KICs through this procurement. Preliminary analysis has identified Cyber Resilience and Artificial Intelligence as KICs applicable to the CD-DAR project. Canada will determine how to leverage the relevant KICs using the VP for the CD-DAR project based on engagement with Qualified Suppliers, as well as broader industry engagement, market research and analysis, and feedback from other stakeholders. As such, following the ITQ evaluation process, Canada will engage further with the Qualified Suppliers on the CD-DAR project to develop any economic benefit requirements.
32	How will prime contractors be incented to partner with Canadian Small and Medium Businesses (SMBs)?	Small and Medium Businesses (SMBs) account for significant job creation in Canada and their participation in global value chains can result in significant growth potential. As such, the ITB Policy requires bidders to make a commitment to undertake business activities in Canada with Canadian SMBs generally no less than 15% of the contract value. On a procurement-by-procurement basis, Canada relies on relevant market analysis and industry feedback in advance of the final RFP to determine the appropriate SMB

		requirement for the given procurement, and may adjust requirements in the final RFP accordingly. In addition, Canada will consider competitive scoring incentives in cases where opportunities exist to leverage significant benefits for Canadian SMBs.
33	Please expand upon what CAF requires in terms of a Cyber Common Operating Picture (cyCOP) beyond the definition in the glossary.	At this point, we are not able to expand on the requirements other than what has already been provided in the ITQ. If Industry requires more information, this could be a discussion during the Due Diligence Phase.
34	Please expand on cyber forensic requirements.	At this point, we are not able to expand on the requirements other than what has already been provided in the ITQ. If Industry requires more information, this could be a discussion during the Due Diligence Phase.
35	Will CD-DAR training be integrated with advanced cyber operator training being delivered under the IDEaS program?	It is feasible that CD-DAR training could be integrated into all aspects of DND/CAF cyber training, including advanced cyber operator training.
36	The ITQ states: "Operational Threat, Penetration and Attack simulation capability to exercise the Cyber Test ranges. It is a replication of the set of operation systems with offline datasets allowing complete range of functionalities and running realistic scenarios for training purposes solution must provide a training simulation capability to support collective operational training in a customizable operational context." Will CD-DAR leverage current cyber test ranges? How will CD-DAR ensure the injection realistic TTPs from current threat actors? Presumably bidders would require deep operational understanding of APTs operating against CAF today.	CD-DAR will leverage current test ranges. Deep operational understanding of APTs operating against CAF is not required in order to qualify as part of the ITQ.
37	The ITQ publicly released a substantive amount of information including operational and technical requirements, ORBAT, CONOPS and capability deficiencies. Will there be an operational security plan for subsequent stages in the process?	Subsequent stages of the RFP will have additional security measures applied to it as outlined in the Security Requirements Checklist (SRCL).
38	The ITQ did not discuss Supply Chain Security. Will supply chain security be a requirement?	Supply Chain Security will be a requirement for future stages of the RFP.
39	Endpoint Specifications: Given the desired scope to deploy across the entire DND/CAF Command Network, starting with Comd-Net and DWAN, the number of endpoints specified in each Serial from Table 1 (Mandatory Technical Evaluation Criteria) and Requirement # from Table 2 (Point Rated Technical Evaluation Criteria) seems quite small.	The number off endpoints specified in the ITQ evaluation criteria was selected to balance industry participation with DND requirements.

	Does the DND/CAF believe that these requirements are representative of the total scale of the project? Or are these requirements viewed as the foundational staring point?	
40	Data Formats: Mandatory Criteria M3 emphasizes the ability to parse and standardize formats. Our experience with projects of a similar nature is that data format standardization is not the primary challenge. Data scale is the most technically challenging factor that DND/CAF should consider incorporating into the ITQ. Has the DND/CAF considered including qualification criteria that includes an emphasis on a solution's ability to handle/manage data at a specified data scale?	Criteria for managing data at scale is already embedded within the mandatory criteria in Annex A.
