CANADA

TREATY SERIES **2026/8** RECUEIL DES TRAITÉS

UKRAINE / DEFENCE

Agreement Between Canada and Ukraine on the Mutual Protection of Classified Information

Done at Brussels on 3 December 2024

In Force on 7 April 2026

UKRAINE / DÉFENSE

Accord entre le Canada et l'Ukraine sur la protection mutuelle des informations classifiées

Fait à Bruxelles le 3 décembre 2024

En vigueur le 7 avril 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

Catalogue No: FR4-2026/8-PDF
ISBN: 978-0-660-99602-8

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

Nº de catalogue : FR4-2026/8-PDF
ISBN : 978-0-660-99602-8

CANADA

TREATY SERIES **2026/8** RECUEIL DES TRAITÉS

UKRAINE / DEFENCE

Agreement Between Canada and Ukraine on the Mutual Protection of Classified Information

Done at Brussels on 3 December 2024

In Force on 7 April 2026

UKRAINE / DÉFENSE

Accord entre le Canada et l'Ukraine sur la protection mutuelle des informations classifiées

Fait à Bruxelles le 3 décembre 2024

En vigueur le 7 avril 2026

AGREEMENT

BETWEEN

CANADA

AND

UKRAINE

ON THE MUTUAL PROTECTION OF CLASSIFIED INFORMATION

CANADA AND UKRAINE (the "Parties"),

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

RECOGNIZING the important role of their bilateral co-operation in ensuring peace, international security, and mutual confidence,

REALIZING that they may have to exchange classified information on co-operation in strengthening of defence and security,

DESIRING to create practices and procedures to govern the reciprocal protection of classified information for both Parties,

HAVE AGREED as follows:

ARTICLE 1

Definitions

In this Agreement:

(a) "classified information" means any information that is assigned a security classification marking by a Party and which requires protection against unauthorised disclosure, access, or destruction in the interest of national security and in accordance with its 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 marked PROTECTED A/PROTÉGÉ A, PROTECTED B/PROTÉGÉ B or PROTECTED C/PROTÉGÉ C unless otherwise specified;

ACCORD

ENTRE

LE CANADA

ET

L'UKRAINE

SUR LA PROTECTION MUTUELLE DES INFORMATIONS CLASSIFIÉES

LE CANADA ET L'UKRAINE (les « Parties »),

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

RECONNAISSANT l'importance de leur coopération bilatérale dans les efforts visant à garantir la paix et la sécurité internationale et à assurer une confiance réciproque;

CONSCIENTS qu'ils pourraient être appelés à échanger des informations classifiées sur la coopération nécessaire au renforcement de la défense et de la sécurité;

DÉSIRANT mettre en place des pratiques et des procédures régissant la protection réciproque des informations classifiées des deux Parties,

SONT CONVENUS de ce qui suit :

ARTICLE PREMIER

Définitions

Aux fins du présent accord :

a) « informations classifiées » désigne toutes les informations auxquelles une Partie a attribué un marquage 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 prendre une forme orale, visuelle, électronique, magnétique ou documentaire, ou se présenter 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'information classifiée dans le présent accord vise également les informations protégées du Canada marquées PROTÉGÉ A/PROTECTED A, PROTÉGÉ B/PROTECTED B ou PROTÉGÉ C/PROTECTED C, sauf indication contraire;

(b) “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;

(c) “competent authorities” (CAs) means governmental organisations designated by Canada and state authorities designated by Ukraine, as the authorities responsible, within their respective competence under the national laws and regulations, for the handling of classified information;

(d) “compromise” means the unauthorized access to, disclosure or provision of, destruction, removal, modification, use or interruption 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 authorised 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;

(l) “security authority” (SA) means a governmental organisation designated by Canada, and a state authority designated by Ukraine, to administer the implementation of this Agreement; and

b) « 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 vise également les contrats de sous-traitance et les activités préalables à l'attribution d'un contrat;

c) « autorités compétentes » (AC) désigne les organisations gouvernementales désignées par le Canada et les autorités d'État désignées par l'Ukraine comme autorités responsables, dans les limites de leurs compétences respectives en vertu des lois et 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, l'utilisation ou l'interruption non autorisées de ces informations;

e) « contractant » désigne une personne physique ou morale ayant la capacité juridique de conclure un contrat classifié. Ce terme vise également un sous-traitant;

f) « habilitation de sécurité d'installation » (HSI) s'entend de 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) s'entend de 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 ou d'un projet » (ISP) désigne les règlements et procédures en matière de sécurité colligés à partir de la politique de sécurité nationale et des directives connexes, qui sont appliqués à un projet ou à un programme 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 le Canada, et une autorité d'État désignée par l'Ukraine, qui est chargée d'administrer la mise en œuvre du présent accord;

(m) "third party" means any individual, legal entity, country, or organisation of any form under its jurisdiction, or an international organisation not being a party to this Agreement. 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.

