



**CANADA**

TREATY SERIES **2026/16** RECUEIL DES TRAITÉS

---

**REPUBLIC OF KOREA / DEFENCE**

Agreement between the Government of Canada and the Government of the  
Republic of Korea on the Protection of Military and Defence Classified Information

Done at Ottawa on 25 February 2026

In Force on 12 June 2026

---

**RÉPUBLIQUE DE CORÉE / DÉFENSE**

Accord entre le Gouvernement du Canada et le Gouvernement de la  
République de Corée sur la protection des informations classifiées militaires et de défense

Fait à Ottawa le 25 février 2026

En vigueur le 12 juin 2026

---

© His Majesty the King in Right of Canada, as represented  
by the Minister of Foreign Affairs, 2026

The Canada Treaty Series is published by  
the Treaty Law Division  
of the Department of Foreign Affairs,  
Trade and Development  
[www.treaty-accord.gc.ca](http://www.treaty-accord.gc.ca)

Catalogue No: FR4-2026/16-PDF  
ISBN: 978-0-662-43234-0

© Sa Majesté le roi du chef du Canada, représenté par le  
ministre des Affaires étrangères, 2026

Le Recueil des traités du Canada est publié par  
la Direction du droit des traités  
du ministère des Affaires étrangères,  
du Commerce et du Développement  
[www.treaty-accord.gc.ca](http://www.treaty-accord.gc.ca)

N° de catalogue : FR4-2026/16-PDF  
ISBN : 978-0-662-43234-0



**CANADA**

TREATY SERIES **2026/16** RECUEIL DES TRAITÉS

---

**REPUBLIC OF KOREA / DEFENCE**

Agreement between the Government of Canada and the Government of the  
Republic of Korea on the Protection of Military and Defence Classified Information

Done at Ottawa on 25 February 2026

In Force on 12 June 2026

---

**RÉPUBLIQUE DE CORÉE / DÉFENSE**

Accord entre le Gouvernement du Canada et le Gouvernement de la  
République de Corée sur la protection des informations classifiées militaires et de défense

Fait à Ottawa le 25 février 2026

En vigueur le 12 juin 2026

---

**AGREEMENT  
BETWEEN  
THE GOVERNMENT OF CANADA  
AND  
THE GOVERNMENT OF THE REPUBLIC OF KOREA  
ON THE PROTECTION OF MILITARY  
AND DEFENCE CLASSIFIED INFORMATION**

**THE GOVERNMENT OF CANADA AND THE GOVERNMENT OF THE REPUBLIC OF KOREA** (hereinafter referred to as the “Parties”),

**WISHING** to ensure the protection of classified information that is provided or disclosed between the Parties in the context of defence and defence industrial security, and

**ACKNOWLEDGING** that this Agreement supersedes and replaces the Agreement between the Government of Canada and the Government of the Republic of Korea on the Exchange and Protection of Classified Military Information done at Ottawa on July 5, 1999,

**HAVE AGREED** as follows:

**ARTICLE 1**

**Definitions**

In this Agreement:

- (a) “classified contract” means a legally binding instrument that requires a contractor to access the classified information of a Party to provide a good or service. This term includes a sub-contract or a pre-contractual activity;
- (b) “classified information” means any military or defence information that is assigned a security classification level by a Party, and which requires protection against unauthorized disclosure, access, or destruction in the interest of national security and in accordance with that Party’s national laws and regulations. This information may be in oral, visual, electronic, magnetic, or documentary form, or in the form of material, equipment, or technology, and includes reproductions, translations, and material in the process of development. A reference to classified information in this Agreement also includes Canadian protected information, unless otherwise specified;

**ACCORD**  
**ENTRE**  
**LE GOUVERNEMENT DU CANADA**  
**ET**  
**LE GOUVERNEMENT DE LA RÉPUBLIQUE DE CORÉE**  
**SUR LA PROTECTION DES INFORMATIONS**  
**CLASSIFIÉES MILITAIRES ET DE DÉFENSE**

**LE GOUVERNEMENT DU CANADA ET LE GOUVERNEMENT DE LA RÉPUBLIQUE DE CORÉE** (ci-après dénommés les « Parties »),

**SOUHAITANT** assurer la protection des informations classifiées fournies ou communiquées par une Partie à l'autre dans le contexte de défense et de sécurité industrielle de défense,

**RECONNAISSANT** que le présent accord met fin à l'Accord entre le Gouvernement du Canada et le Gouvernement de la République de Corée sur l'échange et la protection des renseignements militaires classifiés, fait à Ottawa le 5 juillet 1999, et le remplace

**SONT CONVENUS** de ce qui suit :

**ARTICLE PREMIER**

**Définitions**

Aux fins du présent accord :

- a) « contrat classifié » désigne un instrument juridiquement contraignant en vertu duquel un contractant doit avoir accès à des informations classifiées d'une Partie pour fournir un produit ou un service. Ce terme désigne également les contrats de sous-traitance et les activités préalables à l'attribution d'un contrat;
- b) « information classifiée » désigne toutes les informations militaires ou de défense auxquelles l'une ou l'autre Partie a attribué un niveau de classification de sécurité et qui requièrent une protection contre la divulgation, l'accès ou la destruction non autorisés dans l'intérêt de la sécurité nationale et conformément aux lois et règlements nationaux de cette Partie. Ces informations peuvent se présenter sous forme orale, visuelle, électronique, magnétique ou documentaire, ou sous forme de matériel, d'équipement ou de technologie, et elles comprennent les reproductions, les traductions et le matériel en cours de développement. Toute mention d'informations classifiées dans le présent accord vise également les informations protégées du Canada, sauf indication contraire;

