PART 6 - SECURITY, FINANCIAL AND OTHER REQUIREMENTS [for the anticipated Request for Proposal (RFP)]

6.1 Security Requirements

(a) Before award of a contract, the following conditions must be met:

(i) Canadian bidders must hold a valid organization security clearance as indicated in Part 7 –Resulting Contract Clauses, 7.6.1 (A) Security Requirement for Canadian Suppliers, clause 1.

(ii) Canadian bidders' proposed individuals requiring access to protected information, assets or sensitive work site(s) must meet the security requirement as indicated in Part 7 - Resulting Contract Clauses, 7.6.1(A) Security Requirement for Canadian Suppliers, clause 2.

(iii) International Bidders must be from a country that has an international bilateral industrial security instrument with the Industrial Security Program (ISP) of PWGSC as indicated in Part 7 – Resulting Contract Clauses, 7.6.1(B). The 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-iisr-eng.html.

(b) Canada will not delay the award of any contract to allow bidders to obtain or complete the required security screening activities.

(c) Bidders that do not currently have personnel and organization security clearances through the Canadian federal government, or bidders that do not meet the security requirements outlined in Part 7, or bidders seeking additional information on security requirements, should refer to the Industrial Security Program (ISP) of Public Works and Government Services Canada (http://ssi-iss.tpsgc-pwgsc.gc.ca/index-eng.html) website.

(d) In the case of a joint venture bidder, each member of the joint venture must meet the security requirements.

6.2 Data Sovereignty

The protection of information, from a privacy and security perspective, is core to the integrity of government programs, which underpins confidence in Canada. All information managed by Canada requires protection, including information published publicly in order to appropriately protect the confidentiality, integrity and availability of the information. EPS will process information up to and including “Protected B” and it is incumbent that the solution incorporates the appropriate controls in order to safeguard the interests of Canada and those of its partners to this level of security. No information above Protected B will be processed by this solution.

Furthermore, security controls, which ensure the confidentiality, integrity and availability of the solution, are imperative requirements for the EPS, as Canadians expect Canada to take all appropriate measures to protect personal and sensitive information.

Therefore, the EPS and infrastructure will be required to be established within the geographic boundaries of Canada. Stringent contractual and technical measures must be put

in place to ensure that government information is secured at all times, at rest and in motion, through encryption protection and is only accessed by those authorized to access the infrastructure for those purposes approved by the EPS.