ARTICLE 2

Objective and Scope

1. This Agreement sets out the standards and procedures for the protection of classified information regarding defence and security that is provided or disclosed, in an industrial security or defence context, by one Party to the other Party, or by one Party to a contractor from the other Party, or by a contractor from one Party to a contractor from the other Party.

2. This Agreement cannot be construed to compel a Party to provide or disclose classified information.

ARTICLE 3

Security Authorities

1. For the purpose of this Agreement, the SAs of the Parties are:

(a) for Canada:

International Industrial Security Directorate,

Industrial Security Sector,

Public Works and Government Services Canada,

(also known as Public Services and Procurement Canada)

(b) for Ukraine:

the Security Service of Ukraine

or their respective successors.

2. The SAs of the Parties shall notify, in writing, each other of the CAs of its Party for this Agreement.

m) « tierce partie » désigne toute personne physique ou morale, toute organisation internationale, ou tout pays ou organisation relevant de la juridiction de celui-ci, quelle que soit sa forme, qui n'est pas partie au présent accord. Aux fins du présent accord, une personne qui possède une HSP ou un contractant qui possède une HSI délivrée par l'une ou l'autre des Parties n'est pas considéré comme une tierce partie.

ARTICLE 2

Objectif et portée

1. Le présent accord énonce les normes et les procédures régissant la protection des informations classifiées concernant la défense et la sécurité qui sont fournies ou communiquées, dans un contexte de sécurité industrielle ou de défense, par une Partie à l'autre Partie, ou par une Partie à un contractant de l'autre Partie, ou encore par un contractant d'une Partie à un contractant 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. Aux fins du présent accord, les AS des Parties sont :

a) pour le Canada :
Direction de la sécurité industrielle internationale
Secteur de la sécurité industrielle
Travaux publics et Services gouvernementaux Canada
(aussi connu sous le nom de Services publics et Approvisionnement Canada)

b) pour l'Ukraine :
le Service de sécurité de l'Ukraine,

ou leurs successeurs respectifs.

2. Les AS des Parties se notifient, par écrit, les noms des AC de leur Partie au titre du présent accord.

ARTICLE 4

Security Classification Markings

1. The originating Party shall assign a security classification marking 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, shall mark classified information that is provided or disclosed by the originating Party with a security classification marking that is at least equivalent to the security classification marking assigned by the originating Party, in accordance with Table 1 and Table 2.

3. Table 1 identifies equivalence of the security classification markings of classified information used by the respective Parties:

Table 1: Classified Information

In Canada (English)	**In Canada (French)**	**In Ukraine (Ukrainian)**	**Remark**
TOP SECRET	TRÈS SECRET	Особливої важливості	
SECRET	SECRET	Цілком таємно	
CONFIDENTIAL	CONFIDENTIEL	Таємно	
PROTECTED A	PROTÉGÉ A	Для службового користування	See paragraph 4

4. Canada may identify additional security requirements in contract clauses for the protection and handling of the PROTECTED A/PROTÉGÉ A information to govern the access to such information by contractors from Ukraine.

5. Ukraine shall protect Canadian information marked PROTECTED A/ PROTÉGÉ A, PROTECTED B/PROTÉGÉ B or PROTECTED C/PROTÉGÉ C at the security classification marking identified in Table 2:

ARTICLE 4

Marquage de classification de sécurité

1. La Partie d'origine attribue un marquage de classification de sécurité aux informations classifiées et y appose les marques de classification de sécurité requises en vertu de ses lois et règlements nationaux.

2. La Partie destinataire, conformément à ses lois et règlements nationaux, appose sur les informations classifiées fournies ou communiquées par la Partie d'origine des marques de classification de sécurité au moins équivalentes aux marques de classification de sécurité attribuées par la Partie d'origine, conformément au tableau 1 et au tableau 2.