41	Specialized tools will always be necessary – interoperability is paramount: As the DND/CAF is aware and has described in the CONOPS, the landscape of malicious cyber actors is constantly evolving. The tools of today may no longer be sufficient tomorrow. It is to DND/CAF's benefit that CD-DAR is able to accept new tooling/solutions and maintain its ability to support the mission into the future. 1) Interoperability is one of the most important pre-requisite of any successful large-scale project as appears in the HLMR #6 from the Statement of Requirements. We believe that this is the only way to guarantee that large-scale IT investments are future-proof, prevent vendor lock-in and successfully integrate with the existing landscape of our customers. We therefore suggest that interoperability with existing/future systems be included as a requirement in the ITQ. 2) The CONOPS mentions several tools/system (e.g. SIEM, threat intelligence, case management). Is it expected that those tools/systems will need to be delivered by the selected supplier as part of the solution, or will the proposed solution need to interoperate/integrate with these existing tools/systems?	1) Interoperability is not a requirement of the ITQ, but could be a requirement or condition of the RFP and resulting contract. 2) It is reasonable to assume that the final solution will need to be a combination of vendor supplied tools and systems that are integrated into existing DND/CAF tools and systems.
42	Organizational change considerations: Implementation of CD-DAR will require significant organizational change management across the CDS. In section 2.5.2 of the CONOPS, DND/CAF has already defined a comprehensive list of well-defined roles and responsibilities that are required to address the existing cyber activities they are responsible for. Transition from the current multitude of disparate systems that require manual use to a more efficient and consolidated	At this stage of the project DND is not able to share its change management plan for CD-DAR.

	solution under CD-DAR will require an update of existing (and possible introduction of new) roles and responsibilities as well as update of existing (introduction of new) processes/procedures. Additionally, as the cyber threat landscape evolves, CD-DAR will need the flexibility to adapt to the exigent threats across a large and complex organization landscape of the CDS. Hence, there will need to be significant preparations to train of personnel, develop of new process/procedures, and likely introduction of new roles with new responsibilities. Is DND/CAF willing and able to share how it is planning to address and ultimately implement the change management process as this knowledge will influence the partners we select as part of our response? (e.g. partners that are best equipped to assist with the organizational change management that will be necessarily planned in conjunction with the technical implementation)	
43	ITQ reference - 3.6 Changes to the Respondent Core Team Could the Crown please confirm that as noted in subsection 3.6.1 and 3.6.2 of the ITQ, Respondents must maintain the Respondent Core Team throughout this procurement process and are not permitted to add or remove Respondent Core Team Members after pre-qualifying under this ITQ?	As detailed in Amendment 006-5 and as per sections 3.6.1 and 3.6.2 of the ITQ no changes the members of a Respondent Core Team will be permitted throughout the entire procurement process up to and including Contract Award and Implementation unless approved in writing by the contracting authority. Changes to the core team members may, at the discretion of Canada, result in the Respondent becoming ineligible to continue in the CD-DAR procurement process.
44	Reference - Annex A: Mandatory Evaluation Criteria, pages 26-37 While we appreciate that the Crown would like to conduct reference checks to verify Respondents' compliance with the ITQ evaluation criteria, due to the confidential and classified nature of the projects that meet this criteria, defense and/or other government clients do not consent to their contact information being shared at this stage of the procurement process. In most cases, approval is required at a high level of the defense organization to include the reference organization or name – a common practice for national defense organizations. As such, this requirement for client reference information will significantly restrict, if not eliminate, the number of FVEY projects that Respondents can put forward, and consequently, will artificially reduce the pool of well qualified and experienced organizations who will be able to qualify under this process. We do not believe that this is the Crown's intention as it would negatively impact DND/CAF's ability to achieve its objectives under this important and critical procurement.	As detailed in Amendments 006-1 and 006-9 to this solicitation for all projects Canada will accept client contact information after the closing date of the invitation to qualify up to the release of the final RFP. Respondents however will not be considered pre-qualified until the client contact information is provided and the referenced project experience has been confirmed by Canada. Suppliers that are not pre-qualified will not be able to participate in any activities open to pre-qualified suppliers including receipt of the final RFP.

