



Royal
Canadian
Mounted
Police

Gendarmerie
royale
du
Canada

1200 Vanier Parkway
Ottawa, Ontario
K1A 0R2

1200, promenade Vanier
Ottawa (Ontario)
K1A 0R2

CSE / CST
Chief's Office / Bureau du chef
09-01509
JUL 06 2009
File / Dossier _____

SECRET

July 3rd, 2009

John Adams
Chief
Communications Security Establishment Canada
719 Heron Road
Ottawa, ON
K1G 3Z4

Dear Mr. Adams:

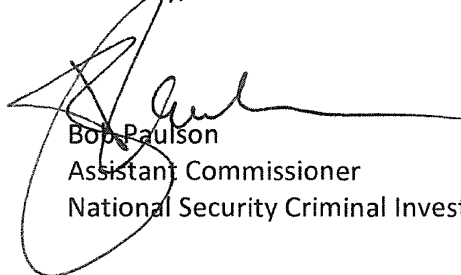
RE: Signing of CSEC-RCMP Memorandum of Understanding (MoU)

Please find attached a signed copy of the MoU between the Royal Mounted Canadian Police and the Communications Security Establishment Canada. The MoU in both English and French has been duly signed.

The enclosed copies are for your records.

I look forward to continuing our partnership between our organizations.

Sincerely,



Bob Paulson
Assistant Commissioner
National Security Criminal Investigations

Canada

SECRET

MEMORANDUM OF UNDERSTANDING
BETWEEN
THE COMMUNICATIONS SECURITY ESTABLISHMENT
AND
THE ROYAL CANADIAN MOUNTED POLICE

Collectively referred to as the “Participants”

1. PURPOSE

- 1.1 This Memorandum of Understanding (MoU) between the Communications Security Establishment (CSE) and the Royal Canadian Mounted Police (RCMP) establishes a framework under which the two organizations will enhance cooperation on intelligence-sharing and provision of services, in accordance with their respective legal authorities. All other arrangements, including Memoranda of Understanding, between CSE and the RCMP pursuant to this MOU will be considered annexes and set out in a list at Annex A.
- 1.2 CSE is mandated to provide foreign intelligence in accordance with the Government of Canada intelligence priorities, to help protect electronic information and information systems of importance to the Government of Canada and to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties. CSE is the National Authority for SIGINT and COMSEC. As well, it has responsibilities in conducting, analysing and responding to sophisticated computer network operations and in the provision of information technology security advice, guidance and services.
- 1.3 The RCMP is Canada’s national police service, mandated to preserve the peace, uphold the law and provide quality service in partnership with communities. It has responsibilities in the areas of law enforcement, criminal and national security criminal investigations and international peace operations. Within the Government of Canada, the RCMP provides advice, guidance and training related to physical security.

2. BACKGROUND

- 2.1 To remain effective in the face of complex security threats and rapidly changing technology, Canada's security and intelligence community seeks to improve the results of its activities, including enhanced cooperation and appropriate information sharing among its members. Accordingly, the RCMP and CSE have already enjoyed a number of important successes based on close technical and operational cooperation as well as intelligence sharing. Yet, both organizations recognize that challenges remain.
- 2.2 RCMP investigations, including national security criminal investigations, may ultimately result in criminal proceedings where the Crown is obligated to disclose to the accused all relevant information in its possession or control that would allow the accused to make full answer and defence. Should the evidentiary chain include intelligence or other sensitive information, Canada and its allies' critical intelligence targets, sources and methods could be compromised. To address this issue and achieve an acceptable balance between the use and protection of sensitive or potentially injurious information, the Government of Canada is currently considering this issue on a community-wide basis. Once the way forward has been clarified, CSE and the RCMP may be better positioned to address a broader range of foreign intelligence-sharing scenarios.
- 2.3 To ensure continued progress in areas where there is greater certainty, CSE and the RCMP have established a list of priority activities for enhanced cooperation relating to intelligence-sharing and provision of services. A list of Priority Activities for Enhanced Cooperation is appended at Annex B to this MoU. Until such a time as an updated SIGINT-handling MOU is in place, the Participants agree to continue to follow, in so far as possible, existing day-to-day practices with regard to the provision and use of SIGINT.

