INVITATION TO QUALIFY

Annex A

Phase 1 Evaluation Requirements

Cyber Security Procurement Vehicle

(CSPV)

ANNEX A – Phase 1 Evaluation Requirements

1.0 Introduction

For a full description of the ITQ Phase 1 – Mandatory Criteria Evaluation Process, refer to section 4.2 of the ITQ document.

2.0 Evaluation of Mandatory Requirements

As part of the Phase 1 – Evaluation Requirements, Respondents must substantiate their compliance to the following mandatory requirements in the form of a written response:

Table 1		
Mandatory ID	**Sub-Category**	**Requirement**
M1	Technical	The Respondent must have developed, deployed, implemented or certified at least one (1) cyber security solution or product, that meets at least one (1) of the following security functions and services*: **For evaluation purposes for M1, Security Functions and services are the numbered elements (i.e. 1. Data Loss Prevention) not the individual bullets underneath the security function or service.* 1. Data Loss Prevention (DLP) ▪ Data Labelling / Tagging ▪ Endpoint DLP Enforcement ▪ Network DLP Enforcement ▪ Information Rights Management 2. Encryption ▪ File Encryption ▪ Full Disk Encryption ▪ Removable Media Encryption ▪ Hardware Security Modules ▪ Application Layer Encryption ▪ Database Encryption ▪ Email Encryption 3. Data Science ▪ Modelling / Grooming ▪ Sanitizing 4. Key Management ▪ Enterprise Key Management Tools ▪ Hardware Security Modules (HSM)

		5. Malware Prevention ▪ Email Anti-malware ▪ Email Anti-Spam ▪ Host Anti-malware ▪ Host Intrusion and Protection (HIPS) 6. Detection and Response ▪ Endpoint Detection and Response (EDR) 7. Protection ▪ Application Virtualization / Containment ▪ Application Whitelisting ▪ File Integrity Monitoring ▪ Host Firewall ▪ Port and Device Control 8. Authentication ▪ Authentication, Authorization and Auditing (AAA) ▪ Timestamping ▪ Code and Document Signing ▪ Multi-factor Authentication ▪ Single-Sign On / Federation 9. Credential Management ▪ Non-Person Entity Certificates ▪ Person entity credentials at levels of assurance 1-4 ▪ Certificate Lifecycle Management / Automation ▪ Identity as a Service ▪ Public Key Infrastructure ▪ Secrets Management 10. Directories ▪ Access Management ▪ Change Auditing ▪ Enterprise Directory and Identity Stores ▪ Identity Governance and Administration ▪ Privileged Access Management 11. Cloud / DC ▪ Cloud Access Security Brokers ▪ Cloud-based security services 12. Firewall ▪ Application Firewall ▪ Network Firewall ▪ Web Application Firewall ▪ Web Content Filtering 13. Network / Perimeter ▪ Network Access Controls (RA, VPN, UTM) ▪ Sinkhole ▪ Content Filtering

		▪ Data Diodes ▪ Cross Domain Appliances ▪ Forward Proxy / Reverse Proxy ▪ Secure Web Gateway ▪ SMTP Email Relays ▪ URL Reputation 14. Network Detection and Prevention ▪ DDoS / DoS: Cloud ▪ DDoS / DoS: In-line ▪ IDPS ▪ Network inline Anti-Virus ▪ Sandboxing 15. Centralized Logging Services (CLS) ▪ Centralized Log Collection ▪ Centralized Log Storage 16. Infrastructure Awareness ▪ Infrastructure Discovery ▪ Network and Behaviour Analytics ▪ Policy Compliance (Tool Automation) ▪ Visualization Tool (Dashboard) 17. Threat Intelligence Feeds (CTI) 18. Security Configuration Management ▪ Asset Discovery ▪ Configuration Automation ▪ Infrastructure Security CMDB 19. Security Orchestration, Automation and Response (SOAR) ▪ Containment Automation ▪ Incident Containment ▪ Playbook Automation ▪ Report Automation 20. Vulnerability Management ▪ OS and Application Scans ▪ Vulnerability Assessment 21. Digital Identity (identity-related services) ▪ Identity validation ▪ Identity verification 22. Secure Communication ▪ Secure Video Conferencing ▪ Secure Audio Conferencing ▪ Secure Instant Messaging ▪ Secure Remote Management

M2	Corporate	The Respondent must have a minimum of $6M in billable revenue over the last 3 years as of the ITQ posting date; **-OR-** The Respondent must have a Commercially Available product related to the security function or service they identified in M1, with a minimum of 5 current paying customers; **-OR-** The Respondent must have received a grant or signed a contract related to cyber security innovation from either: ▪ the Build in Canada Innovation Program (BCIP); ▪ the Defence Research Innovation for Defence Excellence and Security (IDEaS); ▪ The National Research Council Canada Industrial Research Assistance Program (IRAP); ▪ Canadian Centre for Cyber Security (CCCS); ▪ Innovative Solutions Canada; or ▪ A Canadian Post-Secondary Institution.
M3	Security / Corporate	The Respondent must provide the following information as well as any other requested information related to the ownership and control of the Respondent, its owners, its management and any related* (see definition below) entities. 1. An organization chart for the Respondent showing all related entities; 2. A list of all the Respondent's shareholders and/or partners, as applicable; if the Respondent is a subsidiary, this information must be provided for each parent corporation or partnership, up to the ultimate owner(s); and 3. A list of the Respondent's Directors and officers. If the Respondent is a subsidiary, this information must be provided for each parent corporation or partnership, up to the ultimate owner(s).