Council of the
European Union

Brussels, 21 September 2017
(OR. en)

12447/17

CSC 211

NOTE

From:	General Secretariat of the Council
On:	21 September 2017
To:	Delegations
No. prev. doc.:	ST 11233/17
Subject:	Implementing Administrative Arrangement for protecting classified information exchanged between the EU and Canada

Delegations find attached at Annex the Implementing Administrative Arrangement for protecting classified information exchanged between the EU and Canada, as approved by the Council Security Committee on 20 April 2017, and finalised by the Council lawyer-linguists and Canadian jurilinguists.

IMPLEMENTING ADMINISTRATIVE ARRANGEMENT
BETWEEN THE DEPARTMENT OF FOREIGN AFFAIRS, TRADE
AND DEVELOPMENT AND THE DEPARTMENT OF PUBLIC WORKS
AND GOVERNMENT SERVICES OF CANADA
AND THE DIRECTORATE OF SAFETY AND SECURITY OF THE GENERAL
SECRETARIAT OF THE COUNCIL OF THE EUROPEAN UNION,
THE SECURITY DIRECTORATE OF THE EUROPEAN COMMISSION,
AND THE EUROPEAN EXTERNAL ACTION SERVICE SECURITY DEPARTMENT,
ON THE EXCHANGE AND PROTECTION OF CLASSIFIED INFORMATION

I. INTRODUCTION

Pursuant to Article 11 of the Agreement between Canada and the European Union on security procedures for exchanging and protecting classified information ("the Agreement"), the Department of Foreign Affairs, Trade and Development (DFATD) and the Department of Public Works and Government Services (PWGSC) of Canada, the Directorate of Safety and Security of the General Secretariat of the European Union (GSCDSS), the Security Directorate of the European Commission (ECSD) and the European External Action Service Security Department (EEAS DGBA.IBS), hereinafter referred to as the "Participants", hereby establish reciprocal standards for exchanging and protecting classified information. The Participants will implement and oversee these standards.

Unless otherwise specified, all references in this Implementing Administrative Arrangement (the "Arrangement") to classified information are deemed to refer also to Canadian protected information pursuant to Article 2 of the Agreement.

II. PERSONNEL SECURITY CLEARANCE AND AUTHORISATION FOR ACCESS

1. The Participants understand that, for the purposes of implementing Article 6 of the Agreement:

(i) for the EU, the national security authority of the Member State of the individual who requires access to classified information will ensure that security screening procedures and investigations on that individual have been carried out in accordance with the appropriate EU security standards;

(ii) for Canada, the federal department or agency of the individual who requires access to classified information will ensure that security screening procedures and investigations on that individual have been carried out in accordance with appropriate Canada security standards.

2. The Participants understand that the Parties to the Agreement ("the Parties") will identify specific positions in their respective institutions and entities which may have access to classified information exchanged under the Agreement. Before giving access to such information, and at regular intervals thereafter, the Participants understand that the Parties will:

(i) brief all individuals who will have access to classified information on the security regulations and requirements relevant to the classification of the information;

(ii) obtain an acknowledgment in writing that those individuals understand their responsibilities to protect the information;

(iii) inform those individuals that any breach of the security regulations may result in disciplinary action and possible further legal action in accordance with the receiving Party's laws, rules and regulations.

III. CLASSIFICATION AND RELEASABILITY MARKINGS

The Participants understand that:

1. the Parties will use the security classification markings set out in Article 4(2) of the Agreement to indicate the sensitivity of the classified information and thus the security regulations and procedures which apply to its exchange and protection;

2. Article 4(4) of the Agreement provides that Canadian information marked PROTECTED A or PROTÉGÉ A will be handled and stored in the same manner as the EU information classified RESTREINT UE/EU RESTRICTED, and thus determines the security regulations and/or procedures which apply to its handling and storage;

3. the security regulations and procedures which apply to the exchange and protection of Canadian information marked PROTECTED B or PROTÉGÉ B and PROTECTED C or PROTÉGÉ C are described in paragraphs (3) and (4) of Section VII of this Arrangement;

4. information originating in one of the Parties and provided to the other will include an express releasability marking, such as:

SECRET
RELEASABLE TO THE EU

SECRET UE/EU SECRET
RELEASABLE TO CANADA

5. the Parties may add further access or distribution limitations to the releasability statement as deemed necessary by the providing Party.

