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
Place du Portage, Phase III
Core 0B2 / Noyau 0B2
11 Laurier St.\11, rue Laurier
Gatineau
K1A 0S5
Bid Fax: (819) 997-9776

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
THERE IS A SECURITY REQUIREMENT ASSOCIATED WITH THIS SOLICITATION

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

Issuing Office - Bureau de distribution
Business Transformation and Systems Integration Service/Division de transformation des opérations et d'intégrat
Special Procurement Initiative Dir
Dir. des initiatives speciales d'approvisionnement
11 Laurier, Place du Portage III
12C1
Gatineau
Québec
KIA 0S5

Title - Sujet ISS Transformation - RFP	
Solicitation No. - N° de l'invitation EP243-170549/B	**Amendment No. - N° modif.** 009
Client Reference No. - N° de référence du client 20170549	**Date** 2017-08-16
GETS Reference No. - N° de référence de SEAG PW-$$XE-678-31237	
File No. - N° de dossier 678xe.EP243-170549	**CCC No./N° CCC - FMS No./N° VME**
Solicitation Closes - L'invitation prend fin **at - à 02:00 PM** **on - le 2017-08-25**	**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: Oates, Christine	**Buyer Id - Id de l'acheteur** 678xe
Telephone No. - N° de téléphone (873) 469-3917 ( )	**FAX No. - N° de FAX** ( ) -
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 Number 009
Purpose:

A. To identify changes to the (Request for Proposal) RFP.
B. To provide answers to questions received with regards to this RFP.

A. CHANGES

Change 87:

At ANNEX A, SECTION 3: TECHNICAL REQUIREMENTS, under 1.2 Technical Requirements:

DELETE:

Tech. 34	Develop Logical and Physical architecture blueprints, under the guidance of GC using the GC templates, and construct the Solution based on the Conceptual architecture.

INSERT:

Tech. 34	Develop ISST Logical and Physical architecture blueprints (using GC templates) based on the ISST Conceptual architecture blueprint. These blueprints are subject to GC approval.

Change 88:

At Attachment 1 to Part 4 – Technical Evaluation, 4. Point Rated Criteria, R1, under the heading Point Rated Criteria, **DELETE** the second paragraph in its entirety and **REPLACE** with the following:

> Canada will evaluate the Bidder's Preliminary Project Management Plan based on the degree to which it responds to the following requested elements and how they support the intended outcomes listed in ANNEX A, Section 1 and 7:

Change 89:

At Attachment 1 to Part 4 – Technical Evaluation, 4. Point Rated Criteria, R4, under the heading Maximum Available Points:

DELETE:

> **Maximum Points : 360**
>
> Part A Maximum Points : 120
>
> Part B Maximum Points : 80
>
> Part C Maximum Points: 80
>
> Part D Maximum Points : 80

INSERT:

Maximum Points : 360

Part A Maximum Points : 90

SC.47 a) Three sub parts, 10 pts each
SC.47 b) Fifteen sub parts, 4 pts each

Part B Maximum Points : 120

SC.16 Three sub parts, 40 pts each

Part C Maximum Points: 75

SC.9 a) One part, 75 pts

Part D Maximum Points : 75

SC.42 a) One part, 26 pts
SC.42 b) One part, 25 pts
SC.42 c) Four sub parts, 6 pts each

Change 90:

At Attachment 1 to Part 4 – Technical Evaluation, 4. Point Rated Criteria, R9, under the heading Point Rated Criteria, **DELETE** the second paragraph in its entirety and **REPLACE** with the following:

For the purposes of the evaluation, Case Management is defined as the management of activities including but not limited to: the initiation, coordination, research, maintenance and completion of a service request action from a client, until its resolution. COTS Web Portal is defined as a commercially available (Off the Shelf) software package that provides a public-facing vertical internet-based information exchange component (on-premises) of the Solution that integrates with the Case Management platform (on-premises) and serves as the central, self-service interface enabling communication and interaction.

B. QUESTIONS

Question 143:

In reference to Attachment 1 to Part 4 – Technical Evaluation, 3. Point Rated Criteria, R4 Security Management (page 8 of 10), the requirement states:

"The document should highlight the requirements for security, as indicated in the Security Requirements section of ANNEX A, Section 4. Canada will evaluate the degree to which the Bidder's approach to Security management reflects the required security controls. In particular, the approach should:

A. Contain a high level, end to end description of security operations;"

The bidder is not responsible for operational security management of the solution and the RFP does not provide any detail on Canada's IT environments, such as how they are secured, monitored, or how Canada handles security incidents internally.

Will Canada consider amending this requirement to make it consistent with the role of the bidder (e.g. the bidder has no role in security operations of the solution, or the IT environment in which it is hosted)?

Answer 143:

The Contractor is responsible for assisting the GC in the implementation of security requirements found within the SOW. For the purpose of evaluating the Bidder's experience with security implementation, GC is requesting the Bidder to provide operational scenarios with applied security controls as indicated in the Security Requirements section of ANNEX A, Section 4. It should be noted that Technical Evaluation R4 has been clarified in Amendment 004, Question 73. Evaluation Item A referenced in the question has been removed.

Question 144:

In reference to Attachment 1 to Part 4 – Technical Evaluation, 3. Point Rated Criteria, R4 Security Management (page 8 of 10), the requirement states:

"Reference and address all parts of SC-01 Access Control and Account Management".

The bidder will not be creating and managing accounts or access.

Will Canada consider amending this requirement to have the bidder describe the technical capabilities of the solution and how it would be configured to interface with users and operators consistent with GC standards?

Answer 144:

In reference to the creation and management of accounts or access, GC confirms that the Contractor must meet the requirements as indicated in SC.01 of the SOW.

In terms of responsibility, the Contractor must configure the Solution to create and manage account(s) and access. This includes the creation of the first account and the validation of permissions and access. All subsequent accounts will be created and maintained by the GC.

R4 has been clarified and changes to the referenced Security Controls have been included. Bidders should review the revised R4 posted in Amendment 004, Question 50.

Question 145:

In reference to Attachment 1 to Part 4 – Technical Evaluation, 3. Point Rated Criteria, R4 Security Management (page 8 of 10), the requirement states:

"Reference and address all parts of SC-07 Identification and Authentication within the Security Operations document".

The bidder will not be responsible for GC credentials/authentication systems.

Will Canada consider to amend this requirement to have the bidder describe how the solution will leverage credentials and identities issued and managed by the GC as the operational authority consistent with GC standards?