- (c) “competent authorities” (CAs) means governmental organizations which are designated by a Party as the authorities responsible, within their respective competence under that Party’s national laws and regulations, for the handling of classified information;
- (d) “compromise” means the unauthorized access to, disclosure or provision of, destruction, removal, modification, or use of classified information;
- (e) “contractor” means an individual or a legal entity that has the legal capacity to enter into a classified contract. This term includes a sub-contractor;
- (f) “facility security clearance” (FSC) means a determination by a Party, through its security authority (SA), that a contractor meets the security requirements to handle classified information within a specified facility in accordance with the national laws and regulations of that Party;
- (g) “need-to-know” means that access to classified information is limited to authorized individuals who need to have access to that classified information in order to perform their official duties;
- (h) “originating Party” means the Party which provides classified information to the receiving Party;
- (i) “personnel security clearance” (PSC) means a determination by a Party that an individual is eligible to access classified information in accordance with the national laws and regulations of that Party;
- (j) “Program/Project Security Instruction” (PSI) means a compilation of security regulations and procedures based on national security policy and supporting directives which are applied to a specific program or project in order to standardize security procedures;
- (k) “receiving Party” means the Party which receives classified information provided by the originating Party; and
- (l) “security authority” (SA) means a governmental organization designated by a Party to administer the implementation of this Agreement.

- c) « autorités compétentes » (AC) désigne les organisations gouvernementales désignées par une Partie comme autorités responsables, dans les limites de leurs compétences respectives en vertu des lois et des règlements nationaux, du traitement des informations classifiées;
- d) « compromission » désigne l'accès non autorisé à des informations classifiées, ou la divulgation, la fourniture, la destruction, la suppression, la modification ou l'utilisation non autorisées de ces informations;
- e) « contractant » désigne une personne physique ou morale ayant la capacité juridique de conclure un contrat classifié. Ce terme désigne également un sous-traitant;
- f) « habilitation de sécurité d'installation » (HSI) désigne la décision d'une Partie, prononcée par l'autorité de sécurité (AS) de cette dernière, établissant qu'un contractant satisfait aux exigences de sécurité requises pour traiter des informations classifiées à l'intérieur d'une installation déterminée conformément aux lois et règlements nationaux de cette Partie;
- g) « besoin d'en connaître » désigne le principe selon lequel l'accès aux informations classifiées est limité aux personnes autorisées à y avoir accès qui ont besoin de connaître ces informations pour s'acquitter de leurs fonctions officielles;
- h) « Partie d'origine » désigne la Partie qui fournit des informations classifiées à la Partie destinataire;
- i) « habilitation de sécurité du personnel » (HSP) désigne la décision d'une Partie établissant qu'une personne peut avoir accès à des informations classifiées conformément aux lois et règlements nationaux de cette Partie;
- j) « instructions de sécurité d'un programme/projet » (ISP) désigne un recueil de règlements et de procédures en matière de sécurité établi à partir de la politique de sécurité nationale et des directives connexes, qui sont appliqués à un programme ou à un projet particulier afin d'uniformiser les procédures de sécurité;
- k) « Partie destinataire » désigne la Partie qui reçoit des informations classifiées fournies par la Partie d'origine;
- l) « autorité de sécurité » (AS) désigne une organisation gouvernementale désignée par une Partie pour administrer la mise en œuvre du présent accord.

## **ARTICLE 2**

### **Objective and Scope**

1. This Agreement sets out the standards and procedures for the protection of classified information that is provided or disclosed, in a defence industrial security or defence context, by one Party to the other Party, or by one Party to a contractor located in the territory of the other Party, or by a contractor located in the territory of one Party to a contractor located in the territory of the other Party.
2. This Agreement cannot be construed to compel a Party to provide or disclose classified information.

## **ARTICLE 3**

### **Security Authorities**

1. The Parties designate the following as their respective SAs:
  - (a) for the Government of the Republic of Korea:  
Intelligence Planning Directorate,  
Korean Defense Intelligence Agency,  
Ministry of National Defense,
  - (b) for the Government of Canada:  
International Industrial Security Directorate,  
Industrial Security Sector,  
Department of Public Works and Government Services,  
(also known as Public Services and Procurement Canada),or their respective successors. The Parties shall inform each other through diplomatic channels of any subsequent changes to their SAs.
2. The Parties shall notify each other of their CAs for this Agreement.

## **ARTICLE 4**

### **Security Classification Levels**

1. The originating Party shall assign a security classification level to classified information and shall mark the classified information according to its national laws and regulations.
2. The receiving Party, in accordance with its national laws and regulations, may mark classified information that is provided or disclosed by the originating Party with a security classification level that is at least equivalent to the security classification level assigned by the originating Party, in accordance with Table 1 and Table 2 in this Article.



## **ARTICLE 2**

### **Objectif et portée**

1. Le présent accord énonce les normes et les procédures régissant la protection des informations classifiées qui sont fournies ou communiquées, dans un contexte de défense ou de sécurité industrielle de défense, par une Partie à l'autre Partie, ou par une Partie à un contractant situé sur le territoire de l'autre Partie, ou encore par un contractant situé sur le territoire d'une Partie à un contractant situé sur le territoire de l'autre Partie.
2. Le présent accord ne peut être interprété comme obligeant une Partie à fournir ou à communiquer des informations classifiées.

## **ARTICLE 3**

### **Autorités de sécurité**

1. Les autorités suivantes sont désignées comme AS respectives des Parties :
  - a) pour le Gouvernement de la République de Corée :  
Direction de la planification du renseignement  
Bureau coréen du renseignement de défense  
Ministère de la Défense nationale
  - b) pour le Gouvernement du Canada :  
Direction de la sécurité industrielle internationale  
Secteur de la sécurité industrielle  
Ministère des Travaux publics et des Services gouvernementaux  
(aussi connu sous le nom de Services publics et Approvisionnement Canada)

ou leurs successeurs respectifs. Les Parties se notifient mutuellement, par la voie diplomatique, de tout changement concernant leurs AS.
2. Les Parties se notifient mutuellement les noms des AC au titre du présent accord.