IV. REGISTRIES AND CONTROL OF CLASSIFIED INFORMATION

Registries

1. The Participants understand that:

(i) the Parties will establish registries in the Mission of Canada to the European Union, the General Secretariat of the Council, the European Commission and the EEAS for the receipt, dispatch, control and storage of classified information;

(ii) the registries will be in charge of the distribution and control of classified information. The registry that constitutes the point of entry or exit for classified information will record the arrival or departure of that information in a logbook, indicating the date received, particulars of the document (date, reference and copy number), the subject of the document, the security markings, the title, the addressee's name or title, and any additional information regarding its handling, distribution, storage, return or destruction that is not covered in this Arrangement;

(iii) registries will be in charge of the final disposal (including return if so requested) and, subject to instructions by the providing Party, downgrading and/or declassification of classified information, including the maintenance of destruction certificates.

Oversight of registries

2. The Participants will oversee their respective registries and will inform the other Participants of the establishment/disestablishment of registries containing classified information exchanged under the Agreement.

V. MANAGEMENT OF CLASSIFIED INFORMATION IN ACCORDANCE WITH ARTICLE 4 OF THE AGREEMENT

The Participants understand that:

Storage

1. a Party will store classified information provided by the other Party only in secure and controlled locations as follows:

(i) information classified as SECRET UE/EU SECRET or Canadian SECRET, CONFIDENTIEL UE/EU CONFIDENTIAL or Canadian CONFIDENTIAL or CONFIDENTIEL will be stored in a secured area that is monitored in such a way that it can be protected from access by unauthorised persons by means of internally established controls and in accordance with the receiving Party's laws, rules and regulations. It will be stored in a security container or in a strong room, in accordance with the receiving Party's laws, rules and regulations;

(ii) information classified as TRÈS SECRET UE/EU TOP SECRET or Canadian TOP SECRET or TRÈS SECRET will be stored in a secured area that is continuously monitored in such a way that it can be protected from access by unauthorised persons by means of internally established controls and in accordance with the receiving Party's laws, rules and regulations. It will be stored in a security container or in a strong room, in accordance with the receiving Party's laws, rules and regulations;

Handling

2. a Party will handle classified information provided by the other Party only in secure and controlled locations as follows:

(i) the EU will handle Canadian information classified as SECRET or CONFIDENTIAL or CONFIDENTIEL in areas where it can be protected from access by unauthorised persons, in accordance with its rules and regulations, where no additional handling limitations are marked on the information;

(ii) Canada will handle information classified as CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET in secured areas where it can be protected from access by unauthorised persons, in accordance with its laws, rules and regulations;

(iii) information classified as TRÈS SECRET UE/EU TOP SECRET or Canadian TOP SECRET or TRÈS SECRET will be handled in a secured area that is monitored in such a way that it can be protected from access by unauthorised persons by means of internally established controls and in accordance with the receiving Party's laws, rules and regulations;

Copying and translation

3. information classified as SECRET UE/EU SECRET or Canadian SECRET and above may be reproduced, copied or translated by the receiving Party only with the providing Party's prior written consent;

4. information classified as CONFIDENTIEL UE/EU CONFIDENTIAL or Canadian CONFIDENTIAL or CONFIDENTIEL may be reproduced, copied or translated by the receiving Party without the providing Party's prior written consent, where the providing Party has not imposed caveats on reproducing, copying or translating;

5. the receiving Party may only reproduce, copy or translate classified information on approved equipment;

