
PART 7 – RESULTING CONTRACT CLAUSES [for the anticipated Request for Proposal (RFP)]

7.6 Security Requirements

A. SECURITY REQUIREMENTS FOR CANADIAN SUPPLIER:

PWGSC FILE #: EN578-131350 Revised # 3

1. The Contractor/Offeror must, at all times during the performance of the Contract/Standing Offer, hold a valid Facility Security Clearance at the level of **SECRET**, with approved Document Safeguarding at the level of **PROTECTED B**, issued by the Canadian Industrial Security Directorate (CISD), Public Works and Government Services Canada (PWGSC).
2. The Contractor/Offeror personnel requiring access to **PROTECTED** information, assets or sensitive work site(s) must **EACH** hold a valid personnel security screening at the level of **SECRET**, or **RELIABILITY STATUS, as required**, granted or approved by the CISD, PWGSC.
3. Until the security screening of the Contractor/Offeror personnel required by this Contract/Standing Offer has been completed satisfactorily by the Canadian Industrial Security Directorate, Public Works and Government Services Canada, the Contractor/Offeror personnel **MAY NOT HAVE ACCESS to PROTECTED** information or assets, and **MAY NOT ENTER** sites where such information or assets are kept, without an escort.
4. The Contractor **MUST NOT** utilize its Information Technology systems to electronically process, produce or store any sensitive **PROTECTED** information until CISD/PWGSC has issued written approval. After approval has been granted, these tasks may be performed at the level of **PROTECTED B including an IT link at the level of PROTECTED B**.
5. Subcontracts which contain security requirements are **NOT** to be awarded without the prior written permission of CISD/PWGSC.
6. The Contractor/Offeror must comply with the provisions of the:
 - (a) Security Requirements Check List and security guide (if applicable), attached at Annex 7;
 - (b) *Industrial Security Manual* (Latest Edition).

B. SECURITY REQUIREMENTS FOR INTERNATIONAL SUPPLIERS:

PWGSC FILE # EN578131350 Rev # 3

The **Contractor/Offeror /Subcontractor** must be from a Country with which Canada has an international bilateral industrial security instrument. The Industrial Security Program (ISP) has international bilateral industrial security instruments with the countries listed on the following PWGSC website: <http://ssi-iss.tpsgc-pwgsc.gc.ca/gvrnmnt/risi-ijsr-eng.html>
All **CANADA PROTECTED** information/assets, furnished to the Foreign recipient **Contractor / Offeror / Subcontractor**, shall be safeguarded as follows:

1. The Canadian Designated Security Authority (DSA) (Canadian DSA) is the International Industrial Security Directorate (IISD), Public Works and Government Services Canada (PWGSC). The Canadian DSA reserves the right to conduct compliance visits at its sole discretion, to ensure compliance with the below listed security measures.
2. The Foreign recipient **Contractor / Offeror / Subcontractor** shall, at all times during the performance of the **Contract**, hold a valid Facility Security Clearance, issued by the NSA/DSA of the supplier's country, at the equivalent level of **SECRET**, and hold an approved Document Safeguarding Capability Clearance at the level of **PROTECTED B**.
3. All **CANADA PROTECTED** information/assets provided or generated under this **contract** will continue to be safeguarded in the event of withdrawal by the recipient party or upon termination of the **Contract**, in accordance with the National Policies of the supplier's country.
4. The Foreign recipient **Contractor / Offeror / Subcontractor** shall provide the **CANADA PROTECTED** information/ assets a degree of safeguarding no less stringent than that provided by the Government of Canada in accordance with the National Policies, National Security legislation and regulations and as prescribed by the NSA/DSA of the supplier's country.
5. All **CANADA PROTECTED** information/assets provided to the Foreign recipient **Contractor / Offeror / Subcontractor** pursuant to this **contract** by the Government of Canada, shall be marked by the Foreign recipient **Contractor / Offeror / Subcontractor** with the equivalent security classification utilized by the supplier's country and in accordance with the National Policies of the supplier's country.
6. The Foreign recipient **Contractor / Offeror / Subcontractor** shall, at all times during the performance of this **Contract**, ensure the transfer of **CANADA PROTECTED** information /assets be facilitated in accordance with the National Policies of the supplier's country, and in compliance with the provisions of the Bilateral Industrial Security Instrument between the supplier's country and Canada.
7. Upon completion of the Work, the Foreign recipient **Contractor / Offeror / Subcontractor** shall return to the Government of Canada, via government-to-government channels, all **CANADA PROTECTED** information/assets furnished or produced pursuant to this **Contract**, including all **CANADA PROTECTED** information/assets released to and / or produced by its subcontractors.
8. In accordance with the Security Classification Guide **CANADA PROTECTED** information/assets shall be released only to Foreign recipient **Contractor / Offeror / Subcontractor** personnel, who have a need-to-know for the performance of the **contract** and who have a Personnel Security Clearance at the level of **RELIABILITY STATUS**, granted

by their respective NSA/DSA, in accordance with the National Policies of their respective country.