## **ARTICLE 4**

### **Niveaux de classification de sécurité**

1. La Partie d'origine attribue un niveau de classification de sécurité aux informations classifiées et y appose les marques de classification de sécurité requis en vertu de ses lois et règlements nationaux.
2. La Partie destinataire, conformément à ses lois et règlements nationaux, peut apposer sur les informations classifiées fournies ou communiquées par la Partie d'origine des marques correspondant à un niveau de classification de sécurité qui équivaut, au minimum, au niveau de classification de sécurité attribué par la Partie d'origine, conformément aux tableaux 1 et 2 du présent article.

3. The receiving Party shall protect the classified information of the originating Party at the equivalent security classification level identified in Table 1:

**Table 1: Classified Information**

| <b>In the Republic of Korea<br/>(Korean)</b> | <b>In Canada<br/>(English)</b> | <b>In Canada<br/>(French)</b> |
|----------------------------------------------|--------------------------------|-------------------------------|
| 군사I급비밀                                       | TOP SECRET                     | TRÈS SECRET                   |
| 군사II급비밀                                      | SECRET                         | SECRET                        |
| 군사III급비밀                                     | CONFIDENTIAL                   | CONFIDENTIEL                  |

4. The Republic of Korea shall protect Canadian protected information at the security classification level identified in Table 2:

**Table 2: Canadian Protected Information**

| <b>In the Republic of Korea<br/>(Korean)</b> | <b>In Canada<br/>(English)</b> | <b>In Canada<br/>(French)</b> |
|----------------------------------------------|--------------------------------|-------------------------------|
| 군사I급비밀                                       | PROTECTED C                    | PROTÉGÉ C                     |
| 군사II급비밀                                      | PROTECTED B                    | PROTÉGÉ B                     |
| 군사III급비밀                                     | PROTECTED A                    | PROTÉGÉ A                     |

3. La Partie destinataire protège les informations classifiées de la Partie d'origine selon le niveau de classification de sécurité équivalent indiqué dans le tableau 1 :

**Tableau 1 : Informations classifiées**

| <b>En République de Corée<br/>(coréen)</b> | <b>Au Canada<br/>(anglais)</b> | <b>Au Canada<br/>(français)</b> |
|--------------------------------------------|--------------------------------|---------------------------------|
| 군사I급비밀                                     | TOP SECRET                     | TRÈS SECRET                     |
| 군사II급비밀                                    | SECRET                         | SECRET                          |
| 군사III급비밀                                   | CONFIDENTIAL                   | CONFIDENTIEL                    |

4. La République de Corée protège les informations protégées du Canada selon le niveau de classification de sécurité indiqué dans le tableau 2 :

**Tableau 2 : Informations protégées du Canada**

| <b>En République de Corée<br/>(coréen)</b> | <b>Au Canada<br/>(anglais)</b> | <b>Au Canada<br/>(français)</b> |
|--------------------------------------------|--------------------------------|---------------------------------|
| 군사I급비밀                                     | PROTECTED C                    | PROTÉGÉ C                       |
| 군사II급비밀                                    | PROTECTED B                    | PROTÉGÉ B                       |
| 군사III급비밀                                   | PROTECTED A                    | PROTÉGÉ A                       |

## **ARTICLE 5**

### **Protection and Use of Classified Information**

1. The Parties shall protect and use classified information as follows:
  - (a) the receiving Party shall give protection that is at least equal to the protection that it gives to its own information of an equivalent security classification level;
  - (b) the receiving Party shall use classified information only for the purpose for which it is provided or disclosed unless the originating Party gives prior consent in writing to do otherwise through the Parties' respective SAs or CAs;
  - (c) the originating Party may specify, in writing, limitations on the use of classified information by the receiving Party, and the receiving Party shall comply with such limitations;
  - (d) the receiving Party shall not downgrade the security classification level of classified information or declassify classified information without the prior consent, in writing, of the originating Party through the Parties' respective SAs or CAs;
  - (e) the originating Party shall inform the receiving Party of any change in the security classification level of classified information; and
  - (f) the receiving Party shall use every available means to prevent the loss or compromise of classified information provided by the originating Party.
2. The Parties may jointly determine, in writing, additional security requirements for the protection of classified information.
3. A Party shall notify the other Party of any changes in its national laws and regulations that could affect the protection of classified information provided or disclosed under this Agreement.

## **ARTICLE 6**

### **Access to Classified Information**

The Parties shall not give an individual access to classified information based only on that individual's rank, appointment, or PSC. The Parties shall give an individual access to classified information only if that individual:

- (a) has a need-to-know;

## **ARTICLE 5**

### **Protection et utilisation des informations classifiées**

1. Les Parties protègent et utilisent les informations classifiées conformément aux dispositions suivantes :
  - a) la Partie destinataire assure une protection au moins égale à celle qu'elle accorde à ses propres informations d'un niveau de classification de sécurité équivalent;
  - b) la Partie destinataire n'utilise les informations classifiées qu'aux fins pour lesquelles celles-ci ont été fournies ou communiquées, sauf avec le consentement préalable écrit de la Partie d'origine, donné par l'entremise des AS ou des AC respectives des Parties;
  - c) la Partie d'origine peut indiquer, par écrit, que l'utilisation des informations classifiées par la Partie destinataire est soumise à des restrictions, auquel cas la Partie destinataire respecte ces restrictions;
  - d) la Partie ne peut déclasser ou déclassifier les informations classifiées sans le consentement préalable écrit de la Partie d'origine, donné par l'entremise des AS ou des AC respectives des Parties;
  - e) la Partie d'origine informe la Partie destinataire de toute modification apportée au niveau de la classification de sécurité des informations classifiées;
  - f) la Partie destinataire emploie tous les moyens à sa disposition pour empêcher la perte ou la compromission des informations classifiées fournies par la Partie d'origine.
2. Les Parties peuvent définir conjointement, par écrit, des exigences de sécurité supplémentaires applicables à la protection des informations classifiées.
3. Une Partie notifie à l'autre Partie toute modification apportée à ses lois et règlements nationaux qui est susceptible d'avoir une incidence sur la protection des informations classifiées fournies ou communiquées au titre du présent accord.