6. when the receiving Party reproduces, copies or translates classified documents or media containing classified information, that Party will also reproduce or mark on each copy all original security markings. The receiving Party will place such reproduced documents or media under the same protection as the original documents or media. The number of copies will be limited to that required for official purposes;

Destruction

7. the receiving Party will destroy documents or media containing classified information received from the providing Party when those documents or media are no longer needed, or on instruction from the providing Party, in accordance with the receiving Party's laws, rules and regulations or, if requested, will return the documents or media to the providing Party for destruction;

8. the receiving Party will destroy material, including equipment, containing classified information in whole or in part, so that it is no longer recognisable and so as to preclude reconstruction of the classified information in whole or in part;

9. when destroying information classified as CONFIDENTIEL UE/EU CONFIDENTIAL or Canadian CONFIDENTIAL or CONFIDENTIEL, the receiving Party will certify the destruction and retain a certificate for at least five years. When information classified as SECRET UE/EU SECRET or Canadian SECRET is destroyed, destruction will be certified and witnessed by an appropriately security cleared person from the receiving Party and a certificate will be retained for at least five years. When information classified as TRÈS SECRET UE/EU TOP SECRET or Canadian TOP SECRET or TRÈS SECRET is destroyed, destruction will be certified and witnessed by at least one appropriately security cleared person from the receiving Party and the certificate will be retained for at least ten years.

VI. SPECIFIC REQUIREMENTS FOR INFORMATION CLASSIFIED RESTREINT UE/EU RESTRICTED

The Participants understand that pursuant to Article 4(3) of the Agreement, Canada will afford information classified as RESTREINT UE/EU RESTRICTED a level of protection which is at least equivalent to that afforded by the EU. This means that:

Who may have access

(i) Canada will grant access to RESTREINT UE/EU RESTRICTED information only to individuals who have an established need-to-know for the performance of their duties, and who have been briefed on and acknowledge in writing their responsibilities to protect the information appropriately;

Physical protection

(ii) Canada will handle and store RESTREINT UE/EU RESTRICTED information in administrative/operational areas. These will be composed of a visibly defined perimeter which allows individuals and, where possible, vehicles, to be checked. Only duly authorised individuals may have access to such areas. All other individuals will be escorted at all times or be subject to equivalent controls. Inside these areas RESTREINT UE/EU RESTRICTED information will be stored in locked office furniture;

Registry roles

(iii) the Mission of Canada to the European Union will keep a record of all RESTREINT UE/EU RESTRICTED information received;

Electronic handling

(iv) all Canadian communication and information systems (CIS) that handle information classified as RESTREINT UE/EU RESTRICTED will require accreditation by a Canadian governmental security accreditation authority resulting in a statement of compliance with the relevant EU security rules, policies and guidelines. Transmission will require protection by an EU approved cryptographic product;

Copying and translation

(v) Canada may reproduce, copy or translate RESTREINT UE/EU RESTRICTED information without the EU's prior consent;

Destruction

(vi) Canada will destroy RESTREINT UE/EU RESTRICTED information in such a manner that it is no longer recognisable or usable and so as to preclude reconstruction of the classified information in whole or in part.

VII. SPECIFIC REQUIREMENTS FOR CANADA'S PROTECTED INFORMATION

1. The Participants understand that:

(i) the provisions on the protection of protected information set out in this Arrangement are applicable only to the protected information released by Canada to the EU under the Agreement. According to Article 14 of the Agreement these provisions cannot be considered a precedent or a model with regard to the content of any bilateral agreements between individual EU Member States and Canada on the protection of classified information;

(ii) Canada requires that the EU carry out as a minimum an EU record of good conduct check unless a security clearance at the level CONFIDENTIEL UE/EU CONFIDENTIAL or above has already been granted prior to an individual having access to protected information.