3. COOPERATION PRINCIPLES

- 3.1 CSE and the RCMP will cooperate to the greatest extent practicable to address threats to Canada's national security and public safety without compromising intelligence assets, sources or methods, and will do so in a manner that reflects the participants' legal authorities and obligations and recognizes the rights of Canadians and others.
 - 3.1.1 Sections 3.2 to 3.8 apply subject to 3.1.
- 3.2 CSE and the RCMP acknowledge that the former's sharing of foreign intelligence with the RCMP may include information on terrorism, [REDACTED]
[REDACTED]
- 3.3 CSE and the RCMP, subject to broader Government of Canada intelligence priorities and initiatives, intend to continue to develop principles and mechanisms to facilitate the

SECRET

sharing of foreign intelligence and manage the risk of its potential use in criminal investigations.

- 3.4 CSE and the RCMP intend to continue to develop principles and mechanisms to facilitate the sharing of information related to information technology security and computer network defence.
- 3.5 CSE and the RCMP intend to continue to develop principles and mechanisms to facilitate the provision of technical and operational support and assistance.
- 3.6 CSE and the RCMP intend to monitor the performance and results of this MoU by conducting a senior-level review biennially, or more frequently if required.
- 3.7 CSE and the RCMP intend that all Protected and Classified information exchanged or generated between Participants in connection with this MOU must be safeguarded through the creation, maintenance, release, transmittal, transportation, declassification, handling, use, storage and disposal in accordance with the guidelines outlined in the Government of Canada, Government Security Policy (GSP), and all RCMP and CSE Security policies.
- 3.8 CSE and the RCMP recognize that the respective heads of their organizations – Chief, CSE and Commissioner, RCMP – are accountable for the outcomes of this MoU.

4. ADMINISTRATION AND MANAGEMENT:

- 4.1 A Joint Senior Management Team (JSMT) with representation from both agencies, will be comprised of:

For CSE: Director General, SIGINT Programs
 Director General, IT Security Strategic Management
 Director General, Policy and Communications
 Director, Corporate and Operational Policy

For RCMP: Director General, National Security Criminal Operations
 Director General, RCMP Criminal Intelligence Program
 Director General, International Policing
 Director, Strategic Services Branch, Technical Operations

- 4.2 The JSMT will meet on a biannual basis, or more frequently if necessary, to review and modify or confirm priority activities identified in Annex B.
- 4.3 Director General, Policy and Communications, CSE, and Director General, National Security Criminal Operations, RCMP, will co-ordinate meetings of the JSMT and will

report to the JSMT on progress and outstanding issues, providing recommendations as necessary.

5. REPRESENTATION

- 5.1 CSE and the RCMP will designate Director General Policy and Communications, CSE, and Director General National Security Criminal Operations, RCMP, to ensure regular and ongoing engagement on matters relating to this MOU. These representatives may establish working groups to provide recommendations on specific issues relating to the priority activities for enhanced cooperation.

6. DISPUTE RESOLUTION PROCESS

- 6.1 Any dispute arising from the interpretation or operation of this MOU shall be referred to the JSMT for resolution.

7. FINANCIAL AND ADMINISTRATIVE ARRANGEMENTS

- 7.1 CSE and the RCMP will be responsible for ensuring that financial authorities and authorizations are identified and confirmed prior to undertaking any cooperative arrangements having financial implications.
- 7.2 CSE and the RCMP will be responsible for any costs incurred to meet their respective administrative obligations contained within this MOU, including:
- maintaining secure office facilities, including the acquisition of approved security containers, telecommunications equipment, electronic equipment, room and building design; and
 - ensuring that all personnel seeking access to either Participant's information have an appropriate security clearance and indoctrination level.

8. CONFIDENTIALITY AND USE OF INFORMATION

CSE and the RCMP intend to:

- 8.1 Use the information provided by the other Participant solely for the purpose for which it was provided.
- 8.2 Not disseminate the information to any third party without the prior written consent of the supplying Participant, except as required by law in which case prior notice must be provided where possible to the supplying Participant.

- 8.3 Limit access to the information to those of its employees whose duties require such access, who are legally bound to keep confidences and who have the appropriate security clearance.

9. INFORMATION MANAGEMENT

- 9.1 The information disclosed under this arrangement shall be administered and maintained, and disposed of in accordance with the law that applies to record retention and personal information and all applicable policies and guidelines. This includes the *Privacy Act*, the *National Archives of Canada Act* and *Government Security Policy*.