Answer 145:

In reference to identification and authentication, GC confirms that the Solution must meet the requirements as indicated in SC.07 of the SOW. The Contractor must ensure that the Solution can successfully and uniquely identify and authenticate users and that authentication mechanisms meet noted

standards. R4 has been clarified and changes to the referenced Security Controls have been included. Bidders should review the revised R4 posted in Amendment 004, Question 50.

Question 146:

In reference to Annex A – Statement of Work, Section 5: IT Security Requirements, 1.2 Detailed Requirements, SC.32 (page 46 of 70). The Contractor must assist the GC and aid in the response to all suspected or actual incidents related to the Solution for the duration of the contract.

This is an unbound financial risk as it is impossible to estimate the number of incidents that this would be required and include it in a bid quotation. It depends entirely on the security posture of the overall IT environment, the granularity of SSC security detections and the changing threat environment. Will Canada consider amending this requirement to have this assistance be subject to separate invoicing as a post-deployment professional service, or assign a maximum number of instances (and days of effort for each) so that it can be estimated and priced accordingly?

Answer 146:

In reference to SC.32, the expectation of work is to provide services in a post "go-live" environment as the development environment will not be connected to the internet. During this time, the Contractor will be responsible for incidents that are the result of an error or oversight in work executed by the Contractor. Additionally, the Contractor must adhere to item 05 of the General Conditions 2035, which reads "All services rendered under the Contract must, at the time of acceptance, be free from defects in workmanship and conform to the requirements of the Contract. If the Contractor is required to correct or replace the Work or any part of the Work, it will be at no cost to Canada.

Should work beyond the areas of responsibility stated above be required of the Contractor by the GC, the GC will exercise the Optional Services through a Task Authorization.

Question 147:

In reference to Annex A – Statement of Work, Section 5: IT Security Requirements, 1.2 Detailed Requirements, SC.34 (page 47 of 70). The Contractor must provide support and assistance to the GC in implementing mitigation measures (e.g., firewall blocks, customized Intrusion Detection Prevention signatures, and removing malicious malwares) to contain a Security Incident and to protect against cyber threats or address vulnerabilities, when requested by PWGSC authorized representatives, as specified by PWGSC in accordance with Canada's priority level for the duration of the contract.

This is an unbound financial risk as it is impossible to estimate the number of incidents that this would be required and include it in a bid quotation. It depends entirely on the security posture of the overall IT environment, the granularity of SSC security detections and the changing threat environment. Will Canada consider amending this requirement to have this assistance be subject to separate invoicing as a post-deployment professional service, or assign a maximum number of instances (and days of effort for each) so that it can be estimated and costed accordingly?

Answer 147:

Anticipated security risks requiring mitigation measures that are assessed during the design and development of the solution are the responsibility of the Contractor. The Contractor must deliver the logical and physical architecture as per Tech.34, for which they must include, in the system's design, mitigation measures for these anticipated incidents. For post go-live incident mitigation, please refer to Question 146 in this Amendment 009.

Question 148:

In reference to Annex A – Statement of Work, Section 5: IT Security Requirements, 1.2 Detailed Requirements, SC.36 (page 47 of 70). The Contractor must provide support and assistance to the GC in the development of a Security Incident post-mortem report when required by PWGSC for the duration of the contract.

This is an unbound financial risk as it is impossible to estimate the number of incidents that this would be required and include it in a bid quotation. It depends entirely on the security posture of the overall IT environment, the granularity of SSC security detections and the changing threat environment. Will Canada consider amending this requirement to have this assistance be subject to separate invoicing as a post-deployment professional service, or assign a maximum number of instances (and days of effort for each) so that it can be estimated and costed accordingly?

Answer 148:

Please refer to the response to Question 146 in this Amendment 009.

Question 149:

In reference to Annex A – Statement of Work, Section 5: IT Security Requirements, 1.2 Detailed Requirements, SC.40 (page 47 of 70). The Contractor must for the duration of the contract implement patches and corrective measures as part of vulnerability assessment activity. The Contractor must create Service Request Tickets for any required patch or corrective measure that cannot be implemented as part of the vulnerability assessment activity.

Unless it is Canada's intent to provide a system maintenance service contract to the bidder for the duration of the contract, this is normally the responsibility of the IT operating authority, with solution-specific 2nd/3rd line support from the bidder, as required.

Will Canada please clarify the requirement?

Answer 149:

The Contractor must, based on the results of the vulnerability assessment which is completed by the GC, implement patches and corrective measures within the scoped solution for the duration of the contract. In the event that the Contractor is unable to perform implementation due to factors such as restricted access, they will utilize the PWGSC IT Change Management process to have patches implemented and corrective measures actioned by GC through Service Request Tickets. All changes must be thoroughly documented.

Question 150:

Question 36 is about the scope of the security controls requested by the Crown and what should be in the solution or not. In its response, the Crown refers to the answer to question 35. The answer to Question 35 states that "Note that not all ITSG-33 controls are to be implemented by the Contractor. Many of the technologies to be integrated are implemented and have security controls in place. As well, security controls / requirements pertinent to the infrastructure will be implemented by Shared Services Canada. The SOW only contains those requirements which require effort on the part of the Contractor."

Based on the above answer, requirement SC.38 states The Contractor must for the duration of the contract assist and support the GC in ensuring that the security posture of the Solution is maintained by continuously identifying and notifying the GC of:

(a) Threats and vulnerabilities; and

(b) Malicious activities and unauthorized access "is the responsibility of the contractor to implement as part of the solution."

SC.38 is surely an SSC responsibility of monitoring threats and vulnerabilities, and malicious activities and unauthorized access based on the means implemented in the Solution, i.e. as an example SC.04 "Generate audit records of security events in a format suitable for submission to a Security Information and Event Management (SIEM) system;". One would assume that such SIEM would be managed by SSC.

Will the Crown provide a clear responsibility matrix of security controls in the RFP for the Contractor and SSC in order to:

- Remove overlap of Solution capabilities and associated costs to the Crown;
- Provide a clear scope of Contractor solution and security services; and
- Clearly leverage existing SSC responsibilities and capabilities

Answer 150:

An update on the Solution's sensitivity profile and subsequent additions of security controls was made in Amendment 003 and further expanded upon in Amendment 008. As observed, there are many security controls to be considered, those that support the PB/M/M sensitive components and those additional controls that address the recently added concerns for PB/H/M sensitivities. Controls that are the responsibility of the contractor to be implemented within the solution are represented as technical requirements within the SOW. The Contractor is required to meet all the technical requirements, meaning those controls which the technical requirements represent.

Additionally, the Contractor will present an overarching physical architecture where the high level inclusion of all controls is identified. The Contractor is not expected to provide those controls that are outside of the scoped Contractor work, but must consider the impact of those controls when configuring and constructing the scoped solution.