PROTECTED A or PROTÉGÉ A

2. The Participants understand that, pursuant to Article 4(4) of the Agreement:

(i) the EU will handle and store PROTECTED A or PROTÉGÉ A information in the same manner as the EU information classified RESTREINT UE/EU RESTRICTED, thus providing a level of protection which is at least equivalent;

(ii) the EU may grant access to PROTECTED A or PROTÉGÉ A information only to individuals who have an established need-to-know for the performance of their duties and who have undergone an EU record of good conduct check unless a security clearance at the level of CONFIDENTIEL UE/EU CONFIDENTIAL or above has already been granted.

PROTECTED B or PROTÉGÉ B

3. The Participants understand that, in accordance with Article 4(4) of the Agreement, the EU will handle and store PROTECTED B or PROTÉGÉ B information at a level of protection which is at least equivalent to that afforded by Canada. This means that:

Who may have access

(i) the EU may grant access to PROTECTED B or PROTÉGÉ B information only to individuals who have an established need-to-know for the performance of their duties, have been briefed on and acknowledged in writing their responsibilities to protect the information appropriately, and have undergone an EU record of good conduct check unless a security clearance at the level of CONFIDENTIEL UE/EU CONFIDENTIAL or above has already been granted;

Physical protection

(ii) the EU may only handle PROTECTED B or PROTÉGÉ B information in areas where it can be protected from access by unauthorised persons and will be stored in a security container or in a strong room;

Registry roles

(iii) the receiving EU registry will keep a record of all PROTECTED B or PROTÉGÉ B information received;

Electronic handling

(iv) all EU CIS that handle information marked as PROTECTED B or PROTÉGÉ B will require an accreditation by an EU security accreditation authority resulting in a statement of compliance with the relevant Canadian security rules, policies and guidelines. The transmission will require protection by a Canada approved cryptographic product;

Copying and translation

(v) the EU may reproduce, copy or translate PROTECTED B or PROTÉGÉ B information with Canada's prior approval on approved equipment;

Destruction

(vi) the EU will destroy PROTECTED B or PROTÉGÉ B information in such a manner that it is no longer recognisable or usable and so as to preclude reconstruction of the information in whole or in part.

PROTECTED C or PROTÉGÉ C

4. The Participants understand that, in accordance with Article 4(4) of the Agreement, the EU will handle and store PROTECTED C or PROTÉGÉ C information at a level of protection which is at least equivalent to that afforded by Canada. This means that:

Who may have access

(i) the EU may grant access to PROTECTED C or PROTÉGÉ C information only to individuals who have an established need-to-know for the performance of their duties, have been briefed on and acknowledged in writing their responsibilities to protect the information appropriately, and have undergone an EU record of good conduct check unless a security clearance at the level of CONFIDENTIEL UE/EU CONFIDENTIAL or above has already been granted;

Physical protection

(ii) the EU may handle PROTECTED C or PROTÉGÉ C only in secured areas that are monitored, where it can be protected from access by unauthorised persons and where it will be stored in a security container or in a strong room;

Registry roles

(iii) the receiving EU registry will keep a record of all PROTECTED C or PROTÉGÉ C information received;

Electronic handling

(iv) all EU CIS that handle information marked as PROTECTED C or PROTÉGÉ C will require accreditation by an EU security accreditation authority resulting in a statement of compliance with the relevant Canadian security rules, policies and guidelines. Transmission will require protection by a Canada approved cryptographic product;

Copying and translation

(v) the EU may reproduce, copy or translate PROTECTED C or PROTÉGÉ C information with Canada's prior approval on approved equipment;

Destruction

(vi) the EU will destroy PROTECTED C or PROTÉGÉ C information in such a manner that it is no longer recognisable or usable and so as to preclude reconstruction of the information in whole or in part.