## **ARTICLE 6**

### **Accès aux informations classifiées**

Les Parties ne peuvent autoriser une personne physique à accéder à des informations classifiées uniquement en raison de son rang, d'une nomination ou d'une HSP. Les Parties ne peuvent autoriser une personne physique à accéder à des informations classifiées que si la personne, à la fois :

- a) a besoin d'en connaître;

- (b) has a PSC to the appropriate level, as required; and
- (c) is briefed on the protection of classified information in accordance with the Parties' respective national laws and regulations.

## **ARTICLE 7**

### **Transmission of Classified Information**

1. The Parties shall ensure that classified information is transmitted only by approved courier or by other means jointly approved by their respective SAs or CAs.
2. At the request of the originating Party, the receiving Party shall provide the originating Party with confirmation, in writing, that it has received classified information.
3. The Parties, through their respective SAs, shall advise contractors of the means and the packaging standards for the transmission of classified information in accordance with their national laws and regulations.
4. If classified information is too voluminous to be transmitted by approved courier, the Parties, through their respective SAs, shall jointly draft a transportation plan that describes how they intend to transmit the classified information. That plan may include the type of transport, the route, and the type of escort for the classified information.
5. The Parties shall ensure that classified information in the form of or contained in equipment is securely packaged or protected for transmission in order to prevent identification of its contents and is kept under continuous control to prevent access by unauthorized individuals.
6. The Parties may jointly authorize the transmission of classified information by protected electronic means and shall jointly determine the applicable security procedures.

## **ARTICLE 8**

### **Translation, Reproduction, and Destruction of Classified Information**

1. The Parties shall ensure that classified information is not translated or reproduced without the written consent of the originating Party given through its SA or one of its CAs.
2. The Parties shall ensure that a translation or a reproduction of classified information that is authorized by the originating Party retains the security classification level of the original classified information and is given the same protection.

- b) possède une HSP de niveau approprié, selon le cas;
- c) est informée des exigences des lois et règlements nationaux respectifs des Parties concernant la protection des informations classifiées.

## **ARTICLE 7**

### **Transmission des informations classifiées**

1. Les Parties font en sorte que les informations classifiées ne soient transmises que par un service de messagerie autorisé à cette fin, ou par tout autre moyen approuvé conjointement par leurs AS ou AC respectives.
2. À la demande de la Partie d'origine, la Partie destinataire accuse réception, par écrit, des informations classifiées.
3. Les Parties, par l'entremise de leurs AS respectives, informent les contractants des moyens de transmission et des normes d'emballage devant être utilisés pour la transmission des informations classifiées conformément à leurs lois et règlements nationaux.
4. Si les informations classifiées sont trop volumineuses pour être transmises par un service de messagerie autorisé à cette fin, les Parties, par l'entremise de leurs AS respectives, rédigent conjointement un plan de transport décrivant la manière dont elles entendent procéder à la transmission des informations classifiées. Le plan en question peut notamment préciser le moyen de transport, l'itinéraire et le type d'escorte retenus pour la transmission des informations classifiées.
5. Les Parties font en sorte que les informations classifiées qui se présentent sous forme d'équipement ou qui sont contenues dans un équipement soient emballées de manière à garantir leur sécurité ou protégées pendant leur transmission pour éviter que leur contenu ne soit visible, et qu'elles fassent l'objet d'une surveillance continue pour empêcher tout accès non autorisé.
6. Les Parties peuvent autoriser conjointement la transmission des informations classifiées par des moyens électroniques sécurisés, auquel cas elles déterminent conjointement les procédures de sécurité applicables.

## **ARTICLE 8**

### **Traduction, reproduction et destruction des informations classifiées**

1. Les Parties font en sorte que les informations classifiées ne soient pas traduites ou reproduites sans le consentement écrit de la Partie d'origine, donné par l'entremise de son AS ou de l'une de ses AC.
2. Les Parties font en sorte que toute traduction ou reproduction des informations classifiées autorisée par la Partie d'origine conserve le niveau de classification de sécurité qui leur a été attribué, et se voie accorder la même protection.

3. If the receiving Party no longer requires the classified information and the originating Party authorizes its destruction or return, or if the originating Party requests its destruction or return, the receiving Party shall destroy or return the classified information in accordance with the level of protection that the receiving Party gives to its own classified information at the equivalent security classification level.

4. If a contractor completes a classified contract or no longer needs to retain classified information, the receiving Party shall ensure that the classified information is returned to the originating Party, unless the originating Party gives specific instructions, in writing, that the contractor needs to destroy the classified information.

## **ARTICLE 9**

### **Classified Contracts**

1. The receiving Party, prior to providing or disclosing classified information to a contractor, shall ensure that:

- (a) the contractor and the facility of that contractor meet the security requirements to protect the classified information in accordance with the national laws and regulations of the receiving Party;
- (b) the facility of the contractor has a valid FSC to handle classified information;
- (c) any individual who has access to classified information has a need-to-know and a valid PSC to the appropriate level;
- (d) any individual who has access to classified information is informed of that individual's duty to protect the classified information in accordance with the national laws and regulations of the receiving Party and the provisions of this Agreement; and
- (e) the facility of the contractor is periodically inspected to determine if it continues to meet the security requirements to handle classified information.

2. The receiving Party shall ensure that a facility of a contractor that handles classified information has a facility security officer holding a valid PSC to the appropriate level to protect that classified information.