The Contractor may be asked to assist the GC with the implementation of controls outside the scope of work where the implementation requires multiple teams' involvement. This work would be conducted under a Task Authorization.

Question 151:

In reference to Annex A – Statement of Work, Section 5: IT Security Requirements, 1.2 Detailed Requirements, SC.50 (page 49 of 70). The Contractor must for the duration of the contract provide support and assistance to GC in conducting the security installation verification in accordance with the approved Security Installation Verification Plan.

It is difficult to estimate cost as written.

Does this only apply to bidder-supplied software updates? If not, can Canada please provide the types of activities they would want included on an ongoing basis and the number of instances/year (or days of effort)?

Answer 151:

For the duration of the Contract, the Contractor is expected to provide support and assistance to the GC, as per SC.50, in conducting the security installation verification for the Contractor provided or prepared or

configured Solution components only. The Contractor must provide support for the subsequent security installation verifications, expected to be performed after every installation during implementation. The Security installation verification may be required to be repeated when platform upgrades may negatively affect the contractor provided solution security controls.

Question 152:

In reference to Annex A – Statement of Work, Section 5: IT Security Requirements, 1.2 Detailed Requirements, SC.51 (page 49 of 70). The Contractor must correct installation and configuration errors and omissions that are detected as a result of the security installation verification.

As per SC.50. It is difficult to estimate cost as written.

Does this only apply to bidder-supplied software updates? If not, can Canada please provide the types of activities they would want included on an ongoing basis and the number of instances/year (or days of effort)?

Answer 152:

The security installation verification must be completed by the GC, with support from the Contractor, before the date for go-live, which includes but is not limited to any installation or configuration errors or omissions remediation as it relates to the Contractor's work. Please refer to the response to Question 146 of this Amendment 009, for installation and configuration errors or omissions post go-live.

Question 153:

In reference to Annex A – Statement of Work, Section 5: IT Security Requirements, 1.2 Detailed Requirements, SC.41 (page 47 of 70). The Solution, at a minimum, must comply with the requirements of the PB/M/M profile in ITSG-33, ANNEX 4A (https://www.csecst.gc.ca/en/system/files/pdf_documents/itsg33-ann4a-1-eng_4.pdf).

The Prot B MM default profile in ITSG-33 is not intended solely for application-level solution deliveries by a contractor. It contains approx. 430 controls that are in addition to those specified in the RFP, many of which are well beyond the bidder's apparent scope. It will also exponentially expand the scope of the SA&A.

Uncertainty in this area will cause confusion during the SA&A and will introduce risk to bidders, which will ultimately have to be covered by cost in the bid estimates.

Will Canada please indicate which of the controls in this profile are the contractual responsibility of the Bidder, which are the responsibility of Canada, and which (if any) are not applicable?

Answer 153:

Please refer to the response to Question 150 in this Amendment 009.

Question 154:

Appendix 2 to Annex A – Key Activities – the schedule listed indicates that both the "Planning and Analysis" and "Solution Design" are both to be completed by the end of December 2017. Our approach proposes that the "Planning and Analysis" recommendations are to be reviewed and approved by the ISST Project

Authority prior to completing the “Solution Design” activities, and that the Solution Design is also approved by ISST prior to deliverables being considered complete.

As such, both being complete by the end of December 2017 may not be feasible.

Can these “Planning and Analysis” and “Solution Design” milestone dates be left as flexible, as long as our overall plan targets the “Solution Development and Configuration” milestone to be achieved in 2018 August?

Answer 154:

The Milestone Schedule as provided in APPENDIX 2 to ANNEX A was presented to outline the project timeline and when milestones are expected. In preparation of a bid, the Bidder may propose new milestone timelines for the Milestone Schedule as long as listed key activities are presented and are completed while retaining the existing Solution Pilot, Phased Rollout and Solution Stabilization and Transition Out milestones.

Question 155:

Change 55 has replaced R4 with an entirely different rated requirement. Can PWGSC please clarify how many points the new R4 will be evaluated at and how points will be determined?

Answer 155:

Technical Evaluation R4 has been amended to provide the requested point schedule. Please see Change 89 in this Amendment.

Question 156:

The financial evaluation table (sample) seems to have an error in it. The denominator in the formulas for bidder 1 and 2 seem to be flipped.

Answer 156:

Canada confirms that the formulae in the Example of Bid Selection table at item 4.4.1.9 of Part 4 of the RFP are correct.

Question 157:

Regarding Amendment 004 Change 55 which replaces the original description for R4, we have several concerns.

a) Regardless of the operational scenarios chosen, the applicability to the end state Dynamics CRM and Portal solution will be very assumptive until the reality of the scenarios can be confirmed with CISD and other stakeholders throughout the business process re-engineering portions of the solution delivery. Bidders are already being evaluated on business process re-engineering in other sections of the evaluation.

b) Secondly, there are a wide range of operational scenarios that can be chosen of varying levels of complexity. This brings the possibility of significant variability and subjectivity to the R4 assessment, making it difficult for a common, fair “apples to apples” assessment amongst the various bidders.

Given this, a bidder’s ability to demonstrate the application of the security requirements for ISST and the Government of Canada ITSG-33 Security Assessment and Authorization (SA&A) process would be more indicative by replacing R4 with a requirement to provide a Security Concept, which includes the following:

a) A description of the bidder's approach to security for the ISST solution from contract award to go-live, as well as for the bidder's sustainment of the ISST solution through its lifecycle.

b) A proposed ITSG-33/38 compliant security topology diagram with accompanying explanatory notes, which assumes that the ISST will be hosted in a compliant GC host environment, and which highlights suitable proposed solution security safeguards, including:

- Zoning;
- Encryption;
- Intrusion Detection;
- Monitoring;
- Access control;
- Data segregation; and
- Data flow control.

c) A narrative description which demonstrates the bidder's understanding of the ITSG-33 SA&A process and how they would approach key activities for each SA&A gate to ensure success.

We are requesting that the Crown revise R4 as per the above description to address the identified concerns with R4. However, if the Crown takes the decision to continue with the revised amendment 004 R4 scenarios approach, it is requested that the Crown identify the operational scenarios by providing a description of 3 scenarios from which bidders are required to select any 2 scenarios. This would ensure that bidders would be submitting scenarios of equivalent complexity, that could be evaluated on a common" apples to apples" basis.

Answer 157:

The original R4 differs little from the revised version. Examples of Operational Scenarios have now been provided, and references to specific security controls were changed to better reflect a wider scope of necessary controls.

