	National Defence Défense nationale		Retour à la liste des DED

DATA ITEM DESCRIPTION – DESCRIPTION DE DONNÉES

1. TITLE – TITRE	**2. IDENTIFICATION NUMBER – NUMÉRO D'IDENTIFICATION**
DÉFINITION DE LA PORTÉE EN MATIÈRE DE SÉCURITÉ	**DED 3.10.4**

3. DESCRIPTION / PURPOSE – DESCRIPTION / OBJET

Le but de la définition de la portée en matière de sécurité est de fournir une description des biens, y compris leurs surfaces d'attaque et vecteurs d'attaque pour le système d'armes. Le processus comprend la définition du périmètre de sécurité global et de l'environnement à la fois au niveau de la plateforme (capacité de soutien des armes) et au niveau du système.
Le présent document est utilisé comme intrant pour l'évaluation des risques pour la sécurité, LDEC 3.10.5.

4. APPROVAL DATE DATE D'APPROBATION	**5. OFFICE OF PRIMARY INTEREST (OPI) BUREAU DE PREMIÈRE RESPONSABILITÉ (BPR)**	**6. GIDEP APPLICABLE APPLICABLE AU GIDEP**
ÀD	Autorité technique (AT) de l'OSAN	S.O.

7. APPLICATION / INTERRELATIONSHIP – APPLICATION / INTERDÉPENDANCE

Consulter la LDEC 3.10.4 et le paragraphe 3.10.1 de l'EDT.
Cette DED énonce les instructions relatives au format et au contenu des données produites dans le contexte des tâches énoncées à l'EDT pour le fonctionnement et l'entretien du Système d'alerte du Nord.

8. ORIGINATOR - AUTEUR	**9. APPLICABLE FORMS – FORMULES PERTINENTES**
AT OSAN	AUCUNE.

10. PREPARATION INSTRUCTIONS – INSTRUCTIONS SUR LA PRÉSENTATION DES DONNÉES

10.1 Document source

10.1.1 EDT de F et E du SAN section 3, paragraphe 3.10.4.
10.1.2 Processus d'assurance de la cybermission basé sur les risques.
10.1.3 NIST 800-160 v1 Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems
10.1.4 NIST 800-160 v2 Developing Cyber Resilient Systems: A Systems Security Engineering Approach

10.2 Contenu et format

10.2.1 La définition de la portée en matière de sécurité doit être préparée et livrée selon le format utilisé par L'Entrepreneur.

10.2.2. La définition de la portée en matière de sécurité doit être documentée à l'aide des objectifs précisés dans le volume 1 du document NIST 800-160 et élargie en utilisant les lignes directrices et les méthodes précisées dans le volume 2 du document NIST 800-160 pour la cybersécurité ou d'autres normes acceptables pour le Canada. Au minimum, les éléments suivants doivent être détaillés en utilisant les lignes directrices :

a. Identification des biens.
b. Périmètre de sécurité.
c. Environnement de sécurité et confiance en la sécurité.
d. Gestion des changements dans l'environnement de sécurité.

10.2.3. En outre, la définition de la portée en matière de sécurité doit documenter ce qui suit à l'aide des lignes directrices du PAMCR pour l'assurance des missions cybernétiques ou d'autres normes acceptables pour le Canada :

a. Identification des biens qui nécessitent une évaluation des risques. Les biens peuvent être décrits de façon imbriquée, des installations aux plateformes, en passant par les systèmes et leurs composants. Au minimum, deux niveaux de biens sont proposés, soit au niveau de la plateforme et au niveau du système.
b. Description des biens, y compris leur surface d'attaque et leur environnement de sécurité. Les cinq classes de surface d'attaque (logique, détection et rayonnement électromagnétique, personnel, physique et indirect) sont accompagnées de mesures de sécurité correspondantes. Au niveau du système, cela devrait inclure une description de ses fonctions, de ses caractéristiques matérielles (p. ex. processeurs, jeux de puces et mémoire, fonctions de sécurité telles que la résistance à la falsification physique, la détection de falsification/intrusion, la réduction à zéro, le cryptoprocesseur, etc.) et des fonctionnalités logicielles, y compris les cas d'utilisation, les systèmes d'exploitation, y compris l'information de configuration (utilisateurs, droits et privilèges, modes, etc.), les applications et services, les bases de données et les mesures de sécurité, y compris les mesures techniques (p. ex. les autorisations d'accès aux répertoires/fichiers) et opérationnelles (p. ex. politique sur les médias portables).
c. Hypothèses de confiance à l'égard des entités et biens externes.
d. Identification des vecteurs d'attaque. L'identification des vecteurs d'attaque doit inclure une description du bien en question, de son interface, des entités en interaction, des mesures de sécurité prises par les entités en interaction et la nature de l'interaction (autorisée ou non).

10.2.4. La catégorisation de sécurité de la portée en matière de sécurité livrable doit être effectuée lors de la création du document, car la définition de la portée en matière de sécurité, ou certaines de ses parties, pourraient être protégées. L'étiquetage et le marquage de sécurité, ainsi que la manipulation, l'entreposage et la transmission de la définition de la portée en matière de sécurité doivent être mis en œuvre conformément aux Ordonnances et directives de sécurité de la Défense nationale (ODSDN). Outre le marquage de sécurité, qui est placé dans l'en-tête et le pied de page de chaque page, un ensemble d'énoncés informatifs sera imprimé sur la couverture, ou la première page du document et, dans certains cas, également sur la page verso (au verso de la page de titre ou de la couverture) selon les besoins.

10.2.5. Il incombera à L'Entrepreneur de mener la gestion des changements, tel que décrit ci-dessous :

a. La définition de la portée en matière de sécurité doit comprendre une section sommaire de l'historique des modifications, qui renferme ce qui suit :
   i. Un identifiant clair et unique de la version/révision pour chaque soumission ou nouvelle soumission de la définition de la portée en matière de sécurité.
   ii. Une identification claire des révisions ou des modifications apportées au document par rapport à sa soumission précédente.
   iii. Le bien-fondé des révisions et des modifications.
b. Toutes les révisions/modifications mentionnées ci-dessus doivent être clairement définies dans le document à l'aide de la fonction de suivi des modifications appropriée du logiciel de traitement de texte utilisé pour produire le document, par exemple, fonction de « Suivi des modifications » dans Microsoft-Word®, barres latérales, etc.

Page 2 de 2
Décembre 2020