3. Si la Partie destinataire n'a plus besoin des informations classifiées et que la Partie d'origine autorise ou demande leur destruction ou leur renvoi dans le pays d'origine, la Partie destinataire détruit ou renvoie les informations classifiées conformément au niveau de protection qu'elle attribue à ses propres informations classifiées de niveau de classification de sécurité équivalent.
4. Si un contractant achève l'exécution d'un contrat classifié ou qu'il n'a plus besoin de conserver les informations classifiées, la Partie destinataire fait en sorte que les informations classifiées soient renvoyées à la Partie d'origine, à moins que cette dernière ne demande expressément, par écrit, que le contractant détruise les informations classifiées.

## **ARTICLE 9**

### **Contrats classifiés**

1. Avant de fournir ou de communiquer des informations classifiées à un contractant, la Partie destinataire fait en sorte que :
  - a) le contractant et l'installation de celui-ci satisfassent aux exigences de sécurité requises pour protéger les informations classifiées conformément aux lois et règlements nationaux de la Partie destinataire;
  - b) l'installation du contractant possède une HSI en cours de validité pour traiter des informations classifiées;
  - c) toute personne physique ayant accès aux informations classifiées ait le besoin d'en connaître et possède une HSP en cours de validité de niveau approprié;
  - d) toute personne physique ayant accès aux informations classifiées soit informée de l'obligation qui lui incombe de protéger les informations classifiées conformément aux lois et règlements nationaux de la Partie destinataire et aux dispositions du présent accord;
  - e) l'installation du contractant soit inspectée périodiquement pour vérifier si elle continue de satisfaire aux exigences de sécurité requises pour traiter des informations classifiées.
2. La Partie destinataire fait en sorte que toute installation d'un contractant qui traite des informations classifiées dispose d'un agent de sécurité d'installation qui possède une HSP en cours de validité du niveau approprié pour protéger ces informations classifiées.

## **ARTICLE 10**

### **Contract Security Clauses**

Each Party shall ensure that:

- (a) classified contracts that require access to classified information are governed by security clauses in accordance with the national laws and regulations of that Party and the provisions of this Agreement;
- (b) classified contracts include a description of the security requirements to handle classified information. The description of the security requirements shall indicate the classified information that is provided or disclosed to or generated by the contractor and the security classification level that is assigned to that classified information;
- (c) for classified contracts that are performed in the territory of the receiving Party, the SA or one of the CAs of the originating Party ensures the provision to the SA of the receiving Party a copy of the description of the security requirements; and
- (d) security clauses that govern classified contracts include at least:
  - i. a requirement that the contractor provide or disclose the classified information only to an individual who has a PSC and a need-to-know, and has had a briefing on the protection of classified information in accordance with that Party's national laws and regulations;
  - ii. the means to be used to transmit the classified information;
  - iii. the procedures to request an international visit to an industrial or a governmental facility in a Party's territory, in accordance with Article 14;
  - iv. the procedures for a Party, through its SA, to inspect a facility of a contractor located in its territory;
  - v. the procedures for a contractor to promptly notify the SA of the Party in whose territory the contractor is based on the possibility that classified information has been lost or compromised;
  - vi. a requirement that classified information provided or disclosed in the context of a classified contract only be used for the purpose of that classified contract;

## ARTICLE 10

### Clauses contractuelles relatives à la sécurité

Chaque Partie fait en sorte :

- a) que les contrats classifiés exigeant l'accès à des informations classifiées soient régis par des clauses de sécurité conformément aux lois et règlements nationaux de cette Partie et aux dispositions du présent accord;
- b) que les contrats classifiés comportent une description des exigences de sécurité requises pour traiter des informations classifiées. La description des exigences de sécurité doit préciser quelles informations classifiées sont fournies ou communiquées au contractant, ou produites par celui-ci, ainsi que le niveau de classification de sécurité attribué à ces informations classifiées;
- c) s'agissant de contrats classifiés exécutés sur le territoire de la Partie destinataire, que l'AS ou l'une des AC de la Partie d'origine s'assure de fournir à l'AS de la Partie destinataire une copie de la description des exigences de sécurité;
- d) que les clauses de sécurité régissant les contrats classifiés prévoient au minimum :
  - i. une disposition stipulant que le contractant ne peut fournir ou communiquer les informations classifiées qu'à une personne physique qui possède une HSP et a le besoin d'en connaître, et qui a été informée des exigences relatives à la protection des informations classifiées des lois et règlements nationaux de cette Partie;
  - ii. les moyens à utiliser pour transmettre les informations classifiées;
  - iii. les procédures à suivre pour demander une visite internationale d'une installation industrielle ou gouvernementale située sur le territoire d'une Partie, conformément à l'article 14;
  - iv. les procédures devant être suivies par une Partie, par l'entremise de son AS, pour inspecter une installation d'un contractant située sur son territoire;
  - v. les procédures devant être suivies par un contractant pour informer promptement l'AS de la Partie sur le territoire de laquelle il est établi de la perte ou de la compromission possible des informations classifiées;
  - vi. une disposition stipulant que les informations classifiées fournies ou communiquées au titre d'un contrat classifié ne peuvent être utilisées qu'aux fins de ce contrat;

- vii. the procedures for the final disposal of classified information;
- viii. a requirement that a contractor not provide or disclose classified information to a third country or to an individual or legal entity from a third country without the consent, in writing, of the SA of the originating Party; and
- ix. the security requirements to protect classified information.

## **ARTICLE 11**

### **Security Requirements in Contracts**

1. The Party in whose territory a classified contract is performed shall ensure that a description of the security requirements pertaining to the classified contract is provided to the SA of the Party in whose territory the contractor is based. The Parties shall provide the descriptions of the security requirements in accordance with their national laws and regulations.
2. When the Parties determine that the size or complexity of a program or project and the classified information involved require the application of additional security requirements, the SAs of the Parties shall jointly prepare a PSI and include it in the contract as an annex.

