



CENTRE GOUVERNEMENTAL
DE CYBERDÉFENSE

SA-400(06)

Protection des données en cours d'utilisation

Juill. 2026



Acquisition sécurisée des systèmes/services

System and Services

SA-400(06) – Protection des données en cours d'utilisation (Pb--)

Énoncés :

Éviter que les données soient utilisées dans des territoires qui relèvent d'autres compétences juridiques.

Responsable : Aucun

Discussion :

Permettre aux données en cours d'utilisation de résider dans d'autres juridictions fournit une occasion de contraindre les données. Le fait de traiter les données dans des juridictions canadiennes uniquement élimine plusieurs capacités de contrainte. Aucune méthode de chiffrement n'a encore été approuvée pour protéger les données en cours d'utilisation. En principe, une forme de chiffrement connue sous le nom de « chiffrement homomorphique » pourrait permettre certains types de traitement alors que les données restent chiffrées, mais le Centre pour la cybersécurité ne considère pas pour l'instant que le chiffrement homomorphique est suffisant pour assurer le chiffrement conformément à son document Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B (ITSP.40.111). Par conséquent, si le chiffrement homomorphique est employé pour protéger les données en cours d'utilisation, il convient actuellement de l'évaluer en tant que texte en clair (c'est-à-dire n'offrant aucune protection cryptographique selon le contrôle SC-13). Il n'y a aucun délai minimum après lequel les données sont considérées en cours d'utilisation. Leur présence dans un système pour un seul cycle d'UCT devrait suffire pour l'imposition d'une contrainte.