	Therefore, can Canada confirm that if client reference contact information is not provided within a Respondent's ITQ response, the Respondent will have 5 working weeks to gain approvals required to provide these contact details at the contract award / negotiation stage of the formal RFP? This option will be beneficial to the Crown and would provide it with the assurance it needs before any contract would be signed.	
45	We are working on the CD_DAR ITQ response. We saw the recent amendment changing the closing date to 12/1/2021. Can you please confirm that the ITQ response to Mandatory Requirements is also now delayed until 12/1/2021?	Only the closing date for the RFI was amended to December 1, 2021. The RFI W6369-20-CY06/B is posted under https://buyandsell.gc.ca/procurement-data/tender-notice/PW-QE-049-27832 As detailed on the main posting page of that RFI, the RFI although open, is not currently active. The Invitation to Qualify (ITQ) can be found on buyandsell under the Notice of Proposed Procurement (NPP): W6369-20-CY06/C at https://buyandsell.gc.ca/procurement-data/tender-notice/PW-QE-049-28197 All suppliers interested in becoming a qualified supplier to CD-DAR must submit a response to that ITQ.
46	We are interested in initiating the process for obtaining a corporate security clearance in order to be eligible to bid on the future RFP. Please advise us of the required steps in order to obtain a required security clearances.	Canada will only assist suppliers that have qualified under the ITQ in obtaining the required security clearances for the next phases of the procurement. Interested respondents are reminded to review the security requirements in section 1.2 Security Requirements for Phase 3 – Due Diligence, Phase 4 – RFP and section 1.3 Security Requirements for Phase 5 - Contract. These Security Requirements include limiting, to varying degrees, the Draft RFP/RFP and Contract to citizens of Canada, United States, United Kingdom, Australia, or New Zealand. Information on the Organization Security Screening Process can be found at: https://www.tpsgc-pwgsc.gc.ca/esc-src/organisation-organization/index-eng.html
Questions and Answers in Amendment 007		
No.	**Question**	**Answer**
47	Incremental and Experimental Approach: CD-DAR's approach as described is thorough and comprehensive. However, the results and value from deployment of the project's capabilities will not be tangible for ~ 3-4 years. A single year is a lifetime in the cyber realm. CD-DAR capabilities, as scoped and discussed in this traditional procurement process, may no longer be relevant at the time of	1. CD-DAR plans to take an agile approach to system design and implementation. 2. CD-DAR plans to implement a phased and incremental approach to modernizing the defensive cyber capabilities of DND/CAF.

	implementation. During this entire period, DND/CAF will also have not have experienced any real-time benefits. 1. Has DND/CAF considered a more agile implementation approach to system design and implementation that includes experimental implementation to continue to inform the ongoing process over this period of time? 2. Has DND/CAF considered a more phased / incremental approach to modernizing the defensive cyber posture to begin to address current challenges faced by the cyber organization today? (e.g. running pilots to gain capability and test ability to evolve)	
48	In Annex A, Section 3, Table 1 - Mandatory Technical Evaluation Criteria several of the mandatory criteria for successful implementation state that Cyber Security and Cyber Decision Analysis and Response integrated solutions must be deployed on "IM/IT Networks of 8,000 or more Endpoints". Under Table 2 – Point Rated Technical Evaluation Criteria - points are awarded based on the number of Endpoints that are under the required 8,000 Endpoints as defined in Table 1. Is it Canada's position that respondents will be awarded points from 2,001 up to 8,000 endpoints?"	Points will be allocated in accordance with the scoring criteria detailed in Table 2 of Annex A. For the mandatory criteria, a minimum of 8000 endpoints is required.
49	Person year – clarification (ITQ reference - Annex A, 1.3 Projects, 1.3.4 (h), pg 27 of amendment 001) As person years are defined and calculated in a variety of ways, could the Crown please provide its definition to ensure that Respondents are providing consistent responses?	A Person-Year is the total number of personnel resources that worked on a project full time over the course of one year. If a team of 5 people worked full time for a year, then the number of person years would be 5 person/year.