With respect to Technical Evaluation R4, the Bidder will not be evaluated on business process re-engineering aspects that do not relate to security management or other non-security aspects of their response. The purpose of R4 is to evaluate the Bidders ability to understand and implement the necessary security requirements. Irrespective of the complexity of the scenarios the Bidder chooses, the Bidder must provide appropriate detailed responses to be awarded full points.

Question 158:

We are requesting the revised evaluation grid for R4, including the overall score and the distribution of points for each sub element of the grid be provided to bidders.

Answer 158:

Please see response to Question 155 in this Amendment 009.

Question 159:

Attachment 1to Part 4, M2, Item E; Amendment 003, Changes 40, 41& 42; Amendment 004, Answer 38 – Item E of M2 requires one of the reference projects to have the same security requirements as identified in Annex A, Section 5, 1.2 which essentially requires that the project adhere to ITSG-33 or NIST. Amendment 003, Changes 40, 41 & 42 raised the integrity requirements from Medium Integrity to High Integrity, thus imposing further restrictions on the reference project.

Canada has acknowledged (Amd 004, A38) there may be a limited number of government projects that would satisfy M2; yet the security requirements almost certainly require a government project in order to meet the security requirements of Annex A, Section 5, 1.2.

By their nature, security controls must work in the same way regardless of volumetrics, diversity of transactions, etc., as such the requirement that a project needs to not only meet the security requirements, but also other elements listed in M2 is highly restrictive.

It is requested that requirement be changed to allow the Bidder to demonstrate experience on a project (not required to be one of the 3 in support of M2) where they have implemented security controls similar to those in Annex A, Section 5, 1.2 – with MEDIUM integrity – to comply with Item E of M2.

Answer 159:

M2, Item E of the Technical Evaluation has been removed. Please see Change 81 in Amendment 008.

Question 160:

Amendment 3 (changes 21 and 44) amended the SRCL to indicate that this procurement is restricted to Canada, including permanent residents, as the supplier will be required to access INFOSEC information or assets. Part 7, item 7.4 of the RFP now includes a requirement for a Foreign Ownership, Control and Influence assessment. In the interests of complying with this mandatory requirement, would Canada please provide the FOCI questionnaire to ensure that all Bidders complete the forms within the timeframes allocated.

Answer 160:

For reference, the FOCI questionnaire is provided as an attachment to this Amendment 009. Please note that the FOCI questionnaire and related documentation must only be submitted after contract award.

Question 161:

In Amendment 7, Answer to question 106:

The Crown confirms that "***both a Preliminary Project Management Plan and Project Management Plan*** are required. Criteria A through F should be included as components of the Project Management Plan and are not separate requirements." Would the Crown please confirm that only the Preliminary Project Management Plan is due at Bid close, and that the Preliminary Project Management Plan is to cover all of the requirements A-F in R1? In addition, would the Crown please confirm that a Project Management Plan will be developed within the Planning and Analysis phase of the project?

Answer 161:

The Crown confirms that the Preliminary Project Management Plan is to be developed for the purpose of the bid evaluation and to feed the contractor's actual Project Management Plan, which is to be developed after contract award during the Planning and Analysis phase. The Crown also confirms that the Preliminary Project Management Plan should contain each component listed in R1 of the Technical Evaluation.

Question 162:

Amendment 6, Change 60 states:

"COTS Web Portal is defined as a commercially available (Off the Shelf) software package that provides a public-facing vertical internet-based information exchange component (on-premises) of the Solution that

integrates with the Case Management platform (on-premises) and serves as the central, self-service interface enabling communication and interaction between External Users and the two Industrial Security Sector programs: Contracts Security Program and Controlled Goods Program."

As the requirement above refers in general to project references that bidders must provide, it is unreasonable to restrict them to solutions that support the PSPC ISS programs as it is currently stated. Would the Crown please remove the following wording from the above paragraph: "between External Users and the two Industrial Security Sector programs: Contracts Security Program and Controlled Goods Program"?

Answer 162:

Canada agrees and will remove the requested wording from the paragraph. Please refer to Change 90 in this Amendment 009.

Question 163:

In follow up to Amendment 007, Answer 106 in response to Question 106: it states "The Crown confirmed that both a Preliminary Project Management Plan and Project Management Plan are required…"

Doesn't the **preliminary** project management plan need to be completed in the NPMS Project Identification Stage prior to releasing the RFP to select an SI to begin the Project Delivery Stage i.e. the preliminary project plan (PPP) should already exist as an artifact?

We recommend the requirement for both a Preliminary Project Management Plan and Project Management Plan be replaced in R1 with "The Bidder should provide its proposed Project Management Plan…"

Answer 163:

Please note that Canada is not referring to the NPMS Preliminary Project Plan in this requirement. Canada indicates the Project Management Plan bidders are proposing in this evaluation is a Preliminary Project Management Plan as bidders cannot complete an actual Project Management Plan until after the contract is awarded. The Preliminary Project Management Plan is only to be used for the bid evaluation. The Project Management Plan will be the actual project deliverable under the Contract. Please refer to Change 88 in this Amendment 009.

ALL OTHER TERMS AND CONDITIONS REMAIN THE SAME

Gouvernement du Canada | Government of Canada

Canada

Respect ◆ Integrity ◆ Excellence ◆ Leadership

Serving GOVERNMENT, Serving CANADIANS.

Foreign Ownership, Control or Influence

Guidelines for Organizations

Revised April 10, 2014

Table of Contents

PART A - PURPOSE OF A FOREIGN OWNERSHIP, CONTROL OR INFLUENCE (FOCI) EVALUATION

Foreign Ownership Control or Influence (FOCI) refers to a situation where a foreign third party individual, firm or government is assumed to possess dominance or authority over a Canadian organization or facility to such a degree that the foreign third party may gain unauthorized access to Classified information.

In certain circumstances, where extremely sensitive Information Security (INFOSEC) programs and contracts are involved, Public Services and Procurement Canada (PSPC) must conduct a Foreign Ownership, Control or Influence evaluation (*FOCI Evaluation)* on the ownership of an organization and examine the degree of actual or potential influence exercised by foreign interests. A FOCI Evaluation is also a requirement under the North Atlantic Treaty Organization (NATO) Security Policy. NATO nations, including Canada, are responsible for granting a Facility Security Clearance (FSC) for facilities located on their territory which are involved in NATO Classified contracts[1] (confidential and above). An assessment of FOCI aspects is part of this process.

When a FOCI evaluation is required for a contract, organizations must provide PSPC's Industrial Security Sector (ISS) with, among other information, details on ownership, actual and potential foreign influence and control, and foreign contracts and liabilities. The evaluation is conducted by PSPC and results in an administrative determination of the nature and extent of foreign dominance over an organization's management and/or operations.

