



**INTERNATIONAL INDUSTRIAL SECURITY DIRECTORATE (IISD)
PUBLIC SERVICES AND PROCUREMENT CANADA**

Version July 18, 2017

GUIDE FOR ALTERNATIVE SOLUTION PROCESS

Table of Contents

GLOSSARY OF TERMS 2

BACKGROUND ON THE ALTERNATIVE SOLUTION PROCESS 3

INTRODUCTION 5

SUBMITTING THE ATTESTATION FORM 5

SUBMITTING PROOF OF INCORPORATION 6

SUBMITTING BACKGROUND VERIFICATIONS AND CRIMINAL RECORD CHECKS 6

CANADIAN DSA VALIDATION OF PROOFS 8

ARRANGING THE REQUEST FOR SITE ACCESS 8

AMENDMENT(S) TO THE SECURITY SCREENING DETAILS LIST 8

CANADIAN VISA REQUIREMENTS 9

APPENDIX A – COMPLETE LIST OF REQUIRED CHECKS 9

GLOSSARY OF TERMS

Canadian Designated Security Authority (Canadian DSA) is the Industrial Security Sector (ISS), Public Services and Procurement Canada (PSPC), administered by International Industrial Security Directorate (IISD), PSPC.

Designated Key Senior Officials (KSO) includes 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 the contract/subcontract.

Contract Security Officer (CSO) shall be appointed by the Chief Executive Officer (CEO) or the designated Key Senior Official (KSO) of the foreign organization.

Departmental Security Officer (DSO) or designate is responsible to manage the Departmental Security program on behalf of their Department(s).

Site Security Officer (SSO) is assigned by the DSO and is responsible for the protection of specific sites, property, people and/or equipment.

BACKGROUND ON THE ALTERNATIVE SOLUTION PROCESS

Many of Canada's trading partners do not recognize Canada's PROTECTED information/asset levels nor do they have an accepted equivalency to RELIABILITY status. As a result, most countries are reluctant to security clear their companies at higher levels as it is costly, time consuming and it exceeds the necessary requirement.

As a result, in January 2014, the Industrial Security Sector (ISS) of Public Services and Procurement Canada (PSPC), received deputy minister approval to develop an alternative solution security framework based on best practices, which ensures that PROTECTED information, handled abroad, is safeguarded according to standards similar to those required for Canadian suppliers, even when there is no international bilateral security instrument. Instead of those instruments, contract-specific security clauses and the contracts themselves are used to ensure that foreign suppliers safeguard the PROTECTED information appropriately.

Based on an overall assessment of these risk factors, contract clauses are used to articulate the required specific safeguarding measures such as personnel background checks, physical security and information technology security in a manner that approximates what would be required in Canada.

Requests for access to Canadian restricted site(s) and/or CANADA PROTECTED information/assets under a contract/subcontract requiring RELIABILITY status is also managed under the Alternative Solution process.

With an Alternative Solution, the foreign suppliers do not have to be registered in the Industrial Security Program of their country. Instead, they must provide proofs to IISD that they meet the security equivalencies accepted by the Canadian DSA for these contracts/subcontracts. Based on adequate amount of supporting information and analysis, and with the application of the contractual security measures listed below, it is assessed that the risk of compromise to information and/or sensitive sites is **LOW**.

HOW AN ALTERNATIVE SOLUTION IS APPLIED

Proposed contractual security mitigating measures are applied as follows *(depending on the Scenario used, some or all of these security measures may apply)*:

- ✓ Security clauses are included in the contract;
- ✓ The Supplier is legally-bound by the PWGSC contract;
- ✓ Contract clauses stipulate security requirements for accessing PROTECTED information/assets including the requirement for: personnel screening, the "need-to-know" principle and physical/IT security requirements;
- ✓ Contract clauses will address security breaches and steps to be taken in the event of loss or compromise of transmitted information/assets;
- ✓ The Supplier must provide proof of incorporation or authorization to do business in their jurisdiction;