Each Participant will:

- 9.2 Promptly notify the other of any unauthorized use or disclosure of the information exchanged under this arrangement and furnish the other Participant with details of such unauthorized use or disclosure. In the event of such an occurrence, the Participant responsible for the safeguarding of the information shall take all reasonably necessary steps to limit the damage of the incident and prevent a re-occurrence. Upon request by either Participant, an investigation must take place.
- 9.3 Upon recognition that unauthorized use or disclosure has occurred and/or upon the request of the other participant, immediately return any such information and ensure that no copies or extracts are retained.
- 9.4 Immediately notify the other if either receives a request under the *Privacy Act*, the *Access to Information Act* or other lawful authority, for information provided under this arrangement. If requested, the Participant shall endeavour to protect the information from disclosure to the extent permitted by law.

10. ACCURACY OF INFORMATION

CSE and the RCMP will:

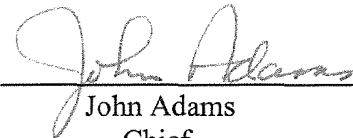
- 10.1 Use their best efforts to verify accuracy and completeness of the information to the other Participant.
- 10.2 Promptly notify the other Participant if it learns that inaccurate or potentially unreliable information may have been provided or received.

11. EFFECTIVE DATE/ AMENDMENT/ TERMINATION

11.1 This MOU:

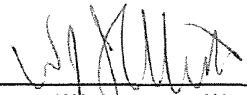
- a) will come into force upon the signature of both Participants, the effective date being the date of the second signature;
- b) upon coming into force immediately replaces any previous Memoranda of Understanding between the Participants, except those cited in Annex A;
- c) will be reviewed as required by the Participants to ensure that it remains current with regard to the agreed principles and expectations;
- d) may be amended at any time by written agreement of both Participants; and
- e) may be terminated at any time by written notification of either Participant. Termination does not release a Participant from any obligations which accrued while the arrangement was in force and the obligations of confidentiality shall survive the expiry or termination of this agreement.

Signed by the authorized officers of the Participants:



John Adams
Chief
Communications Security Establishment

Date: 11 June 2009



William J.S. Elliott
Commissioner
Royal Canadian Mounted Police

Date: Jun 23/09

SECRET

ANNEX A

The following arrangements are annexes to this MOU:

1. RCMP (EDP security) and CSE (COMSEC)'s Respective Roles under the Government of Canada Security Policy, signed 1989-10-31
2. Provision of Criminal Record Names Check Information to CSE, signed 1994-03-01
3. CSE Provision of Advice, Guidance and SPA Services Pursuant to s. 273.64 (1)(b), NDA, signed 2008-01-25

Last updated 2009-05-05

SECRET

ANNEX B

PRIORITY ACTIVITIES FOR ENHANCED COOPERATION

1. Completion of a SIGINT-handling MOU within 12 months of signature of this MOU
2. [REDACTED]
3. IRRELEVANT
4. Information Technology Security support (cyber defence and computer network operations, enterprise security architecture)
5. Support to CSE non-attributable activities
6. Foreign intelligence support (in particular, to support [REDACTED])
7. Lessons learned from recent investigations

PROTOCOLE D'ENTENTE
ENTRE
LE CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS
ET
LA GENDARMERIE ROYALE DU CANADA

appelés collectivement les « Participants »

1. BUT

- 1.1 Le présent protocole d'entente (PE) conclu entre le Centre de la sécurité des télécommunications (CST) et la Gendarmerie royale du Canada (GRC) vise à établir un cadre en vertu duquel les deux organisations pourront favoriser la coopération pour l'échange de renseignements et la prestation de services, conformément à leur mandat respectif. Toute autre entente, y compris des protocoles d'ententes, conclue entre le CST et la GRC aux termes du présent PE, sera considérée comme une annexe et sera inscrite à l'annexe A.
- 1.2 Le CST a pour mandat de fournir du renseignement étranger en conformité avec les priorités du gouvernement du Canada en la matière, d'aider à protéger l'information électronique et les systèmes d'information d'importance pour le gouvernement du Canada, et de fournir une assistance technique et opérationnelle aux organismes fédéraux chargés de l'application de la loi et de la sécurité dans l'exercice des fonctions que la loi leur confère. Le CST est l'autorité nationale pour le renseignement électromagnétique (SIGINT) et la sécurité des communications (COMSEC). De plus, il est chargé d'effectuer et d'analyser des opérations sophistiquées liées aux réseaux informatiques, et d'y donner suite, et de fournir des conseils et des services touchant la sécurité des technologies de l'information.
- 1.3 La GRC est le service de police nationale du Canada, avec pour mandat de préserver la paix, d'appliquer la loi et de fournir des services de qualité en partenariat avec les collectivités. Elle assume des responsabilités dans les domaines de l'exécution de la loi et des enquêtes criminelles, notamment celles concernant la sécurité nationale, ainsi que dans le domaine des opérations internationales de maintien de la paix. Au sein du gouvernement du Canada, la GRC fournit des conseils et de la formation sur la sécurité matérielle.