The existence of Foreign Ownership, Control or Influence does not, in itself, prohibit an organization from holding a Facility Security Clearance. Each case is assessed individually and, where deemed necessary by ISS, details may be reviewed with the organization to determine whether certain measures can be taken to negate potential risks or reduce to an acceptable level.

ISS' evaluation will result in a determination of "Not under FOCI", "*Not under FOCI through Mitigation"* or "Under FOCI".

PART B – REQUIREMENT FOR A FOCI EVALUATION

A FOCI evaluation will be tied to the organization's Facility Security Clearance and will be carried out under the following circumstances among others:

a. an organization receiving a NATO / Foreign Classified or INFOSEC contract is required to undergo a FOCI evaluation as part of its Facility Security Clearance;
b. when there are significant changes to FOCI information previously provided by the organization.

[1] References to Classified throughout document refer to confidential and above

PART C – ORGANIZATION GUIDELINES

These Guidelines have been developed to assist organizations to prepare and submit the documentation needed by PSPC to conduct a FOCI evaluation. Please read them carefully and follow the instructions in detail to prevent delays caused by incomplete FOCI documentation.

Special Instructions:

1) Documents submitted by organizations are viewed as legal and certified business statements which must contain a true and factual account of the organization's business operations. Failure to answer all questions and to provide required and relevant supporting documentation or any misrepresentation (by omission or concealment, or by providing misleading, false or partial answers) may serve as a basis to deny access to INFOSEC and NATO / Foreign Classified material.

2) If an organization is unable to produce the documentation requested by ISS, appropriate alternate documentation must be provided with the necessary legal and certified business statements and an explanation regarding unavailability. If alternate documentation is not available, ISS will ascertain the information required by using alternative procedures such as: requesting additional information; conducting interviews with executives or officers; carrying out on-site visits; performing background checks; and, carrying out various other audit procedures, etc.

3) US ownership must be declared as foreign. During the evaluation PSPC will determine whether this ownership is mitigated by other factors or whether mitigation measures are required. If the organization has already filed a FOCI package in the US and received approval, provide the package along with the certification form. Approval by the US may be considered by PSPC as part of the FOCI evaluation process but will not supplant it.

4) A complete and distinct FOCI package must be prepared and submitted for the organization as well as for each of the organization's immediate (or direct) parent company and ultimate (or indirect) parent company. This consists of Step 1, 2 and 3.

5) All documents provided must cover 3 distinct time periods: the last 2 completed fiscal years and the most recent cumulative interim period of the current fiscal year.

A glossary of terms can be found in Part E.

Documents will be maintained on file by ISS and will be protected in accordance with Treasury Board of Canada Secretariat (TBS) Policy on Government Security, Appendix B of the Operational Security Standard on Physical Security and Appendix C of the Directive on Departmental Security Management.

Step 1 – Complete Organization Questionnaire

PROTECTED when complete

1) This questionnaire must be completed separately for the organization as well as for each of the organization's immediate (or direct) parent company and ultimate (or indirect) parent company.

QUESTION	NO	YES	IF YES, IDENTIFY TO WHAT EXTENT	IF YES, REFER TO STEP 3
1. Is there any Foreign Ownership or interest in your organization?				
1.1. Do foreign interests, directly or indirectly, own or have beneficial ownership in your organization's securities?				Factor 1.1
1.1. Does any foreign interest control or influence, or is any foreign interest in a position to control or influence an election, appointment, or tenure of any of your directors or officers?				Factor 1.2.
1.1. Is any class of your organization's securities or equivalent ownership rights registered in the name of a nominee or in some other method which does not disclose or identify the beneficial owner?				Factor 1.3.
2. Does your organization own any foreign interests in whole or in part?				Factor 2
3. Do any foreign interests have positions, such as directors or officers in your organization?				Factor 3
4. Does your organization derive any income from foreign interests and/or have any arrangements (contacts, agreements, understandings) with foreign interests?				Factors 4.1 and 4.2.
5. Does your organization have any indebtedness, liabilities and/or obligations that are owed to foreign interests?				Factor 5

6. Do any members of your organization's board of directors (or similar governing body) hold any positions with, or serve as consultants for, any foreign interests?				Factor 6
7. Are there any individuals, whether or not they are employees, who may visit your facility (or facilities) in a capacity which may permit them to have access to INFOSEC or NATO / Foreign Classified materials?				Factor 7
8. Does your organization have any other foreign involvement not otherwise stated in your answers to the above questions?				Factor 8

All FOCI Factors identified within the questionnaire will be verified or confirmed by PSPC regardless of whether the response is positive or negative.

REMARKS (attach additional sheets, if necessary)

Step 2 – Prepare Basic Documentation

1. Separate documentation must be prepared and submitted for the organization as well as for each of the organization's immediate parent company and ultimate parent company.

2. All documents must cover the last 2 completed fiscal years and the most recent cumulative interim period of the current fiscal year.

3. Documentation must be provided in sequential order and clearly marked in order to expedite review by ISS and to prevent the documentation from being returned to the organization for update or proper completion.

	File Name	Comments or Clarification (optional)
1. Articles and Certificate of Incorporation		
2. Organizational Charts a) Corporate Ownership Chart – This chart is to identify the original source of ownership (parent) and is to indicate the independent holdings of each organization in the "family tree". All ownership identified within this chart is to be expressed as a percentage (%) of total ownership.		
b) Corporate Board of Directors Chart – The composition of the Boards of Directors of all the companies/corporations involved in the corporate "family tree", including names, titles, citizenship, and security clearance, if any.		
3. Minute Book (or other such titled legal document which is maintained by the Board of Directors according to the organization's charter. If this cannot be produced, excerpts from the Minute Book which are directly related to foreign ownership, control or influence or specific FOCI factors.		
4. Shareholders Registry		
5. Annual Report including a complete set[2] of yearly audited financial statements, along with the accompanying independent auditor's report (for public companies). For private companies, provide a complete set of yearly financial statements (whether or not audited), along with the accompanying independent auditor's report, if applicable.		

[2] Complete set refers to the following as a minimum: 1) Balance sheet (or statement of financial position); 2) Income statement (or statement of operations); 3) Cash flow statement; and 4) Related notes accompanying the financial statements explaining in sufficient details each and every important account, among others.

6. Complete set[1] of unaudited financial statements for the requested most recent cumulative interim period of the current fiscal year.		
7. Other relevant documents and information. In order to provide accurate determinations, PSPC may request additional information/documents from the organization that it feels are pertinent to the evaluation. It is the responsibility of the organization to provide all such documents upon request. Alternatively, and to accelerate the process, you may decide to provide us with any such relevant document that may be useful, even before we request it.		