## **ARTICLE 12**

### **Security Assurances**

1. A Party, through its SA, shall take measures to ensure that a contractor located in the territory of the other Party is not awarded a classified contract or provided classified information until the SA of the other Party confirms that the contractor meets the requisite security requirements.
2. At the request of the SA of the other Party, a Party shall ensure that its SA provides a security assurance, in writing, that indicates whether a contractor has a valid PSC or FSC. This security assurance shall be provided in accordance with the national laws and regulations of that Party to whom the request was made.
3. Upon receipt by a Party of a request to provide a security assurance, that Party shall ensure that:
  - (a) if the SA of the Party to whom the request was made grants an FSC or PSC to a contractor, that SA may subsequently suspend or withdraw that FSC or PSC in accordance with its national laws and regulations. In such case, that SA shall promptly inform the SA of the other Party of that suspension or withdrawal;

- vii. les procédures relatives à l'élimination définitive des informations classifiées;
- viii. une disposition interdisant au contractant de fournir ou de communiquer des informations classifiées à un pays tiers, ou à une personne physique ou morale d'un pays tiers sans le consentement écrit de l'AS de la Partie d'origine;
- ix. les exigences de sécurité applicables à la protection des informations classifiées.

## **ARTICLE 11**

### **Exigences de sécurité stipulées dans les contrats**

1. La Partie sur le territoire de laquelle le contrat classifié est exécuté fait en sorte qu'une description des exigences de sécurité relatives à ce contrat soit fournie à l'AS de la Partie sur le territoire de laquelle est établi le contractant. Les Parties fournissent une description des exigences de sécurité conformément à leurs lois et règlements nationaux.
2. Si les Parties jugent que l'ampleur ou la complexité d'un programme ou d'un projet et les informations classifiées concernées nécessitent l'application d'exigences de sécurité supplémentaires, les AS des Parties élaborent conjointement des ISP et les annexent au contrat.

## **ARTICLE 12**

### **Garanties de sécurité**

1. Une Partie prend, par l'entremise de son AS, les mesures nécessaires pour faire en sorte qu'aucun contrat classifié ne soit attribué à un contractant situé sur le territoire de l'autre Partie, ou qu'il ne soit fourni à ce dernier aucune information classifiée, tant que l'AS de l'autre Partie n'a pas confirmé que le contractant satisfait aux exigences de sécurité requises.
2. À la demande de l'AS de l'autre Partie, une Partie fait en sorte que son AS fournisse, par écrit, une garantie de sécurité qui précise si un contractant possède une HSP ou une HSI en cours de validité. La garantie de sécurité est fournie conformément aux lois et règlements nationaux de la Partie à laquelle la demande a été adressée.
3. À la réception par une Partie d'une demande de fournir une garantie de sécurité, cette Partie fait en sorte que :
  - a) si l'AS de la Partie à laquelle la demande a été adressée délivre une HSI ou une HSP à un contractant, que l'AS en question puisse ensuite suspendre ou retirer cette HSI ou HSP conformément à ses lois et règlements nationaux. Dans ce cas, l'AS en question informe promptement l'AS de l'autre Partie de cette suspension ou de ce retrait;

- (b) if the SA of the Party to whom the request was made cannot provide a security assurance because the contractor does not have an FSC or PSC that meets the security requirements for a classified contract, that SA shall conduct a security assessment to determine if it should grant or upgrade the FSC or PSC of that contractor and if it should provide such security assurance; and
  - (c) if the SA of the Party to whom the request was made cannot promptly provide a security assurance, that SA shall promptly inform the SA of the other Party of the status of the request.
- 4. The SA of the Party that receives a request for a security assurance shall respond within five working days, unless the Parties jointly decide otherwise.
- 5. At the request of the SA of the Party that conducts a security assessment to determine if it should grant a PSC or FSC, the SA of the other Party shall assist it with that security assessment.

## **ARTICLE 13**

### **Security Evaluations and Consultations**

- 1. The Parties may jointly decide to conduct reciprocal visits to evaluate the effectiveness of the security requirements that are implemented under this Agreement. This includes the security requirements that are implemented with respect to a classified contract.
- 2. The Parties may organize meetings to discuss their respective national information security laws, regulations, and procedures relevant to this Agreement to ensure that their application of those laws, regulations, and procedures is consistent.
- 3. The Parties shall jointly determine the frequency, timing, and location of visits and meetings.

## **ARTICLE 14**

### **International Visits**

- 1. A Party shall ensure that:
  - (a) its SA or one of its CAs approves a visit by any individual who works for the other Party or for a contractor located in the territory of that other Party to an industrial or a governmental facility in its territory if the visit is authorized by the SA or one of the CAs of the other Party, if the visitor holds a valid PSC that meets the security requirements of that visit, and if the visitor has a need-to-know;

- b) si l'AS de la Partie à laquelle la demande a été adressée n'est pas en mesure de fournir une garantie de sécurité parce que le contractant ne possède pas d'HSI ou d'HSP qui satisfait aux exigences de sécurité applicables à un contrat classifié, que l'AS en question mène une évaluation de sécurité pour décider si elle devrait délivrer une HSI ou une HSP audit contractant ou relever le niveau de l'HSI ou de l'HSP dont il fait l'objet, et si elle devrait fournir une telle garantie de sécurité;
  - c) si l'AS de la Partie à laquelle la demande a été adressée n'est pas en mesure de fournir promptement la garantie de sécurité, que l'AS en question informe promptement l'AS de l'autre Partie de l'état d'avancement de la demande.
4. L'AS de la Partie qui reçoit une demande de garantie de sécurité y répond dans un délai de cinq jours ouvrables, ou dans tout autre délai déterminé conjointement par les Parties.
5. À la demande de l'AS de la Partie qui mène une évaluation de sécurité pour décider si elle devrait délivrer une HSP ou une HSI, l'AS de l'autre Partie lui apporte son concours à cette évaluation.