3. Le tableau 1 indique les équivalences entre les marques de classification de sécurité des informations classifiées utilisées par les Parties respectives :

Tableau 1 : Informations classifiées

Au Canada (français)	**Au Canada (anglais)**	**En Ukraine (ukrainien)**	**Remarque**
TRÈS SECRET	TOP SECRET	Особливої важливості	
SECRET	SECRET	Цілком таємно	
CONFIDENTIEL	CONFIDENTIAL	Таємно	
PROTÉGÉ A	PROTECTED A	Для службового користування	Voir le paragraphe 4

4. Le Canada peut spécifier des exigences de sécurité supplémentaires dans les clauses contractuelles concernant la protection et le traitement des informations marquées PROTÉGÉ A/PROTECTED A afin de régir l'accès des contractants de l'Ukraine auxdites informations.

5. L'Ukraine accorde aux informations du Canada marquées PROTÉGÉ A/ PROTECTED A, PROTÉGÉ B/PROTECTED B ou PROTÉGÉ C/PROTECTED C une protection correspondant à la marque de classification de sécurité indiquée dans le tableau 2 :

Table 2: Canadian Protected Information

In Canada (English)	In Canada (French)	In Ukraine (Ukrainian)
PROTECTED C	PROTÉGÉ C	Цілком таємно
PROTECTED B	PROTÉGÉ B	Таємно
PROTECTED A	PROTÉGÉ A	Для службового користування

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 classified information of an equivalent security classification marking;

   (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 marking 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 a change in the security classification marking of classified information; and

Tableau 2 : Informations protégées du Canada

Au Canada (français)	Au Canada (anglais)	En Ukraine (ukrainien)
PROTÉGÉ C	PROTECTED C	Цілком таємно
PROTÉGÉ B	PROTECTED B	Таємно
PROTÉGÉ A	PROTECTED A	Для службового користування

ARTICLE 5

Protection et utilisation des informations classifiées

1. Les Parties protègent et utilisent les informations classifiées comme suit :

   a) la Partie destinataire assure une protection au moins égale à celle qu'elle accorde à ses propres informations classifiées portant une marque de classification de sécurité équivalente;

   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'intermédiaire des AS ou 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 destinataire ne peut déclasser la classification de sécurité des informations classifiées ou déclassifier les informations classifiées, sauf avec le consentement préalable écrit de la Partie d'origine, donné par l'intermédiaire des AS ou AC respectives des Parties;

   e) la Partie d'origine informe la Partie destinataire de toute modification apportée à la marque de classification de sécurité apposée sur des informations classifiées;

(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 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, unless the originating Party provides consent to such release in exceptional circumstances. The Parties shall give an individual access to classified information only if that individual:

(a) has a need-to-know;

(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 a contractor of the means and the packaging standards that they have jointly approved for the transmission of classified information.

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.

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 concernant 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 à avoir accès à des informations classifiées uniquement en raison de son rang, d'une nomination ou d'une HSP, à moins que la Partie d'origine n'y consente dans des circonstances exceptionnelles. Les Parties ne peuvent autoriser l'accès aux informations classifiées qu'à une personne qui, à la fois :

a) a le besoin d'en connaître;

b) possède une HSP du 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. Par l'intermédiaire de leurs AS respectives, les Parties informent le contractant des moyens de transmission et des normes d'emballage qu'elles ont approuvés conjointement pour la transmission des informations classifiées.

4. Si les informations classifiées sont trop volumineuses pour être transmises par un service de messagerie autorisé à cette fin, les Parties, par l'intermédiaire de leurs AS respectives, rédigent conjointement une ébauche de plan de transport décrivant de quelle manière 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. 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 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 marked CONFIDENTIAL/ CONFIDENTIEL/Таємно or above is not translated or reproduced without the written consent of the originating Party given through its SA or one of its CAs, when prior consent has not been provided by the originating Party.

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 marking of the original classified information and is given the same 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 marking.

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;

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 à les protéger pendant la 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 marquées CONFIDENTIEL/CONFIDENTIAL/Таємно ou d'un niveau de classification supérieur ne soient pas traduites ou reproduites sans le consentement écrit de la Partie d'origine, donné par l'intermédiaire de son AS ou de l'une de ses AC, en l'absence de consentement préalable de la Partie d'origine.

2. Les Parties font en sorte que toute traduction ou reproduction des informations classifiées autorisée par la Partie d'origine conserve la marque de classification de sécurité qui a été attribuée aux informations classifiées d'origine, et se voie accorder la même protection.