- ✓ The Supplier must provide proof of registration with their National Privacy Authority, in accordance with the foreign legislation which may include authority to prosecute for breaches;
- ✓ The Supplier must provide a high-level description of security solutions to be implemented to meet the security requirements of the contract at bid submission;
- ✓ An Attestation Form must be signed by the Supplier's Chief Executive Officer, or delegate, to attest that the Supplier will abide by the security clauses included in the contract;
- ✓ The Supplier must appoint a Contract Security/Privacy Officer, who formally undertakes to oversee compliance with all privacy and security requirements included in the contract;
- ✓ The Supplier must appoint a Contract Security Officer (CSO) who formally undertakes to oversee compliance with all security requirements included in the contract; and
- ✓ The Supplier must conduct background and criminal records checks on all individuals having access to PROTECTED information/assets and/or restricted site access.
- ✓ The Supplier must provide site-specific security plans for review and approval by IISD. If there are deficiencies in the plans, IISD will notify the Suppliers of the deficiencies to be corrected before approval is granted;
- ✓ The Supplier must provide regular risk assessments and privacy impact assessments to IISD. IISD conducts risk assessments and any risks identified will be re-evaluated on an ongoing basis and any remedial actions will be brought forth to a Risk Advisory Committee with the Client and Contracting Authorities;
- ✓ Compliance visits are carried out on a case-by-case basis by IISD in accordance with the contract clauses;
- ✓ Any database containing PROTECTED B information would have to be located in Canada or in a Trusted Allies country; and
- ✓ IISD participates in bid evaluations (security/privacy group).

INTRODUCTION

- ❖ In accordance with the foreign security requirements of the contract/subcontract, the CSO is responsible for submitting the documents described in this manual, to the Canadian DSA.
- ❖ It is **important** to note that failure to do so may result in a breach of contract/subcontract and may prevent a foreign supplier from accessing Canadian restricted site(s) and/or CANADA PROTECTED information/assets.
- ❖ In summary, the individual(s) requiring access to Canadian restricted site(s) and/or CANADA PROTECTED information/assets under the contract/subcontract **MUST** meet the following requirements:
 - i. The individual(s) have a need to know;
 - ii. The *Attestation Form, Proof of Incorporation, Criminal Record Checks and Background Verification* are completed and sent to the Canadian DSA;
 - iii. The confirmation e-mail of verification/validation from the Canadian DSA has been received by the CSO, DSO and/or SSO;
 - iv. *Request for Site Access* has been submitted to the SSO of the Canadian Government Department/Organization.

IMPORTANT NOTE:

The Procurement Officer or Prime Contractor must not award an Alternative Solution contract/subcontract until the Canadian DSA has validated that all contract security requirements stipulated within the contract have been met and a confirmation e-mail to that effect was provided to the Procurement Officer or Prime Contractor. Refer to the section of this document titled “Canadian DSA Validation of Proofs” for details.

SUBMITTING THE ATTESTATION FORM

- ❖ The Attestation Form must be submitted to the Canadian DSA immediately upon request as follows:
 - ❑ **Part I** must be completed and signed by the foreign supplier’s Chief Executive Officer (CEO), or the Designated Key Senior Official (KSO) of the organization who will appoint an individual as the Contract Security Officer (CSO);
 - ❑ **Part II** must be completed and signed by the appointed CSO to attest that he/she, on behalf of the foreign supplier, will abide by all the security requirements of the contract/subcontract; and
 - ❑ The completed and signed Attestation Form (Parts I and II) shall be submitted to the Canadian DSA for approval.

IMPORTANT NOTES:

- ❖ The Attestation Form is contract-specific and is only valid for the life of the contract/subcontract.
- ❖ An updated Attestation form must be submitted to the Canadian DSA if there is a change in CSO.

SUBMITTING PROOF OF INCORPORATION

- ❖ The CSO will ensure that *Proof of Incorporation* documents (Certificate of Incorporation or other legal documents proving existence of legal entity/authorization to conduct business) are submitted to the Canadian DSA.