50	ITQ reference – R1, pg 35 of amendment 001 Could the Crown please define "re-synchronization" in R1?	Re-synchronization is defined as the ability of a system within a domain to take automatic action to come back immediately to a security state in-line with the rest of the network when the domain, given its approved security configuration (as defined by the organization's baseline) and system readiness, goes out of synchronization due to Disconnected, Intermittent, and Limited (DIL) bandwidth environments. Re-synchronization will also include storing all intermediate cyber security data and logs that were generated locally and transmitting in near-real time to the base network as connectivity/bandwidth becomes available. Re-synchronization must take place in such a way that the network and host security status is preserved, vulnerability is minimized, and the organization is protected from external and internal threats all at the same level before losing connectivity.

51	ITQ reference - Table 3 – Definitions, "successfully implemented", pg 41 of amendment 001 Could the Crown please describe what the proof of acceptance comprises (of considering that clients are already acting as and being provided as references)?	Proof of acceptance would be a signed document from the client to formally acknowledge that the referenced project was completed, all requirements were met and that stabilization support was provided. As stated in the definition, a Letter of Support from the (Federal) client would be acceptable. Client references will be contacted to confirm and verify information provided by the bidder regarding the referenced project.
52	Ref; 1.3 Projects 1.3.1 Where the Respondent must include a description of projects: (i) a project must have been completed by the Respondent itself and cannot include the experience of any proposed subcontractor or any affiliate of the Respondent that are not part of the Respondent Core Team. (ii) a project must have been successfully implemented within the last seven (7) years of the ITQ closing date. (iii) more than one (1) reference project may be used to meet all the evaluation criteria, however, not more than one (1) reference project can be used to meet an individual evaluation criteria. Does this mean, for example, that a supplier cannot use project A (with 2000 endpoints) and project B with 6000 endpoints to equal the mandatory criteria of 8000 end points? Or should this be interpreted that Canada will only evaluate the first project reference used, regardless if other project references are also listed for that same mandatory criteria? The latter is often used on PSPC professional services contracts so does the same apply here?	The supplier cannot combine more than one project in order to meet the minimum number of endpoints. As per Section 1.3 Projects, 1.3.1 (iii) more than one (1) reference project may be used to meet all the evaluation criteria, however, not more than one (1) reference project can be used to meet an individual evaluation criteria. As well, Section 1.3 Projects, 1.3.3 states: Respondents should only provide the required reference project(s) as indicated in each mandatory and point rated requirement. If more than the required number of reference project(s) is provided, the Respondents will be required to clarify which reference project(s) apply to corresponding mandatory or point rated requirement(s).
Questions and Answers in Amendment 008		
No.	**Question**	**Answer**
53	Will priority be given to Canadian bidders and teams?	The ITQ is open to all suppliers able to meet the evaluation criteria.
54	Amendment 005 Q&A 10 appears to create a conflict in the definition of “Association of Entities” and "Core Team Member". Section 2.2.1 clearly states that “Association of Entities” are related entities and mutually exclusive from unrelated affiliates. Further, “Association of Entities” clarifies that it "does not include unrelated affiliates of the Respondent with whom the Respondent is partnering through a Respondent Core Team or Joint Venture (as applicable)”. Section 2.2.1 does not require “Association of Entities” to be named as Core Team members or in a Joint Venture. Please confirm that Section 2.2.1 stands as originally released to industry.	The term "Association of Entity" was included in the ITQ in error and it is not employed in the ITQ aside from appearing as a definition in Section 2.2.1. To avoid confusion, the ITQ has been amended to remove this term. As stated in section 3.3.3 of the ITQ and subsection 1.3.1 (i) of Annex A, a Prime Respondent who is including project experience from another entity must also list that other entity as a Core Team member in their response.

	Our interpretation of Association of Entities was that any Company X reference globally would count under Prime respondent and that if we used a reference from any other loosely aligned affiliate that we would be required to add them as a Core Team Member.	
55	We understand that No Controlled Goods certification is required prior to filing the ITQ. I understand that we must have it before receipt of the RFP. By what date is it estimated that we will have to provide controlled goods certifications in order to receive the RFP?	We are not able to provide a date for the RFP release at this time however general timelines for the procurement process can be found in Section 1.3 - Overview of the Planned Procurement Process, of the ITQ.
