



IT Security Bulletin

Bulletin de sécurité TI

April 2008

ITSB-51

Avril 2008

Secure Communications Interoperability Protocol (SCIP) Device Testing

Purpose

The purpose of this bulletin is to recommend that Government of Canada (GC) departments and agencies conduct secure communication testing (i.e. establishment of secure communications) of their Secure Communications Interoperability Protocol (SCIP) devices.

Background

Communications Security Establishment Canada (CSEC) recommends that GC departments and agencies conduct testing of their SCIP devices to increase operational readiness.

The purpose of these tests is to minimize secure communications downtime and interruptions which could impact GC department's and agency's capacity to conduct business.

Test sur les dispositifs compatibles avec le protocole d'interopérabilité des communications sécurisées (SCIP)

Objet

Ce bulletin a pour objet de recommander aux ministères et aux organismes du gouvernement du Canada de tester (c.-à-d. établir des communications sécurisées) leurs dispositifs compatibles avec le protocole d'interopérabilité des communications sécurisées (dispositifs SCIP).

Contexte

Le Centre de la sécurité des télécommunications Canada (CSTC) recommande aux ministères et aux organismes du GC de tester leurs dispositifs SCIP pour améliorer leur état de préparation opérationnelle.

Ces tests ont pour objet de minimiser le temps d'arrêt et les interruptions des communications sécurisées, qui pourraient avoir une incidence négative sur la capacité opérationnelle des ministères et des organismes du GC.

Recommendations

CSEC provides the following recommendations:

1. Testing should be conducted on a regular basis, at a minimum, every three months;
2. Testing should be conducted with priority clients;
3. Testing should be conducted when CSEC approved software is installed in the SCIP devices;
4. Testing should be conducted when new key material is filled into a SCIP device; and
5. Testing should be conducted when SCIP devices are relocated and when power interruptions occur.

Testing Procedures

CSEC recommends the following tests be conducted on a regular basis:

1. Establish a secure call with priority clients;
2. Test secure fax capability with priority clients (refer to ITSA-46 for secure fax guidance).

Recommandations

Le CSTC recommande d'effectuer les tests :

1. de façon régulière, au moins tous les trois mois;
2. en collaborant avec les clients prioritaires;
3. lorsqu'un logiciel approuvé par le CSTC est installé sur les dispositifs SCIP;
4. lorsqu'on charge du nouveau matériel de chiffrement dans un dispositif SCIP;
5. lorsqu'un dispositif SCIP est relocalisé et lorsque des pannes d'électricité se produisent.

Procédures de test

Le CSTC recommande d'effectuer les tests suivants de façon régulière :

1. Établir une communication sécurisée avec les clients prioritaires;
2. Tester la fonction de télécopie sécurisée avec les clients prioritaires (voir l'ITSA-46 pour des conseils sur la télécopie sécurisée).

Contacts and Assistance

GC departments and agencies that experience problems as a result of the testing should contact the Crypto Material Assistance Centre (CMAC).

CMAC
PO Box 9703, Terminal
Ottawa, Ontario K1G 3Z4
Telephone: (613) 991-8600
E-mail: cmac@cse-cst.gc.ca

Personnes-ressources et aide

Les ministères et les organismes qui rencontrent des problèmes à la suite des tests devraient communiquer avec le Centre d'assistance en matière de matériel cryptographique (CAMC).

CAMC
C.P. 9703, Terminus
Ottawa, Ontario K1G 3Z4
Téléphone : 613-991-8600
Courriel : cmac@cse-cst.gc.ca

La directrice de la Gestion de la mission de la Sécurité des TI,

Gwen Beauchemin
Director, IT Security Mission Management