## **ARTICLE 13**

### **Évaluations de sécurité et consultations**

1. Les Parties peuvent décider conjointement de procéder à des visites réciproques pour évaluer l'efficacité des exigences de sécurité mises en œuvre au titre du présent accord. Celles-ci englobent les exigences de sécurité mises en œuvre en lien avec un contrat classifié.
2. Les Parties peuvent organiser des réunions pour discuter de leurs lois, réglementations et procédures nationales respectives en matière de sécurité de l'information pertinentes au regard du présent accord, afin de faire en sorte que ces lois, réglementations et procédures soient appliquées de manière cohérente.
3. Les Parties déterminent conjointement la fréquence, le calendrier et le lieu des visites et des réunions.

## **ARTICLE 14**

### **Visites internationales**

1. Une Partie fait en sorte :
  - a) que son AS ou l'une de ses AC autorise la visite d'une personne physique qui travaille pour l'autre Partie, ou pour un contractant situé sur le territoire de cette autre Partie, dans une installation industrielle ou gouvernementale située sur son territoire, si la visite est autorisée par l'AS ou l'une des AC de l'autre Partie, que le visiteur possède une HSP en cours de validité qui satisfait aux exigences de sécurité applicables à cette visite, et qu'il a le besoin de connaître;

- (b) if an individual who works for that Party or for a contractor located in the territory of that Party requests a visit to a facility handling classified information in the territory of the other Party, the individual submits that request through the SA of that first Party and complies with the security requirements of the other Party;
- (c) a request for a visit includes the visitor's given name and surname, date and place of birth, nationality, passport or identity card number, rank (if applicable), position, and PSC level, as well as the name of the organization or agency of the visitor, the purpose of the visit, the proposed date of the visit, the contact persons of the visitor, and the name of the organization and location of the facility to be visited; and
- (d) its SA or one of its CAs submits a request for a visit to the SA or one of the CAs of the other Party at least 30 working days before the visit, unless the Parties jointly decide otherwise.

2. In the context of specific classified contracts, the SA or one of the CAs of each of the Parties may jointly decide to permit recurring visits that allow specified individuals to visit specified facilities more than once without further written authorization. A recurring visit normally covers the duration of a government-approved program, project, or contract. Recurring visits covering a period of more than one year may be subject to annual review, to be jointly decided by the SA or one of the CAs of each of the Parties. The duration of a visit shall never be longer than the validity of the PSC of the visitor.

## **ARTICLE 15**

### **Third Country Restrictions**

- 1. The receiving Party shall not provide or disclose classified information to a third country or to an individual or legal entity from a third country without the prior written consent of the SA of the originating Party.
- 2. The Parties shall ensure that the contractors of their respective countries do not provide or disclose classified information to contractors from third countries without the prior written consent of both Parties' SAs.
- 3. For the purposes of this Agreement, an individual who holds a PSC or a contractor who holds an FSC issued by either Party is not considered a third party.



- b) si une personne physique travaillant pour cette Partie ou pour un contractant situé sur le territoire de cette Partie demande à visiter une installation située sur le territoire de l'autre Partie qui traite des informations classifiées, que la personne en question présente sa demande par l'entremise de l'AS de cette première Partie et qu'elle se conforme aux exigences de sécurité de l'autre Partie;
- c) qu'une demande de visite comporte le prénom et le nom de famille du visiteur, sa date et son lieu de naissance, sa nationalité, son numéro de passeport ou de carte d'identité, son grade (le cas échéant), son poste, le niveau de son HSP, ainsi que le nom de l'organisation ou de l'organisme dont il relève, l'objet de sa visite, la date de visite proposée, les personnes-ressources du visiteur et le nom de l'organisation ainsi que l'emplacement de l'installation devant faire l'objet de la visite;
- d) que son AS ou l'une de ses AC présente une demande de visite à l'AS ou à l'une des AC de l'autre Partie au moins 30 jours ouvrables avant la visite, ou dans tout autre délai déterminé conjointement par les Parties.

2. Dans le cas de contrats classifiés particuliers, l'AS ou l'une des AC d'une Partie peut décider, conjointement avec l'AS ou l'une des AC de l'autre Partie, d'autoriser certaines personnes physiques à effectuer des visites répétées dans des installations déterminées, sans autorisation écrite supplémentaire. Les visites répétées couvrent normalement toute la durée d'un programme, d'un projet ou d'un contrat approuvé par le gouvernement. Les visites répétées couvrant une période de plus d'un an peuvent faire l'objet d'un examen annuel, conformément à l'entente intervenue entre les AS des Parties ou leurs AC respectives. La durée d'une visite n'excède en aucun cas la durée de validité de l'HSP du visiteur.

## **ARTICLE 15**

### **Restrictions applicables aux pays tiers**

- 1. La Partie destinataire ne peut fournir ou communiquer des informations classifiées à un pays tiers ou à une personne physique ou morale d'un pays tiers sans le consentement écrit préalable de l'AS de la Partie d'origine.
- 2. Les Parties font en sorte que les contractants de leurs pays respectifs s'abstiennent de fournir ou de communiquer des informations classifiées à des contractants de pays tiers sans le consentement écrit préalable des AS des deux Parties.
- 3. Aux fins du présent accord, les personnes physiques qui possèdent une HSP et les contractants qui possèdent une HSI délivrées par l'une ou l'autre des Parties ne sont pas considérés comme une tierce partie.

## **ARTICLE 16**

### **Loss or Compromise**

1. If the receiving Party becomes aware of the possibility that classified information is lost or compromised, it shall immediately inform the originating Party and initiate an investigation. The receiving Party shall forward the result of the investigation to the originating Party and inform the originating Party of the measures taken to prevent a recurrence.
2. At the request of the receiving Party, the originating Party shall assist the receiving Party with its investigation.