SUBMITTING BACKGROUND VERIFICATIONS AND CRIMINAL RECORD CHECKS

PLEASE REFER TO THE COMPLETE LIST OF REQUIRED CHECKS AT APPENDIX A

- ❖ The CSO is responsible for ensuring that *Background Verification(s)* and *Criminal Record Check(s)* are conducted on all individuals before they can have access to Canadian restricted sites and/or CANADA PROTECTED information/assets.
- ❖ In accordance with the Policy on Government Security, the contract/subcontract security clauses will stipulate that the individual(s) of the foreign organization requiring access to Canadian restricted sites and/or CANADA PROTECTED information/assets shall be security screened at the level of RELIABILITY status. Since other countries do not have an equivalent security screening to Canada, the following documentation is to be completed and submitted to the Canadian DSA:
 - ❑ **CRIMINAL RECORD CHECKS** (covering the last five (5) years) **with favourable results** from a recognized governmental agency or private sector organization of the foreign supplier's country for EACH individual. This **MUST** be in the form of:
 - a) A letter from the governmental agency that conducted the criminal record check.
OR
 - b) A letter from the private sector organization that conducted the criminal record check on behalf of the government in that country.
OR
 - c) Valid proof of security clearance from the NSA/DSA of a country with which Canada has an International Bilateral Industrial Security Instrument.
 - ❑ If submitting in the form of a letter, it **MUST** include the following information for EACH individual:
 - Date the checks were conducted
 - Name of company/individual who conducted the checks
 - Surname and Given Name(s)
 - Gender
 - Date of Birth & Place of Birth
 - Citizenship

IMPORTANT NOTE:

- ❖ The Canadian DSA does not require original or copies of fingerprints.

- **BACKGROUND VERIFICATION** (covering the last five (5) years) consisting of Identity, Residency, Educational, Employment History and Credit Checks for EACH individual, as listed in **Appendix A** of the contract/subcontract (attached at the last page of this Guide). This **MUST** be in the form of:
 - a) Valid proof of background verification conducted by the governmental agency that conducted the check.
 - OR**
 - b) Valid proof of background verification conducted by the private sector organization that conducted the check on behalf of the government in that country.
 - OR**
 - c) A letter from the foreign supplier indicating that a Background Verification consisting of Identity, Residency, Educational, Employment History and Credit Checks for EACH individual was completed.

- The valid proof or letter **MUST** include the following information for **EACH** individual:
 - Date the checks were conducted
 - Name of company/individual who conducted the checks
 - Surname and Given Name(s)
 - Gender
 - Date of Birth & Place of Birth
 - Citizenship
 - Residency (within the last five (5) years)
 - Current Employer

- The CSO is responsible for submitting the *Background Verification(s)* and *Criminal Record Check(s)* for EACH individual to: SSIContratsInternationaux.ISSInternationalContracts@tpsgc-pwgsc.gc.ca

IMPORTANT NOTES:

- ❖ It is important to note that the *Request for Site Access* **CANNOT** proceed until IISD has received all the required security documentation.
- ❖ If the Prime Contractor or Project Officer requires the contract/subcontract to be awarded prior to the *Request for Site Access* (such as a phased approach project where equipment must be built first and the installation take place at a later time) the foreign supplier will still be required to initially submit a completed *Attestation Form* and provide *Proof of Incorporation* to the Canadian DSA. Once the identity of individual(s) is known for access to the site, the *Criminal Record Checks* and *Background Verification* are then completed and sent to the Canadian DSA for validation.
- ❖ The Canadian DSA considers *Background Verifications* and *Criminal Record Checks* to be valid for a period of five (5) years (from the date the Criminal Record Checks were conducted) OR for the duration of the contract/subcontract, whichever of these comes first.
- ❖ Updated security screening documentation must be submitted to the Canadian DSA before the validity expires (during the life of the contract/subcontract).

CANADIAN DSA VALIDATION OF PROOFS

- Once the Canadian DSA has validated the completed *Attestation Form, Proof of Incorporation, Criminal Record Check(s)* and *Background Verification(s)*, a confirmation e-mail will be sent to all stakeholders (including the CSO, Contract and Project Officers and DSO, containing the following information:
 1. Signed and approved *Attestation Form*; and
 2. *Security Screening Details List* of the individual(s) who are deemed to be security screened to the equivalent level of RELIABILITY status.