Step 3 – Prepare Additional Documents Required for Each Factor

1. For each "yes" response in Step 1, follow the instruction(s) associated with the specific Factor and provide the requested documentation. This should be done separately, as appropriate, for the questionnaire completed for the organization, immediate parent and ultimate parent.

2. All documents must cover the last 2 completed fiscal years and the most recent cumulative interim period of the current fiscal year.

FOCI Factor #1 **Foreign ownership or beneficial ownership**
1.1 **Foreign interest ownership or beneficial ownership of the facilities securities or other equivalent ownership rights (1% for private companies; 10% for public companies)**

1. Outline the general distribution of the organization's overall shares/securities by %. Use a chart format (pie graph) to illustrate the associated areas, i.e. organization directors, publicly traded, foreign owned, etc.

2. In text below the chart, provide a detailed breakdown of all-foreign owned shares/securities, identifying %, individuals or organization's name, headquarters address, and country of origin. Include the following:
    a. indirect ownership through subsidiaries; and
    b. voting rights of each class of stock.

3. If there are any shareholder agreements, attach copies. If not, state that there are no shareholder agreements.

4. Ownership by foreign interests of less than the threshold requested (i.e., 1% for private companies and 10% for public companies) must be disclosed if such holdings entitle the interest/individuals to control or influence the appointment or tenure of Key Senior Officials (KSOs).

1.2

Foreign interests that control or influence, or are in position to control or influence, the election, appointment or tenure of directors or officers of the organization, whether or not such power has been exercised

The name, citizenship, address of employment and security clearance, if any, of the foreign interest(s) is to be provided, including all details concerning the individual's extent of involvement in the operations of the organization and control or influence.

1.3

1% or more (private companies) and 5% or more (public companies) of any class of the organization's securities or equivalent ownership rights registered in the name of a nominee or in a manner that does not disclose the beneficial owner.

1. Identify each foreign institutional investor holding 1% (private organizations) or 5% (public organizations) or more of the voting stock. Include individual/organization's name, address, and percentage of stock held.

2. State whether each foreign investor has exerted, or attempted to exert, any management control or influence over the appointment of Key Senior Officials, other management personnel, or the policies of the organization. Detailed information must be provided on any such attempts, the organization's responses, along with the present status.

3. Brokerage houses or investment institutions that are holding stocks in *"street names"* are to be included within this factor. The percentage of stocks that each organization is holding in *"street names"* is to be provided.

FOCI Factor #2

Ownership of 10% or more in any foreign interest by the organization.

1. Provide details of all foreign ownerships (companies/subsidiaries/affiliates) in columns under the following headings: organization name; address; country; % of ownership (account for total ownership); parent company officials - foreign positions (to include name, title, Citizenship, security clearance if applicable and to what extent they are involved in the operations of the Canadian and foreign organizations).

2. If an employee is a *Representative of a Foreign Interest*, a declaration must be made regarding the individual's access to INFOSEC or NATO / Foreign Classified information by virtue of their position, knowledge or expertise.

3. Every employee of the organization who is a *Representative of a Foreign Interest* and who has a security clearance or whose clearance is pending must execute a statement of full disclosure of foreign affiliations. In the case of a Key Senior Official (KSO), the statement must be noted by the Corporate Board of Directors in the organization's Minute Book.

   If a Canadian firm owns organizations in a foreign country, these are to be considered as foreign organizations.

FOCI Factor #3

Management positions such as directors and officers held by foreign interests.

1. Provide the names, citizenship, place and address of employment, position and title and security clearance of all foreign individuals who occupy management positions within the organization.

2. Attach copies of applicable by-laws or articles of incorporation which describe affected position(s). If all of this information is already included in the organization chart requested in Step 2 (Basic Documentation), no additional information is required.

FOCI Factor #4

Arrangements with foreign interests and income derived from them.

4.1

Contracts, agreements or understandings (CAU) with foreign interests.

1. Provide in column format, or use the best means possible to identify required data in the following six categories for each CAU that represents 5% or more of the organization's total revenues or net income: name; address; country; nature of the CAU (see below); amount of income derived (specify currency involved) and % of the total revenues it represents.

2. The nature of the CAU must be identified: the second party; the type of arrangement (contract, agreement, or understanding); details of what it involves and whether it is commercial or defence-related, and; whether it involves INFOSEC or NATO / Foreign Classified information.

3. If, during the evaluation of this section, PSPC is unable to discern the extent of the CAU and/or for any other reason, the organization may be requested to provide a copy and/or briefing on the CAU.

4. When items applicable to Canadian Export Controls are being exported by an organization due to its involvement in contracts, agreements or understandings, compliance with export license requirements must be acknowledged.

5. If a large number of commercial (not defence related) licensing, patent, trade secret, joint venture, or technology transfer agreements are in place with foreign interests, but represent a small percentage of the organization's gross income and do not involve INFOSEC or NATO / Foreign Classified information, the explanation to be provided can be a short generalized statement addressing these elements. The percentage of gross income that these agreements represent, as a total, must be provided.

4.2

Any income derived from foreign interests.

1. Identify whether your organization derived 5% or more of its total revenues or net income (in Canadian dollars or in the currency used to present its financial statements), from any single foreign interest.

2. Identify whether your organization derived, in the aggregate, 30% or more of its total revenues or net income (in Canadian dollars or in the currency used to present its financial statements) from all foreign interests.

3. Provide a detailed schedule of gross revenues (in Canadian dollars or in the currency of origin) broken down by country of origin of the payers, including the revenues generated from the entities referred to in the above questions 1 and 2. This schedule has to be reconciled with the income figures provided in the financial statements.

4. Identify any income (other than the revenues already addressed in the previous questions for Factor # 4.2) from other foreign sources such as dividends from foreign subsidiaries, royalties from licensing and patent agreements, dividends from foreign stock holdings, investments, or real estate (specify the currency involved).

FOCI Factor #5

Indebtedness, liabilities and obligations owed to foreign interests.

1) Identify whether your organization, as borrower, surety, guarantor or otherwise, has any indebtedness, liabilities or obligations to a foreign interest. Provide information on: the amount of any foreign debt (specify the currency involved); the type of debt; name and address of organization involved; collateral used including voting stock; any conditions or covenants and the impact the debt has on the current assets of the organization. Provide a copy of the agreements or pertinent extracts including, among others, procedures to be followed in the event of default.

2) If debentures are involved and they are convertible, specifics (i.e., rights, privileges, conversion features, etc.) must also be provided.

3) Identify if loan payments are or were in default.

4) Provide details if a foreign entity or individual guarantees any indebtedness, liability and/or obligation of the company, or has control or an influence role with regards to financing the operations of the company.