2. CONTEXTE

- 2.1 Pour rester efficace dans le contexte de menaces complexes pour la sécurité et d'une technologie qui évolue rapidement, la collectivité canadienne du renseignement et de la sécurité cherche à améliorer les résultats de ses activités, notamment en rehaussant la coopération et la mise en commun de l'information pertinente entre ses membres. De fait, la GRC et le CST ont déjà obtenu des succès très probants grâce à une étroite coopération technique et opérationnelle ainsi qu'à l'échange de renseignements. Cela dit, les deux organisations reconnaissent que des défis subsistent.
- 2.2 Les enquêtes de la GRC, notamment les enquêtes criminelles relatives à la sécurité nationale, peuvent en définitive entraîner des procédures criminelles où la Couronne se verra obligée de divulguer à l'accusé toute l'information pertinente en sa possession ou sous son contrôle, pour permettre à l'accusé d'élaborer une réponse et une défense complètes. Si la chaîne de la preuve devait comporter du renseignement ou de l'information sensible, les cibles, les sources et les méthodes de renseignement essentielles du Canada et de ses alliés pourraient s'en trouver compromises. Pour résoudre ce problème et atteindre un équilibre raisonnable entre l'utilisation et la protection de l'information sensible ou éventuellement préjudiciable, le gouvernement du Canada envisage actuellement d'examiner la question à l'échelle de la collectivité. Une fois qu'on aura défini l'orientation à prendre, le CST et la GRC seront mieux en mesure d'examiner un éventail élargi de modalités d'échange de renseignements étrangers.
- 2.3 Afin de favoriser les avancées dans les domaines les plus sûrs, le CST et la GRC ont établi une liste d'activités prioritaires pour une coopération accrue en matière d'échange de renseignements et de prestation de services. Une liste d'activités prioritaires pour une coopération améliorée figure donc à l'annexe B du présent PE. D'ici à la conclusion d'un protocole d'entente actualisé sur le traitement du SIGINT, les Participants conviennent de continuer à exercer, dans la mesure du possible, les pratiques quotidiennes existantes pour la production et l'utilisation du SIGINT.

3. PRINCIPES DE COOPÉRATION

- 3.1 Le CST et la GRC entendent coopérer dans la mesure du possible afin de résoudre les menaces qui planent sur la sécurité nationale et la sécurité publique sans compromettre les renseignements, de même que les sources et les méthodes de renseignement, et ce, de façon à refléter les pouvoirs et les obligations juridiques des Participants, et en reconnaissant les droits des Canadiens et des autres.
- 3.1.1 L'application des articles 3.2 à 3.8 est assujettie à l'application de l'article 3.1.
- 3.2 Le CST et la GRC reconnaissent que le renseignement étranger que le CST pourra partager avec la GRC peut inclure de l'information sur le terrorisme, [REDACTED]
- [REDACTED]

- 3.3 Le CST et la GRC, sous réserve des priorités et des initiatives plus vastes du gouvernement du Canada en matière de renseignement, entendent continuer d'élaborer des principes et des mécanismes afin de faciliter l'échange de renseignement étranger et de gérer le risque de son utilisation éventuelle dans des enquêtes criminelles.
- 3.4 Le CST et la GRC entendent continuer d'élaborer des principes et des mécanismes afin de faciliter l'échange d'information liée à la sécurité des technologies de l'information et à la protection des réseaux informatiques.
- 3.5 Le CST et la GRC entendent continuer d'élaborer des principes et des mécanismes afin de faciliter la prestation d'un soutien et d'une assistance techniques et opérationnels.
- 3.6 Le CST et la GRC entendent surveiller le rendement et les résultats du présent PE en effectuant un examen bisannuel au niveau de la gestion supérieure, ou plus fréquemment, au besoin.
- 3.7 Le CST et la GRC entendent faire en sorte que toute l'information protégée ou classifiée échangée ou produite entre les Participants en rapport avec le présent PE soit protégée selon les modalités de création, de conservation, de diffusion, de transmission, de transport, de déclassification, de manipulation, d'utilisation, d'archivage et d'élimination en conformité avec les lignes directrices établies par le gouvernement du Canada et dans la Politique du gouvernement sur la sécurité (PGS), ainsi qu'avec les politiques sur la sécurité de la GRC et du CST.
- 3.8 Le CST et la GRC reconnaissent que leurs dirigeants respectifs – le chef du CST et le commissaire de la GRC – sont responsables des résultats du présent PE.