ARRANGING THE REQUEST FOR SITE ACCESS

- Upon receipt of the Canadian DSA equivalency confirmation e-mail that the security requirements have all been met, the CSO may proceed with arranging the details of the *Request for Site Access*; and
- The CSO is responsible for dealing directly with the DSO office/Site Security Officer (SSO) and ensuring the Canadian DSA is kept informed of agreed upon personnel and timings agreed to between parties .

IMPORTANT NOTES:

- ❖ Foreign suppliers **MUST NOT** submit a traditional *Request for Visit* through their country's NSA/DSA for an Alternative Solution contract/subcontract.
- ❖ Alternative Solution contracts/subcontracts are **not** handled through the traditional *Request for Visit* process via the Contract Security Program since the foreign supplier does not have to be registered in the Industrial Security Program of their country.

The Canadian DSA will **NOT** be involved in arranging details for the *Request for Site Access*, however, must be kept apprised (such as Carbon Copy on final e-mail detailing the names of individuals and agreed upon dates) for the purpose of oversight and validation of information provided. .

AMENDMENT(S) TO THE SECURITY SCREENING DETAILS LIST

Removal of Individual(s) from the Security Screening Details List

- The CSO **must** advise the Canadian DSA and the Canadian Government Department/Organization when an individual or list of individuals on the *Security Screening Details List* no longer requires Canadian restricted sites and/or CANADA PROTECTED information/assets (e.g. an individual leaves the organization or no longer requires access).

Addition of Individual(s) to the Security Screening Details List

- The CSO **must** advise the Canadian DSA and the Canadian Government Department/Organization when there is a new individual or list of new individuals to an existing *Request for Site Access*. The same process as the initial request must be followed.

CANADIAN VISA REQUIREMENTS

- ❖ The Canadian DSA is **NOT** responsible for the visa requirements of the foreign national(s) requiring access to Canadian restricted site(s) and/or CANADA PROTECTED information/assets.
- ❖ The Canadian DSA verification/validation for security screenings of foreign national(s) does not waive the visa requirements for those individual(s) travelling to the site. Please note that Canadian visa requirements differ by country. Please consult the Immigration Refugees Citizenship Canada (IRCC) website for individual requirements – <http://www.cic.gc.ca/english/visit/business.asp>.
- ❖ The foreign supplier is responsible for ensuring that the foreign national(s) have the required information, documents and authorizations before arriving in Canada to perform the contract/subcontract work.
- ❖ The foreign supplier is responsible for all costs incurred as a result of non-compliance with Canada's visa/immigration requirements.

APPENDIX A – COMPLETE LIST OF REQUIRED CHECKS

The Foreign recipient **Contractor/Subcontractor** must perform a security screening of all its personnel who will need access to **Canadian restricted sites and/or access to CANADA PROTECTED A and/or B information/assets**:

a) Identity check:

- i. Copies of two of valid original pieces of government issued identity documentation, one of which must include a photo
- ii. Surname (last name)
- iii. Full given names (first name) – underline or circle usual name used
- iv. Family name at birth
- v. All other names used (aliases)
- vi. Name changes
 1. Must include the name they changed from and the name they changed to, the place of change and the institution changed through
- vii. Sex
- viii. Date of birth
- ix. Place of birth (city, province/state/region, and country)
- x. Citizenship(s)
- xi. Marital status/common-law partnership
 1. Current status (married, common-law, separated, widowed, divorced, single)
 2. All current spouses (if applicable)
 - a. Surname (last name)

- b. Full given names (first name) – underline or circle usual name used
- c. Date and duration of marriage/common-law partnership
- d. Date of birth
- e. Family name at birth
- f. Place of birth (city, province/state/region, and country)
- g. Citizenship(s)

b) Residency check:

- i. The last five (5) years of residency history starting from most recent with no gaps in time.
 - 1. Apartment number, street number, street name, city, province or state, postal code or zip code, country, from-to dates.

c) Educational check:

- i. The educational establishments attended and the corresponding dates.

d) Employment history check:

- i. The last five (5) years of employment history starting from most recent with no gaps in time.
- ii. Three (3) employment reference check from the last five (5) years.

e) Criminal records check:

- i. Report(s) containing all criminal convictions for the last five (5) years in and outside of the candidate's country of residence.

f) Credit check:

- i. Credit check report where available.