National Defence
Défense nationale

CONTRACT DATA REQUIREMENTS LIST
LISTE DES DONNÉES ESSENTIELLES DU CONTRAT

A. Système/ÉLÉMENT Fonctionnement et entretien du Système d'alerte du Nord				**N^{O} DE CONTRAT/DE DEMANDE DE SOUMISSIONS** Contrat n^{o}		
C. IDENTIFICATEUR DE L'EDT EDT 3.10.4		**D. CATÉGORIES DES DONNÉES** Soutien opérationnel		**E. ENTREPRENEUR**		
1. NUMÉRO DE L'ÉLÉMENT **LDEC 3.10.4**		**2. TITRE OU DESCRIPTION DES DONNÉES** **Définition de la portée en matière de sécurité**		**3. SOUS-TITRE**		
4. AUTORITÉ (numéro de données) **DED 3.10.4**		**5. RÉFÉRENCE AU CONTRAT** Paragraphe 3.10.4 de l'EDT		**6. BUREAU DEMANDEUR** Ordonnance du Système d'alerte du Nord (OSAN)		
7. INSPECTION	**9. DONNÉES D'ENTRÉE**	**10. FRÉQUENCE** UNE/R	**12. DATE DE SOUMISSION INITIALE** 1 YACA	**14. DISTRIBUTION ET DESTINATAIRES** AT OSAN 1/1		
				A. DESTI-NATAIRE	B. COPIES	
8. CODE APP		**11. EN DATE DU** 1er avril	**13. DATE DE LA SOUMISSION** Voir la case 16	DPEAG (SR et C)	ÉBAUCHE	VERSION FINALE Rapport / régulier

16. REMARQUES

16.1 Le rapport initial de définition de la portée en matière de sécurité doit être présenté un an après l'attribution du contrat.

16.2 La définition de la portée en matière de sécurité doit être mise à jour après tout changement de grande importance ou changement de profil de risque.

16.3 Documents pertinents :

a. Banque de terminologie de la défense du MDN – On s'attend à ce qu'il soit utilisé conformément à la DOAD 6004-0, Terminologie de la défense, publiée le 1er février 2019.
b. Processus d'assurance de la cybermission basé sur les risques (Analyse de la criticité de la mission et évaluation des actifs, évaluation des risques, développement de la sécurité, glossaire des termes relatifs à l'assurance de la cybermission).
c. Contrôles critiques 29+9 du MDN/des FAC.

16.4 Spécification des exigences techniques :

a. Assurance de la mission cybernétique
   i. L'assurance de la mission cybernétique (AMC) est un sous-élément de l'assurance de la mission et concerne la capacité d'une organisation, d'un service, d'une infrastructure, d'une plateforme, d'un système d'armes ou d'un équipement à fonctionner dans un cyberespace contesté et à accomplir sa mission.
   ii. L'AMC vise à ce qu'on puisse accomplir la mission avec succès malgré les risques d'attaques cybernétiques. Pour ce faire, on suit un processus de gestion de la mission axé sur les risques. Le processus d'assurance de

AT OSAN		1	1
AC		1	
AUTRES			

la mission cybernétique basé sur les risques permet de déterminer les éléments critiques de la mission et leurs liens avec les systèmes et le cyberdomaine, d'évaluer les risques et d'orienter les décisions en matière de cybersécurité pour qu'on puisse faire preuve de résilience lors d'une cyberattaque. La résilience est la capacité d'éviter les cyberattaques, d'y résister ou de s'en remettre (voir les documents techniques applicables de GPEA énumérés ci-dessus). iii. L'Entrepreneur mettra en œuvre des exigences en matière de sécurité qui touchent la prévention, la détection, l'intervention et le rétablissement afin de maintenir l'AMC tout au long du cycle de vie du Système d'alerte du Nord. iv. Les exigences fonctionnelles en matière de sécurité doivent être affinées en fonction des risques en utilisant les directives du rapport d'évaluation des risques dans le cadre du PAMCR, rapport sur le développement de la sécurité. En outre, les Ordonnances et directives de sécurité de la Défense nationale (ODSDN) et la DOAD 2006-0 Sécurité de la défense, doivent être appliquées à la mise en œuvre de la protection des biens. v. L'Entrepreneur respectera les énoncés de criticité de la mission déterminés dans le cadre du processus d'analyse de criticité de la mission et d'évaluation des biens lié au PAMCR.						
PRÉPARÉ PAR SR et C 5-6		DATE ÀD	APPROUVÉ PAR Paul Mondoux				
17. DOSSIER DU CONTRAT NUMÉRO DU DOCUMENT	**18. NOMBRE ESTIMATIF DE PAGES**		**19. COÛT ESTIMATIF**	**15. TOTAL**		2	1