9. In accordance with the Security Classification Guide, Foreign recipient **Contractor Offeror / Subcontractor** personnel requiring privileged access to Information Technology systems shall each hold a valid Personnel Security Clearance at the **Secret** level.
10. Until the Foreign recipient's responsible NSA/DSA for industrial security of supplier's country has provided Canadian DSA with the required written Personnel Security Screening assurances, the Foreign recipient **Contractor / Offeror / Subcontractor** personnel SHALL NOT HAVE ACCESS to **CANADA PROTECTED** information/assets, and SHALL NOT ENTER "Government of Canada" or "Contractor" sites where such information or assets are kept, without an escort. An escort is defined as "a Government of Canada" or "Contractor" employee who holds the appropriate Personnel Security Clearance at the required level.
11. **CANADA PROTECTED** information/assets provided or generated pursuant to this **contract** shall not be further provided to a third party Foreign recipient **Subcontractor** unless:
 - a. written assurance is obtained from the third-party Foreign recipient's NSA/DSA to the effect that the third-party Foreign recipient **Subcontractor** has been approved for access to **CANADA PROTECTED** information by the third-party Foreign recipient's NSA/DSA; and
 - b. written consent is obtained from the NSA/DSA of the supplier's country, if the third-party Foreign recipient **Subcontractor** is located in a third country.
12. **Subcontracts** which contain security requirements are NOT to be awarded without the prior written permission of supplier's country NSA/DSA, in accordance with their National Policies.
13. The Foreign recipient **Contractor / Offeror / Subcontractor** MUST NOT utilize its Information Technology systems to electronically process, produce, or store on a computer system and transfer via an IT link any **PROTECTED B** information until the NSA/DSA of the supplier's country has granted approval to do so. After approval has been granted in writing to the Foreign recipient **Contractor / Offeror / Subcontractor**, these tasks may be performed up to the level of **PROTECTED B**.
14. The Foreign recipient **Contractor / Offeror / Subcontractor** shall not use the **CANADA PROTECTED** information/assets for any purpose other than for the performance of the **contract** without the prior written approval of the Government of Canada. This approval must be obtained by contacting the Canadian DSA.

15. The Foreign recipient **Contractor / Offeror / Subcontractor** visiting Canadian Government or industrial facilities, under this **contract**, will submit a Request for Visit form to Canada DSA, through their respective NSA/DSA.
16. The Foreign recipient **Contractor / Offeror / Subcontractor** shall immediately report to the Canadian DSA all cases in which it is known or there is reason to suspect that **CANADA PROTECTED** information / assets pursuant to this **contract** has been compromised.
17. The Foreign recipient **Contractor / Offeror / Subcontractor** shall immediately report to its respective NSA/DSA all cases in which it is known or there is reason to suspect that **CANADA PROTECTED** information/assets accessed by the Foreign recipient **Contractor / Offeror / Subcontractor**, pursuant this **Contract**, have been lost or disclosed to unauthorized persons.
18. The Foreign recipient **Contractor / Offeror / Subcontractor** shall not disclose the **CANADA PROTECTED** information to a third party government, person, firm or representative thereof, without the prior written consent of the Government of Canada. Such consent shall be sought through the recipient's National Security Authority/ Designated Security Authority (NSA/DSA).
19. The Foreign recipient **Contractor / Offeror / Subcontractor** shall comply with the provisions of the Bilateral Industrial Security Memorandum of Understanding between their country and Canada, in relation to equivalencies.
20. The Foreign recipient **Contractor / Offeror / Subcontractor** must comply with the provisions of the Security Requirements Check List attached at Annex 7.

7.6.1 Contractor's Site(s) or Premises Requiring Safeguarding Measures

[Information to be inserted at contract award, as provided by the bidder in RFP Submission Form (Form 1 to Part 4).]

- 7.6.1.1 The Contractor must diligently maintain up-to-date, the information related to the Contractor's and individual(s) site(s) or premises, where safeguarding measures are required in the performance of the Work, for the following address(es):

Street Number / Street Name, Unit / Suite / Apartment Number
City, Province, Territory / State
Postal Code / Zip Code
Country

7.6.1.2 The Company Security Officer (CSO) must ensure through the Industrial Security Program (ISP) that the Contractor and individual(s) hold a valid security clearance at the required level.