	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**
PLAN DE GESTION DE LA SÉCURITÉ DU SYSTÈME	**DED 3.10.2**

3. DESCRIPTION / PURPOSE – DESCRIPTION / OBJET

Le plan de gestion de la sécurité du système a pour objet d'exposer et de définir le programme de gestion de la sécurité du système de L'Entrepreneur qui sera utilisé pour assurer la protection du système contre les menaces à la cybersécurité pendant l'élaboration du système et pour la mise en service (fonctionnement et entretien, réparation et révision). Le plan vise à déterminer la portée et le contenu des activités de sûreté qui s'appliquent au niveau des systèmes d'armes, des aéronefs et du système, et à inclure les moyens de démontrer la conformité aux exigences de navigabilité liées aux préoccupations en matière de sûreté et à l'assurance de la mission cybernétique.

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 3.10.2 et le paragraphe 3.10.2 de l'EDT.
Cette DED énonce les instructions relatives au format et au contenu des données produites dans le contexte des tâches énoncées dans 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 3.10.2.
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
10.1.5 U.S. National Institute of Standards (NIST) SP 800-37 Rev.2, Risk Management Framework for Information Systems and Organizations

10.2 Contenu et format

10.2.1 Le plan de gestion de la sécurité du système doit être préparé selon le format de L'Entrepreneur.

10.2.2. Il doit documenter ce qui suit :

a. Documents applicables : Liste des documents qui s'appliquent à titre de directives ou d'orientations pendant l'exécution du plan de gestion de la sécurité du système. La liste doit inclure les exigences légales, réglementaires et les autres exigences contractuelles pertinentes publiées qui sont applicables au système en cours d'élaboration. Les exigences et les objectifs en matière de sécurité du système sont tirés de ces documents.
b. But : Énoncé des objectifs de l'ingénierie de la sécurité du système et des principes qui seront appliqués.

c. Organisation : Décrit le placement organisationnel et la dotation de l'organisation de gestion de l'ingénierie de sécurité de L'Entrepreneur. Des graphiques et des diagrammes peuvent être utilisés pour montrer les relations organisationnelles et fonctionnelles.

d. Programme de gestion de l'ingénierie de la sécurité du système : Description des activités prévues si l'on veut atteindre les objectifs du programme d'ingénierie de la sécurité du système. L'utilisation de graphiques ou de diagrammes est encouragée pour illustrer les interfaces fonctionnelles du programme, les exigences en matière d'ingénierie et de conception, les jalons des activités, le processus de gestion et les niveaux d'effort pour chaque phase du programme.

e. Flux de données du programme : Illustration de la façon dont les données de base du programme circulent, indiquant comment l'organisation d'ingénierie de la sécurité du système surveillera tous les efforts du programme et alimentera le processus décisionnel; démontrer que les processus d'ingénierie des systèmes et d'ingénierie de la sécurité du système sont entièrement intégrés pour s'assurer que les interdépendances sont établies et gérées.

f. Examen de la classification des Travaux de cybersécurité : Description de la méthodologie utilisée pour s'assurer que seul le personnel dûment autorisé, conformément à la Liste de vérification des exigences en matière de sécurité du présent contrat, Travaille sur la cybersécurité. Veuillez noter que l'exigence d'une autorisation appropriée du personnel s'applique également aux personnes qui effectuent les essais de cybersécurité et rédigent des rapports, ainsi qu'au personnel contractuel ou administratif qui traite la livraison des essais et des rapports. Une description des moyens utilisés pour protéger toute information classifiée résultant du Travail de cybersécurité. La classification de la LDEC de cybersécurité et la sécurité de l'agrégation des données doivent être traitées.

g. Fonctions d'ingénierie de la sécurité du système : Description des principales fonctions et tâches précises à exécuter comme l'exige l'énoncé de Travail, y compris les suivantes :

   i. Description de la façon dont les règlements de sécurité et les autres lignes directrices du programme seront définis et synthétisés en un ensemble d'exigences et d'objectifs en matière de sécurité.

   ii. Intégration des fonctions de sécurité au processus d'ingénierie du système : Description du processus par lequel les intrants de sécurité seront appliqués à la conception fonctionnelle du système, à l'attribution des exigences, aux études de compromis et aux processus de spécification de conception des communications, de l'électronique et de l'interface (CEI).

   iii. Synthèse et évaluation des systèmes de sécurité : Description de la méthode par laquelle le matériel, les logiciels, les installations et les procédures du système de sécurité seront synthétisés et évalués. Cela comprend les essais de cybersécurité utilisés pour valider l'assurance de la mission cybernétique telle que décrite dans le document CS-007 pour la surveillance continue.

   iv. Contrôle de la configuration : Description de la façon dont les efforts d'ingénierie de la sécurité du système seront intégrés aux activités de contrôle de la configuration du système. Une explication de la façon dont les changements proposés au système auront une incidence sur les efforts de sécurité doit être incluse.