3. Si la Partie destinataire n'a plus besoin des informations classifiées et que la Partie d'origine autorise leur destruction ou leur renvoi dans le pays d'origine, ou que la Partie d'origine demande leur destruction ou leur renvoi, la Partie destinataire détruit ou renvoie les informations classifiées conformément au niveau de protection qu'elle attribue à ses propres informations classifiées portant une marque de classification de sécurité équivalente.

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) the facility of the contractor has a valid FSC to handle classified information marked CONFIDENTIAL/CONFIDENTIEL/Таємно or above;

(c) an individual who has access to classified information has a need-to-know and a valid PSC to the appropriate level;

(d) an 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 that has an FSC 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.

ARTICLE 10

Contract Security Clauses

A Party shall ensure that:

(a) a classified contract that requires access to classified information is governed by security clauses in accordance with the national laws and regulations of that Party and the provisions of this Agreement;

(b) a classified contract includes 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 marking that is assigned to that classified information;

(c) for a classified contract that is performed in the territory of the other Party, the SA or one of the CAs of the originating Party promptly provides to the SA of the other Party a copy of the description of the security requirements;

(d) security clauses that govern a classified contract include at least:

(i) a requirement that the contractor provide or disclose the classified information only to an individual who has a PSC, a need-to-know, and a briefing on the protection of classified information in accordance with that Party's national laws and regulations;

b) l'installation du contractant fasse l'objet d'une HSI en cours de validité lui permettant de traiter des informations classifiées marquées CONFIDENTIEL/CONFIDENTIAL/Таємно ou d'un niveau de classification supérieur;

c) toute personne ayant accès aux informations classifiées ait le besoin d'en connaître et possède une HSP en cours de validité du niveau approprié;

d) toute personne 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 faisant l'objet d'une HSI 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 l'installation d'un contractant qui traite les 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

Clauses contractuelles relatives à la sécurité

Une Partie fait en sorte :

a) qu'un contrat classifié exigeant l'accès à des informations classifiées soit régi par des clauses de sécurité conformément aux lois et règlements nationaux de cette Partie et aux dispositions du présent accord;

b) qu'un contrat classifié comporte 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 générées par celui-ci, ainsi que le marquage de classification de sécurité attribué à ces informations classifiées;

c) s'agissant d'un contrat classifié exécuté sur le territoire de l'autre Partie, que l'AS ou l'une des AC de la Partie d'origine fournisse promptement à l'AS de l'autre Partie une copie de la description des exigences de sécurité;

d) que les clauses de sécurité régissant un contrat classifié prévoient au minimum :

i) une disposition stipulant que le contractant ne peut fournir ou communiquer les informations classifiées qu'à une personne qui possède une HSP, qui 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) the means to be used to transmit the classified information;

(iii) the procedures to request an international visit to a state, governmental, or industrial facility in a Party's territory, in accordance with Article 14 of this Agreement;

(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 where the contractor is located on the possibility that classified information is 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;

(vii) the procedures for the return or destruction of classified information when no longer required;

(viii) a requirement that a contractor not provide or disclose classified information to a third party 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 the classified contract is performed shall ensure that the description of the security requirements pertaining to the classified contract is provided to the SA of the Party where the contractor is located. For Canada, the security requirements are described in a Security Requirements Check List (SRCL). For Ukraine, the security requirements are described in an application letter, the form of which is determined by its SA.

2. When the Parties determine that the size or complexity of the 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.

ii) les moyens à utiliser pour transmettre les informations classifiées;

iii) la procédure à suivre pour demander une visite internationale d'une installation étatique, gouvernementale ou industrielle sur le territoire d'une Partie, conformément à l'article 14 du présent accord;

iv) la procédure à suivre par une Partie, par l'intermédiaire de son AS, pour inspecter une installation d'un contractant située sur son territoire;

v) la procédure à suivre par un contractant pour informer promptement l'AS de la Partie sur le territoire de laquelle il est situé 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) la procédure à suivre pour le renvoi dans le pays d'origine ou la destruction des informations classifiées lorsqu'elles ne sont plus nécessaires;

viii) une disposition interdisant au contractant de fournir ou de communiquer des informations classifiées à une tierce partie 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 que la description des exigences de sécurité relatives à ce contrat soit fournie à l'AS de la Partie sur le territoire de laquelle le contractant est situé. En ce qui concerne le Canada, les exigences de sécurité sont décrites dans une Liste de vérification des exigences relatives à la sécurité (LVERS). En ce qui concerne l'Ukraine, les exigences de sécurité sont décrites dans une lettre de demande dont la forme est déterminée par son AS.