56	Respondent Core Team - follow-up to Q43, amendment 006 We understand that the removal of a core team member that a Respondent has used to qualify under this procurement would not be ideal or beneficial to the Crown. However, as Respondents learn more about the CD-DAR project through the one-on-one meetings and due diligence process, Respondents may uncover a need to enhance their team with the addition of a new core team member to ensure that DND/CAF will receive greatest value and best expertise. Please confirm that Respondents can add core team members after qualifying under the ITQ.	As detailed in the response to Q43 in Amendment 006 for all qualified Respondents any request to change the member(s) of a Respondent Core Team, including a request to add core team members, will be reviewed by Canada at the time of the request to determine if the requested change is acceptable under the terms of the ITQ and the Request for Proposal.
57	Association of entities - follow-up to Q10, amendment 005 While we appreciate the Crown has included a definition of Association of Entities in the RFP, the linkage between the Association of Entities and the Respondent appears to be missing. Would the Crown consider clarifying: 1. That the Respondent includes Respondent affiliates, and 2. That the affiliates of Respondents include the members of the Association of Entities.	The definition of Respondent in section 2.2 of the ITQ does not include affiliates of Respondents and Canada will not amend this definition. The ITQ has been amended to delete "Association of Entities" from section 2.2.
58	For security reasons, we request that the Respondent can be identified as the first point of contact in Form 2 to liaise with the customer for establishing contact between Canada and client, for the purpose of criteria compliance verification.	The Respondent may be identified as the first point of contact in Form 2. Please be reminded, as detailed in Amendment 006 to this solicitation and in response to question 44, although Canada will accept client contact information after the closing date of the invitation to qualify and up to the release of the final RFP, Respondents will not be considered pre-qualified until the client contact information is provided and the referenced project experience has been confirmed by Canada. Suppliers that are not pre-qualified will not be able to participate in any activities open to pre-qualified suppliers including receipt of the final RFP.

Questions and Answers in Amendment 009		
No.	**Question**	**Answer**
59	Regarding criterion R3 (c) (ITQ reference – R3, pg 36 of amendment 001) Could the Crown please clarify if Respondents are expected to provide one (1) reference project that meets all of the elements (a), (b), and (c) in R3? If so, we strongly recommend that the Crown remove (c) from R3 as it would require a Respondent to have one (1) reference project that not only meets R3, but also meets mandatory evaluation criteria #1 to #6. This is overly restrictive at the ITQ stage of this procurement, as Respondents who meet M1-M6 and R3 (a) and (b) would ultimately score 0/20 points based on the current structure of R3.	R3 is amended as follows: The Respondent has Successfully Implemented one (1) Complex IM/IT Project in the last seven (7) years, which included the design, development, integration, implementation, and delivery of Cyber Security and Cyber Decision Analysis and Response COTS/GOTS/MOTS integrated solutions and re-synchronization within FVEY nations and provision of at least 12 months of Stabilization Support for all of the following in a given network: (a) within a globally distributed network components on two (2) or more continents with a minimum of ten (10) separate operating nodes, (b) interconnected at disadvantaged speed (less than 1.544 Mbps links) remoted in austere environments to a High speed (100Mbps or above) central network, and (c) for Cyber Security related data or information a network of: i) 2001 to 4000 endpoints; ii) 4001 to 6000 endpoints; iii) 6001 to 8000 endpoints; and iv) More than 8000 endpoints For R3 (c), the Respondent project must include a minimum of 5 of 9 of the examples listed below of Cyber security related data and information. 1. The identification and tracking of authorized and non-authorized IM/IT assets; 2. Information related to each of the assessment of vulnerabilities, configuration, risk and patch compliance; 3. The analysis of cyber threat information; 4. Detection and assessment logs for suspicious activity; 5. The execution of prevention and response to threats and remediation actions in near real time; 6. Data feeds of cyber threat and analysis information from multiple sources; 7. Threat intelligence information; 8. Integrated Cyber Security incident, data analysis and security alerts; 9. The processing of structured and unstructured data related to cyber security.