5) All guarantees provided by a parent company on behalf of its subsidiaries must be fully documented. Details must be provided on the financial institution involved and the purpose of the loan.

6) Conditions of a loan agreement, such as power to nominate board members of managerial personnel, must be declared and specifics provided.

7) Details of off-balance sheet arrangements, commitments and/or contingencies with foreign interests, if any, must be provided (specify the currency involved).

8) FOCI Factor #5 should be answered in the affirmative if the debt is with a Canadian entity that is owned or controlled either directly or indirectly by a foreign interest. If unknown, so state.

FOCI Factor #6

Directors, officers, executives and senior managers of your organization holding positions with, or serving as consultants for, foreign interests

1) All directors, officers, executives and senior managers of an organization who hold positions with, or serve as consultants to, foreign interests must be identified: name, capacity or title/position held, citizenship, security clearance, foreign organization name(s) and address(es) including country of origin.

2) If a director, officer, executive or senior manager is involved on an interlocking basis with more than one organization at the same time, each organization that he/she is involved with is to be declared and the above information provided.

3) Provide the same information requested above on wholly or partially-owned subsidiaries in foreign countries.

FOCI Factor #7

Access to INFOSEC or NATO / Foreign Classified material within an organization.

1) Identify names, title and position, nationality, security clearance and involvement of all employees who may have access to INFOSEC or NATO / Foreign Classified material.

2) Describe controls and tests put in place to manage the risks related to employees who may have access to INFOSEC or NATO / Foreign Classified material. Indicate the effective date(s) of these controls and the date(s) tests were last conducted.

3) Identify whether organization has had a breach or incident involving INFOSEC or NATO / Foreign Classified information in the past 10 years and describe the additional internal controls put in place to prevent, deter and identify such a breach or incident in the future. Any such breach or incident should be described in detail.

4) Identify if organization has submitted an application for a FOCI evaluation within the past five years with any member of NATO. For each successful FOCI application, provide a general description of the services performed in connection with the contract awarded, the name of the country involved, and the duration of the contract and FOCI clearance certificate. For each unsuccessful FOCI application, provide details as to why the contract was not awarded.

FOCI Factor #8

Any other factor that demonstrates a capability on the part of foreign interests to control or influence the management or operations of an organization.

Provide any relevant comments, observations, clarification and information as it relates to FOCI that has not been addressed or dealt with specifically in your answers to Factors #1-7.

Step 4 – Complete FOCI Certification and Consent Form

The organization must submit a signed FOCI Certification and Consent Form (Part F). This is a legal submission that requires an officer of the organization to certify that all documents being submitted to PSPC are factual, accurate, complete and free from any material misstatement.

Prior to the completion of the form, ensure that all required information and documentation has been prepared and packaged according to these Guidelines. The certification encompasses all documentation that is required within the FOCI evaluation; it should not be signed or dated until all the information available has been collected and gathered together.

Do not certify or distribute an incomplete FOCI evaluation package, as the certification will be rendered ineffective and the package returned for completion.

If PSPC finds that such disclosures are fraudulent or misrepresented after the certification has been completed, it can be grounds to terminate any further proceedings on the FOCI evaluation and thus eliminate the organization from any further participation in INFOSEC or NATO / Foreign Classified contracts or negotiations.

Step 5 – Submit Documentation

When the steps outlined above have been taken, all documents requested in Part C, Steps 1-4 should be submitted by CD/DVD or USB Key. Information should be presented in a clear and concise manner with appropriate names or file names used to identify different documents.

1. Organization Questionnaire *(refer Step 1)*
2. Basic Documentation (Items 1-7) *(refer Step 2)*
3. Additional Documents required for each Factor *(refer Step 3).* Clearly identify and separate each factor being addressed.
4. FOCI Certification Form (signed) *(refer Step 4)*

<u>Send in CD/DVD or USB Key format to:</u>

Industrial Security Sector
PSPC Central Mail Room
Place du Portage, Phase 3, 0B3
11 Laurier Street
Gatineau, Quebec
K1A 0S5
c/o: ISS FOCI Office, 2745 Iris Street (6th Floor)

<u>Contact:</u>

Questions can be sent by e-mail to: SSI Évaluation PCIE - ISS FOCI Evaluation

Step 6 – Advise PSPC of Organizational Changes (Ongoing)

If changes occur within an organization's business operations that affect the information provided to ISS, the organization is responsible to provide ISS with an update as soon as reasonably possible.

> **Important: If the change directly involves Foreign Ownership, Control or Influence, the Industrial Security Sector must be notified in writing immediately.**

PART D – PSPC EVALUATION AND RESULTS

Once the documentation is received, PSPC will conduct an evaluation to determine the nature and extent of foreign dominance over your organization's management and/or operations. For INFOSEC requirements, the Communications Security Establishment Canada (CSEC) is responsible for approving release of INFOSEC to non-government entities. In these circumstances, PSPC will seek CSEC's approval of the results of evaluation.

ISS' evaluation will result in an administrative determination on whether there is:

- No evidence of FOCI
- Evidence of FOCI – no mitigation measures required
    - This will be assigned when ISS can identify existing factors that mitigate risks.
- Evidence of FOCI – mitigation measures required
    - ISS will determine whether measures can be implemented by the company to mitigate any identified risk. In such circumstances, ISS will contact the organization with further instructions.
- Evidence of FOCI – no mitigation possible
    - In these instances, a company will be prohibited from being involved with INFOSEC or NATO / Foreign Classified contracts.

PART E – GLOSSARY

Agreement(s) – A legally enforceable understanding between two or more legally competent parties. Agreements or contracts can relate to voting trusts, licensing, sales, patents, trade secrets, technology transfers, agency arrangements, formation of cartels, partnerships, joint ventures, etc

Beneficial Owner – A person who has the rights of a shareholder although their name is not on the share certificate or is not listed in the register of shareholders. Beneficial ownership includes ownership through any trustee, legal representative, agent or mandatary, or other intermediary.

Bonds – A debt investment in which an investor loans money to an entity (corporate or governmental) that borrows the funds for a defined period of time at a fixed interest rate.

Cartel – An organization created from a formal agreement between a group of producers of a good or service, to regulate supply in an effort to regulate or manipulate prices.

Communications-Electronic Security (COMSEC) – The protection that results from the application of crypto security, transmission security and emission security measures to telecommunications, non-telecommunications emissions, and information handling equipment, and from the application of other measures appropriate to COMSEC information and material. COMSEC also includes the instruction required to effect this protection. These measures are designed to prevent compromise of information stored, transmitted, or processed on information technology systems. COMSEC is also designed to ensure the authenticity of telecommunications.