## **ARTICLE 17**

### **Costs**

Each Party shall bear its own costs incurred to implement this Agreement.

## **ARTICLE 18**

### **Implementing Arrangements**

1. The SAs of the Parties may conclude implementing arrangements pursuant to this Agreement.
2. The CAs of the Parties, in matters within their competence, may conclude implementing arrangements which specify supplementary measures regarding the handling of classified information. These arrangements shall be subordinate to this Agreement.

## **ARTICLE 19**

### **Other Agreements or Arrangements**

This Agreement does not alter existing agreements or arrangements between the Parties, unless otherwise specified in this Agreement.

## **ARTICLE 20**

### **Dispute Settlement**

The Parties shall settle any dispute that arises with respect to the interpretation or implementation of this Agreement through mutual consultation.

## **ARTICLE 16**

### **Perte ou compromission**

1. Si la Partie destinataire prend connaissance d'une perte ou d'une compromission possible des informations classifiées, elle en informe immédiatement la Partie d'origine et ouvre une enquête. La Partie destinataire fait part du résultat de l'enquête à la Partie d'origine, et informe cette dernière des mesures prises pour empêcher que la perte ou la compromission ne se reproduise.
2. À la demande de la Partie destinataire, la Partie d'origine apporte son concours à la Partie destinataire dans le cadre de l'enquête en question.

## **ARTICLE 17**

### **Coûts**

Chaque Partie supporte les coûts qu'elle a engagés pour la mise en œuvre du présent accord.

## **ARTICLE 18**

### **Arrangements de mise en œuvre**

1. Les AS des Parties peuvent conclure des arrangements de mise en œuvre au titre du présent accord.
2. Les AC des Parties peuvent, dans les domaines relevant de leur compétence, conclure des arrangements de mise en œuvre spécifiant des mesures complémentaires concernant le traitement des informations classifiées. Ces arrangements sont subordonnés au présent accord.

## **ARTICLE 19**

### **Autres accords ou arrangements**

Le présent accord n'a pas pour effet de modifier les accords ou arrangements existants entre les Parties, sauf disposition contraire du présent accord.

## **ARTICLE 20**

### **Règlement des différends**

Les Parties règlent tout différend découlant de l'interprétation ou de la mise en œuvre du présent accord par la voie de consultations mutuelles.

## **ARTICLE 21**

### **Final Provisions**

1. This Agreement shall enter into force on the date of the receipt of the last written notification whereby the Parties notify each other, through diplomatic channels, of the completion of their internal procedures required for its entry into force.
2. The Parties may amend this Agreement by mutual consent in writing. Any amendment shall enter into force on the date of the later written notification, through diplomatic channels, that each Party has completed the internal procedures required for the entry into force of that amendment.
3. Either Party may terminate this Agreement by notice, in writing, to the other Party. This Agreement shall terminate six months after the date that the notice is received by the other Party.
4. Notwithstanding the termination of this Agreement, all classified information provided or disclosed pursuant to this Agreement shall continue to be protected according to the provisions set forth in this Agreement, unless the originating Party advises the receiving Party to do otherwise.
5. The Parties shall jointly review this Agreement at least once every five years to determine if amendments are required.
6. Upon its entry into force, this Agreement shall terminate and replace the Agreement between the Government of Canada and the Government of the Republic of Korea on the Exchange and Protection of Classified Military Information done at Ottawa on July 5, 1999.

**IN WITNESS WHEREOF** the undersigned, being duly authorized by their respective Governments, have signed this Agreement.

**DONE** in duplicate at Ottawa, on this 25<sup>th</sup> day of February, 2026, in the English, French, and Korean languages, each version being equally authentic.

**Anita Anand**

**FOR THE GOVERNMENT  
OF CANADA**

**Cho Hyun**

**FOR THE GOVERNMENT  
OF THE REPUBLIC OF KOREA**

## **ARTICLE 21**

### **Dispositions finales**

1. Le présent accord entre en vigueur à la date de la réception de la dernière notification écrite, transmise par la voie diplomatique, confirmant l'accomplissement des procédures internes respectives des Parties nécessaires à cette fin.
2. Les Parties peuvent amender le présent accord par consentement mutuel écrit. Tout amendement entre en vigueur à la date de la dernière des notifications écrites échangées entre les Parties, transmise par la voie diplomatique, pour confirmer l'accomplissement des procédures internes requises pour l'entrée en vigueur dudit amendement.
3. Chaque Partie peut dénoncer le présent accord au moyen d'une notification écrite adressée à l'autre Partie. Le présent accord prend fin six mois après la date de réception de la notification par l'autre Partie.
4. Nonobstant la dénonciation du présent accord, toutes les informations classifiées fournies ou communiquées au titre du présent accord continuent d'être protégées conformément aux dispositions du présent accord, sauf instruction contraire de la Partie d'origine à la Partie destinataire.
5. Les Parties procèdent à un examen conjoint du présent accord au moins une fois tous les cinq ans pour décider si des amendements s'imposent.
6. Dès son entrée en vigueur, le présent accord met fin à l'Accord entre le Gouvernement du Canada et le Gouvernement de la République de Corée sur l'échange et la protection de renseignements militaires classifiés, fait à Ottawa le 5 juillet 1999, et le remplace.

**EN FOI DE QUOI**, les soussignés, dûment autorisés à cet effet par leurs gouvernements respectifs, ont signé le présent accord.

**FAIT** en double exemplaire à Ottawa, ce 25<sup>e</sup> jour de février 2026, en langues française, anglaise et coréenne, chaque version faisant également foi.

**POUR LE GOUVERNEMENT  
DU CANADA**

**Anita Anand**

**POUR LE GOUVERNEMENT  
DE LA RÉPUBLIQUE DE CORÉE**

**Cho Hyun**