   v. Relations avec d'autres entrepreneurs Aperçu des méthodes par lesquelles les efforts d'ingénierie de la sécurité du système des entrepreneurs, sous-traitants et fournisseurs associés seront intégrés dans l'ensemble du Programme d'ingénierie de la sécurité du système.

   vi. Installation du système : Description de la façon dont les efforts d'ingénierie de la sécurité du système et de sécurité industrielle et des produits seront coordonnés pour s'assurer qu'aucune vulnérabilité de sécurité n'est créée pendant l'installation du système.

   vii. Sécurité du produit : Description de la façon dont les principaux composants et produits du système seront sécurisés aux usines d'assemblage de L'Entrepreneur. Identification de la main-d'œuvre, des installations, de l'équipement et des procédures de sécurité à utiliser. L'interface de sécurité avec les entrepreneurs, les sous-traitants et les fournisseurs associés doit être incluse.

   viii. Documentation du dossier du Système informatisé des achats et des contrats (SIAC)/chaîne d'approvisionnement, identifiant pour tous les éléments du SIAC :

      1. Plan de gestion de la sécurité des éléments du SIAC.
      2. Source des éléments du SIAC.
      3. Procédures de livraison et de mise à jour.
      4. Justification de la sélection.
      5. Examens de sécurité du SIAC/chaîne d'approvisionnement.

   ix. Documentation du processus d'assurance de la sécurité, y compris :

      1. Description des méthodes à utiliser pour effectuer l'analyse de criticité de la mission et l'évaluation des biens (ACMEB) et définition de la portée de la sécurité.
      2. Planification de l'évaluation des risques en matière de sécurité.
      3. Plan de définition des spécifications, de la conception et de la mise en œuvre des fonctions de sécurité, y compris l'élaboration du plan des principes de base de la cybersécurité.

4. Plan pour déterminer les exigences en matière d'essais de sécurité, les méthodes d'essai et les critères d'essai.

5. Description des méthodes utilisées pour produire la matrice de traçabilité des exigences de sécurité et le plan d'actions et les jalons.

6. Plan pour élaborer le plan de surveillance continue et le plan d'intervention en cas d'incident.

x. Fourniture de considérations supplémentaires pour toute contrainte légale ou réglementaire concernant les fonctions de sécurité (p. ex. cryptage), TEMPEST (y compris SANS ARRÊT et DÉTOURNEMENT, le cas échéant), l'ingénierie ROUGE/NOIRE et la découverte de vulnérabilités.

xi. Fourniture de considérations de sécurité supplémentaires requises lors de la transition vers le soutien en service.

h. Poursuite des processus de sécurité du système : Description de la façon dont le programme de sécurité du système, ses fonctions et les livrables engendrés seront gérés et mis à jour après l'acceptation et tout au long du cycle de vie du système d'armes.

10.2.3. La catégorisation de sécurité du plan de gestion de la sécurité du système livrable doit être effectuée lors de la création du document, car le plan de gestion de la sécurité du système ou certaines de ses parties pourraient être protégés. L'étiquetage et le marquage de sécurité, ainsi que la manipulation, l'entreposage et la transmission du plan de gestion de la sécurité du système 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.

10.2.4. Le plan de gestion de la sécurité du système comprend un programme de gestion du cycle de vie pour les applications logicielles et les systèmes d'exploitation afin de s'assurer qu'ils restent pris en charge et exempts de vulnérabilités connues. Les vulnérabilités connues sont celles répertoriées dans la base de données MITRE portant sur les vulnérabilités et expositions communes.

10.2.5. Le plan de gestion de la sécurité du système comprend : une autorité d'accès et un plan de sécurité des données qui comprennent au minimum les mesures de contrôle d'accès et de sécurité des données suivantes :

a. Restriction de l'accès physique aux serveurs.
b. Restriction des droits administratifs d'accès au système d'exploitation (S/O) à un minimum de personnel.
c. Établissement d'une politique et de contrôle de mot de passe.
d. Maintien d'une liste de contrôle d'accès pour protéger chaque objet, y compris, sans s'y limiter, les menus, les fichiers et les tableaux.
e. Attribution et contrôle des privilèges d'objet et de système par utilisateur.
f. Contrôle de la création de nouveaux comptes.
g. Vérification logicielle pour enregistrer les connexions et les transactions de l'utilisateur concernant des objets critiques.
h. Maintien d'une capacité de détection des virus et de protection contre les virus.
i. Détection et isolement des utilisateurs du système non autorisés, qu'il s'agisse d'une menace extérieure ou d'une tentative de sabotage interne.
j. Empêchement de l'exécution de logiciels malveillants et de programmes non approuvés.
k. Validation régulière (au moins une fois par mois) du fait que chaque système est corrigé et à jour, dans une configuration sécurisée, et que les vulnérabilités connues sont atténuées.

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

a. Le Plan de gestion de la sécurité du système 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 du plan de gestion de la sécurité du système.
   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 3 de 3
Décembre 2020