2. Si les Parties jugent que l'ampleur ou la complexité du programme ou du 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

Security Assurances

1. A Party, through its SA, shall take measures to ensure that a contractor from the other Party is not awarded a classified contract and does not receive 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 is provided in accordance with the national laws and regulations of that Party.

3. A Party shall ensure that:

(a) if its SA grants a PSC or FSC to a contractor at the request of the other Party, that SA may suspend or withdraw that PSC or FSC in accordance with the national laws and regulations of that Party, and that SA promptly informs the SA of the other Party of that suspension or withdrawal;

(b) if its SA cannot provide a security assurance because a contractor does not have a PSC or FSC that meets the security requirements for a classified contract, that SA, acting at the request of the SA of the other Party, conducts a security assessment to determine if it should grant or upgrade the PSC or FSC of that contractor and if it should provide a security assurance in accordance with paragraph 2 of this Article; and

(c) if its SA cannot promptly provide a security assurance in response to a request from the other Party, that SA informs the SA of the other Party of the status of the request.

4. The SA that receives a request for a security assurance shall respond within eight working days unless the Parties jointly determine otherwise.

5. At the request of the Party that conducts a security assessment to determine if it should grant a PSC or FSC, the other Party shall assist it with that security assessment.

ARTICLE 12

Garanties de sécurité

1. Une Partie prend, par l'intermédiaire de son AS, les mesures nécessaires pour faire en sorte qu'aucun contrat classifié ne soit attribué à un contractant de l'autre Partie, et que ce dernier ne reçoive 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 cette Partie.

3. Une Partie fait en sorte :

a) si son AS délivre une HSP ou une HSI à un contractant à la demande de l'autre Partie, que l'AS en question puisse suspendre ou retirer cette HSP ou HSI conformément aux lois et règlements nationaux de cette Partie, et que l'AS en question informe promptement l'AS de l'autre Partie de cette suspension ou de ce retrait;

b) si son AS n'est pas en mesure de fournir une garantie de sécurité parce qu'un contractant ne possède pas d'HSP ou d'HSI qui satisfait aux exigences de sécurité applicables à un contrat classifié, que l'AS en question, à la demande de l'AS de l'autre Partie, mène une enquête de sécurité pour décider si elle devrait délivrer une HSP ou une HSI audit contractant ou relever le niveau de l'HSP ou de l'HSI dont il fait l'objet, et si elle devrait fournir une garantie de sécurité conformément au paragraphe 2 du présent article;

c) si son AS n'est pas en mesure de fournir promptement la garantie de sécurité demandée par l'autre Partie, que l'AS en question informe l'AS de l'autre Partie de l'état d'avancement de la demande.

4. L'AS qui reçoit une demande de garantie de sécurité y répond dans un délai de huit jours ouvrables, ou dans tout autre délai déterminé conjointement par les Parties.

5. À la demande de la Partie qui mène une enquête de sécurité pour décider si elle devrait délivrer une HSP ou une HSI, l'autre Partie lui apporte son concours dans le cadre de cette enquête.

ARTICLE 13

Security Assessments and Consultations

1. The Parties may jointly determine 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, practices, and procedures relevant to this Agreement to ensure that their application of those laws, regulations, practices, and procedures is consistent.

3. The Parties shall jointly determine the frequency, timing and location of meetings and visits.

ARTICLE 14

International Visits

1. A Party shall ensure that:

   (a) its SA or one of its CAs approves a visit by an individual who works for the other Party or for a contractor from the other Party to a state, governmental or industrial facility in its territory if that 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) if an individual who works for that Party or for a contractor from that Party requests a visit to a facility providing access to classified information with security classification marking at CONFIDENTIAL/CONFIDENTIEL/Таємно or above 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 first name and surname, date and place of birth, nationality, passport or identity card number, service designation (if applicable), position, and PSC level, as well as the name of the parent authority or agency of the visitor, the purpose of the visit, the proposed date of the visit, the contact persons of the visitor, and 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 determine otherwise.

ARTICLE 13

Enquêtes 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, pratiques et procédures nationales respectives en matière de sécurité de l'information qui sont pertinentes au regard du présent accord, afin de faire en sorte que ces lois, réglementations, pratiques et procédures soient appliquées de manière cohérente.