4. ADMINISTRATION ET GESTION :

- 4.1 Une équipe mixte de gestion supérieure (EMGS), dotée de représentants des deux organisations, comptera :
- Pour le CST : Le directeur général, Programmes SIGINT
Le directeur général, Gestion stratégique de la Sécurité des TI
Le directeur général, Politiques et communications
Le directeur, Politiques centrales et opérationnelles
- Pour la GRC: Le directeur général, Opérations criminelles relatives à la sécurité nationale
Le directeur général, Programme des renseignements criminels de la GRC
Le directeur général, de la Police internationale
Le directeur, des Services stratégiques, Opérations techniques
- 4.2 L'EMGS se réunira deux fois par année, ou plus fréquemment au besoin, pour examiner et modifier ou confirmer les activités prioritaires établies à l'annexe B.
- 4.3 Le directeur général, Politiques et communications, au CST, et le directeur général des Opérations criminelles relatives à la sécurité nationale, à la GRC, coordonneront les

réunions de l'EMGS et feront rapport à l'EMGS sur les progrès réalisés et les questions en suspens, et feront des recommandations au besoin.

5. REPRÉSENTATION

- 5.1 Le CST et la GRC désignent le directeur général, Politiques et communications (CST), et le directeur général des Opérations criminelles relatives à la sécurité nationale (GRC) comme responsables d'assurer une mobilisation périodique et suivie concernant toute question découlant du présent PE. Ces représentants peuvent établir des groupes de travail chargés de fournir des recommandations sur des questions particulières touchant les activités prioritaires pour favoriser la coopération.

6. RÉSOLUTION DES CONFLITS

- 6.1 Tout conflit découlant de l'interprétation ou de l'exécution du présent PE doit être soumis à l'EMGS en vue de son règlement.

7. DISPOSITIONS FINANCIÈRES ET ADMINISTRATIVES

- 7.1 Le CST et la GRC sont tenus de faire en sorte que les autorisations et les pouvoirs financiers soient déterminés et confirmés avant d'entreprendre toute entente de coopération ayant des conséquences financières.
- 7.2 Le CST et la GRC sont responsables de tous les coûts engagés pour s'acquitter de leurs obligations administratives respectives prévues dans le présent PE, notamment :
- entretenir des installations sécurisées, y compris l'acquisition de contenants de sécurité approuvés, le matériel de télécommunication et l'équipement électronique, et la conception d'immeubles et de locaux;
 - faire en sorte que tous les membres du personnel cherchant à obtenir accès à l'information de l'un ou l'autre des Participants au PE, aient l'habilitation de sécurité et le niveau d'endoctrinement satisfaisants.

8. CONFIDENTIALITÉ ET UTILISATION DES RENSEIGNEMENTS

Chaque Participant entend :

- 8.1 utiliser l'information fournie par l'autre Participant exclusivement aux fins prévues;
- 8.2 refuser de communiquer l'information à des tiers sans le consentement écrit préalable du Participant qui a fourni l'information, sauf lorsqu'il est tenu de la communiquer par la loi, auquel cas il faudra, dans la mesure du possible, donner un préavis au Participant qui a fourni l'information;
- 8.3 restreindre l'accès à l'information aux employés dont les fonctions exigent pareil accès, qui sont tenus légalement de respecter la confidentialité et qui détiennent l'habilitation de sécurité pertinente.

9. GESTION DE L'INFORMATION

- 9.1 L'information communiquée en vertu du présent PE doit être administrée, tenue et éliminée conformément à la loi qui s'applique à la conservation des dossiers et aux renseignements personnels et à toutes les politiques et lignes directrices applicables. Cela englobe la *Loi sur la protection des renseignements personnels*, la *Loi sur les archives nationales du Canada* et la *Politique du gouvernement sur la sécurité*.

