INVITATION À SE QUALIFIER

Annexe A

Phase 1 : Exigences en matière d'évaluation

Mécanisme d'approvisionnement en matière de cybersécurité (MACS)

Annexe A – Phase 1 : Exigences en matière d'évaluation

1.0 Introduction

Pour obtenir une description complète du processus d'IQ, phase 1 – Processus d'évaluation des critères obligatoires, veuillez consulter la section 4.2 du présent document d'IQ.

2.0 Évaluation des exigences obligatoires

Dans le cadre de la phase 1 – Exigences d'évaluation, les répondants doivent justifier, dans une réponse écrite, leur conformité aux exigences obligatoires suivantes :

Tableau 1		
ID du critère obligatoire	**Sous-catégorie**	**Exigence**
O1	Technique	Le répondant doit avoir élaboré, déployé, mis en œuvre ou certifié au moins une (1) solution de cybersécurité (ou un produit) qui respecte au moins un (1) des services ou fonctions de sécurité suivants* : ** Aux fins d'évaluation pour O1, les services et fonctions de sécurité sont les éléments numérotés (p. ex., 1. Prévention de la perte de données) et non les puces au-dessous de ceux-ci.* 1. Prévention de la perte de données (PPD) ▪ Étiquetage/balisage des données ▪ Application de la PPD aux points d'extrémité ▪ Application de la PPD aux réseaux ▪ Gestion des droits relatifs à l'information 2. Chiffrement ▪ Chiffrement des fichiers ▪ Chiffrement du disque complet ▪ Chiffrement des supports amovibles ▪ Modules de sécurité du matériel ▪ Chiffrement de couche d'application ▪ Chiffrement de base de données ▪ Chiffrement de courriel 3. Science des données ▪ Modélisation/prétraitement

Tableau 1		
ID du critère obligatoire	**Sous-catégorie**	**Exigence**
		▪ Nettoyage 4. Gestion de clés ▪ Outils de gestion de clés d'entreprise ▪ Modules de sécurité du matériel (MSM) 5. Prévention des maliciels ▪ Antimaliciels de courriels ▪ Antipourriels de courriels ▪ Anti-maliciels d'hôtes ▪ Système de prévention des intrusions au niveau des hôtes (SPIH) 6. Détection et intervention ▪ Détection et intervention au niveau des points d'extrémité (DIP) 7. Protection ▪ Virtualisation/confinement des applications ▪ Établissement d'une liste blanche des applications ▪ Surveillance de l'intégrité des fichiers ▪ Pare-feu d'hôtes ▪ Contrôle des ports et des dispositifs 8. Authentification ▪ Authentification, autorisation et audit (AAA) ▪ Horodatage ▪ Signature de code et de document ▪ Authentification multifacteur ▪ Authentification unique/fédération 9. Gestion des justificatifs d'identité ▪ Certificats d'entités autres que des personnes ▪ Justificatifs d'identité d'une entité « personne » au niveau d'assurance 1 à 4 ▪ Gestion du cycle de vie des certificats/automatisation ▪ Identité en tant que service

Tableau 1		
ID du critère obligatoire	**Sous-catégorie**	**Exigence**
		▪ Infrastructure de clés publique ▪ Gestion de secrets 10. Répertoires ▪ Gestion des accès ▪ Audit du changement ▪ Répertoire d'entreprise et magasins d'identité ▪ Gouvernance et administration de l'identité ▪ Gestion des accès privilégiés <u>11. Nuage/CD</u> ▪ Courtiers en sécurité d'accès au nuage ▪ Services de sécurité infonuagiques <u>12. Réseau/Périmètre</u> ▪ Contrôles d'accès au réseau (AD, RPV, GUM) ▪ Puisard ▪ Filtrage de contenu ▪ Diode de données ▪ Appareils interdomaine ▪ Serveur mandataire de sortie/serveur mandataire inverse ▪ Passerelle Web sécurisée ▪ Relais de courriel SMTP ▪ Réputation des adresses URL <u>13. Détection et prévention dans les réseaux</u> ▪ Déni de service distribué (DDos) et déni de service (DoS) : nuage ▪ DDos et DoS : hébergé par SPC ▪ Système de détection et de prévention des intrusions (SDPI) ▪ Antivirus interne sur le réseau ▪ Bac à sable <u>14. Service de journalisation centralisé (SJC)</u> ▪ Collecte centralisée des journaux ▪ Stockage centralisé des journaux

Tableau 1		
ID du critère obligatoire	**Sous-catégorie**	**Exigence**
		16. Connaissance des infrastructures ▪ Découverte des infrastructures ▪ Analyse des réseaux et comportements ▪ Conformité aux politiques (automatisation des outils) ▪ Outil de visualisation (tableau de bord) 17. Alimentations en renseignements sur les menaces (ARM) 18. Gestion de la configuration de la sécurité ▪ Découverte de biens ▪ Automatisation de la configuration ▪ BDGC de sécurité des infrastructures 19. Orchestration et automatisation de la sécurité et intervention (OASI) ▪ Automatisation du confinement ▪ Confinement des incidents ▪ Automatisation des plans de match ▪ Automatisation des rapports 20. Gestion des vulnérabilités ▪ Balayages des SE et applications ▪ Évaluation des vulnérabilités 21. Identité numérique (services liés à l'identité) ▪ Confirmation de l'identité ▪ Vérification de l'identité 22. Communications sécurisées ▪ Vidéoconférences sécurisées ▪ Audioconférences sécurisées ▪ Messagerie instantanée sécurisée ▪ Gestion à distance sécurisée
O2	Organisationnel	Le répondant doit avoir accumulé au moins **6 M$** en recettes liées aux activités facturables durant les 3 années précédant la date d'affichage de l'IQ;

Tableau 1		
ID du critère obligatoire	**Sous-catégorie**	**Exigence**
		– OU – Le répondant doit avoir un produit offert dans le commerce et lié à la fonction ou au service de sécurité qu'il a indiqué en O1, avec au moins 5 clients payeurs actuels; **– OU –** Le répondant doit avoir reçu une subvention ou signé un contrat lié à l'innovation en cybersécurité dans le cadre d'un des éléments ou avec une des entités ci-dessous : ▪ Programme d'innovation Construire au Canada (PICC); ▪ Programme d'innovation pour la défense, l'excellence et la sécurité (IDEeS) de Recherche pour la défense; ▪ Programme d'aide à la recherche industrielle (PARI) du Conseil national de recherches du Canada; ▪ Centre canadien pour la cybersécurité (CCC); ▪ Solutions innovatrices Canada; ▪ Établissement canadien d'enseignement postsecondaire.
O3	Sécurité/Services ministériels	Le répondant doit fournir les informations suivantes, ainsi que toute autre information demandée concernant la propriété et le contrôle du répondant, de ses propriétaires, de sa direction et de toute autre entité liée* (voir la définition ci-dessous). 1. Un organigramme du répondant indiquant toutes les entités liées; 2. Une liste de tous les actionnaires et/ou partenaires du répondant, le cas échéant. Si le répondant est une filiale, cette information doit être fournie pour chaque société mère (personne morale ou société de personnes), et ce, jusqu'au premier propriétaire; 3. Une liste des directeurs et agents du répondant. Si le répondant est une filiale, cette information doit être fournie

Tableau 1		
ID du critère obligatoire	**Sous-catégorie**	**Exigence**
		pour chaque société mère (personne morale ou société de personnes), et ce, jusqu'au premier propriétaire.