3. Les Parties déterminent conjointement la fréquence, le calendrier et le lieu des réunions et des visites.

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 qui travaille pour l'autre Partie, ou pour un contractant de l'autre Partie, dans une installation étatique, gouvernementale ou industrielle 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 d'en connaître;

   b) si une personne qui travaille pour cette Partie ou pour un contractant de cette Partie demande à visiter une installation donnant accès à des informations classifiées marquées CONFIDENTIEL/ CONFIDENTIAL/Таємно ou d'un niveau de classification supérieur sur le territoire de l'autre Partie, que la personne en question présente sa demande par l'intermédiaire de l'AS de la 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 militaire (le cas échéant), son poste, le niveau de son HSP, ainsi que le nom de l'autorité ou de l'organisme dont il relève, l'objet de sa visite, la date de visite proposée, les personnes-ressources du visiteur et 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. In the context of specific classified contracts, the SA or one of the CAs of each of the Parties may jointly determine to permit recurring visits that allow specified individuals to visit specified facilities more than once without further written authorisation. 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 determined 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 visitors.

ARTICLE 15

Third Party Restrictions

1. The receiving Party shall not provide or disclose classified information to a third party without the prior written consent of the SA of the originating Party.

2. The Parties shall ensure that their respective contractors do not provide or disclose classified information to contractors from a third party without the prior written consent of both Parties' SAs.

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 its SA and 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 Party that conducts an investigation, the other Party shall assist it with that investigation.

ARTICLE 17

Costs

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

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 une AC de l'autre Partie d'autoriser certaines personnes 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 des visiteurs.

ARTICLE 15

Restrictions applicables aux tierces parties

1. La Partie destinataire ne peut fournir ou communiquer des informations classifiées à une tierce partie sans le consentement écrit préalable de l'AS de la Partie d'origine.

2. Les Parties font en sorte que leurs contractants respectifs s'abstiennent de fournir ou de communiquer des informations classifiées à des contractants d'une tierce partie sans le consentement écrit préalable des AS des deux Parties.

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 son AS et 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 qui mène une enquête, l'autre Partie lui apporte son concours 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

Implementing Arrangements

1. The SAs of the Parties may conclude implementing arrangements pursuant to this Agreement.

2. 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 are 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 resolve a dispute that arises with respect to this Agreement through consultations.

ARTICLE 21

Final Provisions

1. The Parties shall notify each other in writing, through diplomatic channels, of the completion of the internal requirements for the entry into force of this Agreement. This Agreement enters into force on the date of the later notification.

2. The Parties may amend this Agreement by joint consent in writing. An amendment enters into force on the date of the later notification that each Party has completed the internal requirements for entry into force of that amendment.

3. A Party may terminate this Agreement by notice, in writing, to the other Party. This Agreement terminates three 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 informs to do otherwise.

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 précisant 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 des accords ou arrangements existants entre les Parties, sauf disposition contraire du présent accord.

ARTICLE 20

Règlement des différends

Les Parties règlent tout différend découlant du présent accord par la voie de consultations.

ARTICLE 21

Dispositions finales

1. Les Parties se notifient par écrit, par la voie diplomatique, l'accomplissement des formalités internes requises pour l'entrée en vigueur du présent accord. Le présent accord entre en vigueur à la date de la dernière de ces notifications.

2. Les Parties peuvent amender le présent accord par consentement mutuel écrit. L'amendement entre en vigueur à la date de la dernière des notifications échangées entre les Parties pour confirmer l'accomplissement des formalités internes requises pour l'entrée en vigueur dudit amendement.

3. Une Partie peut dénoncer le présent accord par voie de notification écrite adressée à l'autre Partie. Le présent accord prend fin trois 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.

5. The Parties shall jointly review this Agreement at least once every five years to determine if amendments are required.

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

DONE in duplicate at Brussels on this 3rd day of December 2024, in the English, French, and Ukrainian languages, all language versions being equally authentic.

Mélanie Joly	**Andrii Sybiha**
FOR CANADA	**FOR UKRAINE**

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.

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

FAIT en double exemplaire à Bruxelles, ce 3e jour de décembre 2024, en langues française, anglaise et ukrainienne, toutes les versions linguistiques faisant également foi.

POUR LE CANADA	**POUR L'UKRAINE**
Mélanie Joly	**Andrii Sybiha**