Computer Security (COMPUSEC) – The protection resulting from measures designed to prevent compromise of information stored or processed on a computer system. This protection results from the applications to EDP facilities of hardware, software and operations security, and other measures appropriate for EDP systems and facilities, excluding COMSEC.

Convertible Debentures – Bonds which the holder can exchange for shares of voting stock.

Covenant – Usually a formal agreement between two or more parties to do or not do something. Negative or restrictive covenants forbid the promissor from undertaking certain activities while positive or affirmative covenants require the promissor to meet specific requirements. A Bond Covenant is a legally binding term of an agreement between a bond issuer and a bondholder designed to protect the interests of both parties.

Debenture – A promissory note or bond backed by the issuer's general credit.

Debt Obligation – A bond, debenture, note or other evidence of indebtedness or guarantee of a corporation, whether secured or unsecured.

Director – An individual elected by the shareholder(s) to supervise the management of a corporation. Together, all directors of a corporation are referred to as the "board of directors".

Facility Security Clearance – An administrative determination that an organization is eligible, from a security viewpoint, for access to “Classified” or “Protected” information or assets at the same or lower classification level as the clearance being granted.

Foreign Interest – Any foreign government or agency of a foreign government, any form of business enterprise organized under the laws of any country other than Canada, any form of business enterprise organized or incorporated under the laws of Canada or a province which is owned or controlled by a foreign government, firm, corporation or person. Included in this definition is any natural person who is not a citizen or national of Canada.

Foreign ownership, control or influence – A situation whereby a third party individual, firm or government is assumed to possess dominance or authority over a Canadian organization or facility to such a degree that a third party individual, firm or government may gain unauthorized access to INFOSEC or NATO / Foreign Classified information.

Indebtedness – Owing something or being under obligation to another party.

Information Security (INFOSEC) – All Communications-Electronic Security (COMSEC) or COMPUSEC information and material entrusted to or developed/evaluated by or for the Communications Security Establishment.

- **INFOSEC Contracts** – All contracts, subcontracts, pre-contractual negotiations or other government approved agreements/understandings involving the release of INFOSEC or participation in a CSEC INFOSEC product evaluation program.
- **INFOSEC Equipment** – Equipment, including computer programs or other data, designed to provide security to telecommunications and computer systems.

Joint Venture – A partnership or cooperative agreement between two or more persons or firms usually restricted to a single specific undertaking. Normally the undertaking is of short duration, such as for the design and construction of a building or structure.

Key Senior Official – An individual who must be granted a Personnel Security Clearance before an organization will be granted a Facility Security Clearance. This includes the Company Security Officer and the owners, officers, directors, executives and partners who occupy positions which would enable them to adversely affect the organization's policies or practices in the performance of Classified contracts.

Liability – A broad legal term. In general, a debt owed. The condition of being actually or potentially subject to an obligation; a condition of being responsible for a possible or actual loss, penalty, evil, expense or burden; a condition that creates a duty to perform an act immediately or in the future.

Licensing Agreement – A written agreement entered into by the contractual owner of a property or activity giving permission to another to use that property or engage in an activity in

relation to that property. The property involved in a licensing agreement can be real, personal or intellectual.

Nominee Share – A share of stock of registered bond certification which has been registered in a name other than actual owner.

North Atlantic Treaty Organization (NATO) – An alliance of 28 countries from North America and Europe committed to fulfilling the goals of the 1949 North Atlantic Treaty. NATO's fundamental role is to safeguard the freedom and security of its member countries. Canada's participation in the NATO facilitates the exchange of information with member countries when there is an industrial security requirement.

Obligation – An agreement to pay money or some other valuable consideration.

Off Balance Sheet – Asset or debt or financing activity not on an organization's balance sheet.

Officer – An individual appointed by the director(s) of a corporation to manage the day-to-day business of a corporation, such as president, vice president, secretary, treasurer, the comptroller, the general counsel, the general manager, a managing director, or any other individual who performs functions for a corporation similar to those normally performed by an individual occupying any of those offices. The position of officer is distinct from that of director, although in a small corporation one individual may often occupy both positions.

Organization – Any person or institution, other than a Canadian (federal) government department, agency or crown corporation. This Includes commercial corporations, business entities, university faculties and partnerships.

Representative of a Foreign Interest – Citizens of Canada who are acting as representatives, officials, agents or employees of a foreign government, firm, corporation or person. However, a Canadian Citizen or national who has been appointed by his/her Canadian employer to be its representative in the management of a foreign subsidiary (i.e., foreign firm in which the Canadian company has ownership of at least 51% of the voting stock) will not be considered a representative of a foreign interest solely because of his/her employment, provided the appointing employer is his/her principal employer and is a firm that possesses or is in the process of obtaining a Facility Security Clearance (FSC).

Security/Securities – A share of any class or series of shares or debt obligation of a corporation and includes a certificate evidencing such a share or debt obligation, e.g., any note, stock, treasury stock, bond, debenture, certificate of interest or participation in any profit sharing agreement, etc.

"*Street Name*" – The common practice of registering publicly traded securities in the name of one or more brokerage firms.

Technology Transfer – Agreement between two parties for the sharing or transferring of technology for internal use or sale purposes.

Voting Trust – An agreement whereby a disinterested party, a trustee, agrees to assume responsibility for voting stock and to exercise management of another party's organization, independent of, and without, interference from the other party.

PART F - FOREIGN OWNERSHIP, CONTROL AND INFLUENCE ORGANIZATION CERTIFICATION AND CONSENT

PROTECTED when complete

I certify that I have read and understand this certification, that the statements and the information provided to Public Services and Procurement Canada for the purpose of conducting a Foreign Ownership, Control and Influence Evaluation of the Organization (identified below) have been given in good faith and are true, complete and correct to the best of my knowledge and that I am authorized to execute the certification on behalf of the Organization.

I consent to the disclosure of the information submitted by the Organization for its subsequent verification and/or use in an investigation for the purpose of conducting a Foreign Ownership, Control and Influence Evaluation for a Facility Security Clearance. I acknowledge that the information may also be verified and/or used in an investigation when the Facility Security Clearance is updated or otherwise reviewed for cause under the Policy on Government Security (PGS). I acknowledge that the information collected may be disclosed to the Royal Canadian Mounted Police (RCMP) and the Canadian Security Intelligence Service (CSIS) or other government departments for relevant checks and/or investigation in accordance with the PGS. This consent will remain valid until a Facility Security Clearance is no longer required or until an authorized officer of this organization sends notice, in writing, to the Industrial Security Sector of Public Services and Procurement Canada, revoking it.

_____	_____
Name	Signature
_____	_____
Title	Organization
_____	
Date	