Chaque Participant :

- 9.2 informera rapidement l'autre Participant de toute utilisation ou communication non autorisée de l'information échangée en vertu du présent PE et fournira à l'autre Participant des précisions sur pareille utilisation ou communication non autorisée. En pareille éventualité, le Participant responsable de la protection de l'information devra prendre toutes les mesures nécessaires pour limiter les préjudices causés par l'incident et pour empêcher que la situation ne se reproduise. À la demande de l'un ou l'autre Participant, on devra mener une enquête;
- 9.3 une fois reconnu qu'il y a eu utilisation ou communication non autorisée de l'information, ou à la demande de l'autre Participant, retournera l'information en question et veillera à ce qu'aucune copie ni aucun extrait ne soient conservés;
- 9.4 informera immédiatement l'autre Participant s'il a été saisi d'une demande fondée sur la *Loi sur la protection des renseignements personnels*, la *Loi sur l'accès à l'information* ou autre disposition législative, pour obtenir la communication d'une information fournie en vertu du présent PE. Si on lui en fait la demande, le Participant devra protéger l'information contre toute communication, dans la mesure permise par la loi.

10. EXACTITUDE DE L'INFORMATION

Chaque Participant :

- 10.1 s'efforcera de veiller à ce que l'information fournie à l'autre Participant soit exacte et complète;
- 10.2 informera rapidement l'autre Participant s'il apprend qu'une information inexacte ou susceptible de ne pas être fiable pourrait avoir été fournie ou reçue.

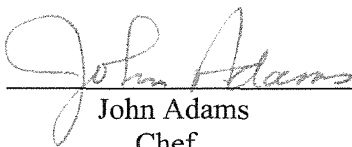
11. ENTRÉE EN VIGUEUR, MODIFICATION ET RÉSILIATION

11.1 Le présent PE :

- a) entre vigueur à la date de sa signature par les Participants, à compter de la date où le second Participant appose sa signature;

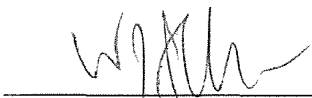
- b) à son entrée en vigueur, remplace immédiatement tout précédent protocole d'entente conclu entre les participants, à l'exception de ceux cités à l'annexe A;
- c) sera examiné au besoin par les Participants afin de veiller à ce qu'il demeure actuel en ce qui a trait aux attentes et aux principes convenus;
- d) peut être modifié en tout temps avec le consentement écrit des Participants;
- e) peut être résilié en tout temps moyennant un avis écrit d'un des Participants. La résiliation ne dégage pas un Participant de toute obligation contractée pendant la période d'application du PE et les obligations de confidentialité demeurent applicables après l'expiration ou la résiliation du présent PE.

Signé par les représentants autorisés des Participants :


John Adams
Chef

Centre de la sécurité des télécommunications

Date : 11 June 2009


William J.S. Elliott
Commissaire
Gendarmerie royale du Canada

Date : 23 11 June / 09
wa

ANNEXE A

Les ententes ci-dessous constituent une annexe au présent PE :

1. Les rôles respectifs de la GRC (sécurité informatique) et du CST (COMSEC) en vertu de la *Politique du gouvernement sur la sécurité*; entente signée le 1989-10-31
2. Prestation au CST de données issues de la vérification de noms dans les casiers judiciaires; entente signée le 1994-03-01
3. Prestation par le CST de conseils, de lignes directrices et de services d'évaluation de la posture de sécurité, conformément à l'alinéa 273.64(1) b) de la *Loi sur la Défense nationale*; entente signée le 2008-01-25

Dernière révision 2009-05-05

ANNEXE B

ACTIVITÉS PRIORITAIRES POUR FAVORISER LA COOPÉRATION

1. Élaboration d'un PE concernant le traitement du renseignement électromagnétique (SIGINT) dans les 12 mois suivant la signature du présent PE.
2. [REDACTED]
3. IRRELEVANT
[REDACTED]
4. Soutien à la sécurité des technologies de l'information (opérations liées à la cyberdéfense et aux réseaux informatiques, architecture de sécurité d'entreprise).
5. Soutien aux activités anonymes du CST.
6. Soutien au renseignement étranger (en particulier, pour soutenir [REDACTED]
[REDACTED])
7. Leçons tirées d'enquêtes récentes.