VIII. TRANSMISSION OF CLASSIFIED INFORMATION BETWEEN THE PARTIES

The Participants understand that:

1. for the purposes of implementing Article 9 of the Agreement:

(i) Canada will send all correspondence containing classified information through the:

Council of the European Union

Chief Registry Officer

Rue de la Loi/Wetstraat 175

B-1048 Brussels;

A. if classified documents are addressed to specific competent officials, organs or services of the European Commission, correspondence will be transmitted through the:

European Commission

Registry Control Officer

SG Central EUCI Registry (CENTER) - SG.A4

Rue de la Loi/Wetstraat 200

B-1049 Brussels

B. if classified documents are addressed to specific competent officials, organs or services of the European External Action Service, correspondence will be transmitted through the:

EEAS Central EUCI Registry

Head of the Central Registry

06/407

Rond Point Robert Schuman/ **ROBERT** Schumanplein 9

B-1040 Brussels

C. all such correspondence may be forwarded by the Chief Registry Officer of the Council to the Member States and to the entities referred to in Article 3 of the Agreement respecting any distribution limitations that are applied to Canadian classified information approved for release to the EU, including any caveats restricting distribution to specific addresses;

(ii) the EU will send all correspondence containing classified information through the Mission of Canada to the European Union. Canadian Participants will notify the EU Participants of the relevant organisations that will be in charge of receiving classified information and of the addresses of those organisations;

2. the Parties will notify each other of any changes to their respective organisations, including addresses, relevant to the transmission of classified information between the Parties;

3. the Parties will transmit classified information physically through their respective diplomatic channels;

4. each Party will use authorised couriers to transmit classified information to the other Party. Upon presentation of the appropriate courier certificate, the other Party will grant such couriers access to the building(s) they need to visit to deliver and collect the documents. The Parties will appropriately security-clear the couriers whenever the information to be transmitted is classified CONFIDENTIEL UE/EU CONFIDENTIAL, Canadian CONFIDENTIAL or CONFIDENTIEL or above. When the information to be transmitted is Canadian PROTECTED C or PROTÉGÉ C information, EU Participants' couriers will have undergone an EU record of good conduct check unless a security clearance at the level of SECRET UE/EU SECRET or above has already been granted;

5. the Parties will transmit information in accordance with the following provisions:

(i) documents or media containing classified information will be transmitted in double, sealed envelopes, the innermost envelope bearing only the classification of the documents or other media and the address of the intended recipient, and the outer envelope bearing the address of the recipient, the address of the sender, and the registry number, if applicable, but no indication of the classification;

(ii) the envelope will be transmitted according to the prescribed procedures of the providing Party;

(iii) receipts will be prepared for envelopes containing classified documents or media transmitted between the Parties, and a receipt for the enclosed documents or media will be signed by the intended recipient and returned to the providing Party.

IX. RELEASE OF CLASSIFIED INFORMATION TO CONTRACTORS OR PROSPECTIVE CONTRACTORS

The Participants understand that for the purposes of implementing Article 8 of the Agreement:

1. the authority in charge of industrial security matters and the provisions in this Section for Canada, is the Director, International Industrial Security and Designated Security Authority, Industrial Security Sector, PWGSC;

2. the Parties will ensure that information classified as CONFIDENTIEL UE/EU CONFIDENTIAL or Canadian CONFIDENTIAL or CONFIDENTIEL and above that is related to industrial security is transferred only by diplomatic courier, by military courier, or by other means jointly approved by them. If that information is too voluminous to be transferred by a diplomatic courier or a military courier, the Parties will jointly draft a transportation plan that describes how they intend to transfer the classified information. That plan may include the type of transport, the route, and the type of escort for the classified information;

3. before information classified CONFIDENTIEL UE/EU CONFIDENTIAL or Canadian CONFIDENTIAL or CONFIDENTIEL and above, is released to contractors of the receiving Party in accordance with Article 8 of the Agreement, the providing Party will request confirmation from the receiving Party that such contractors and their personnel requiring access to classified information hold an appropriate personnel security clearance, and that such contractors have committed, as part of their contractual obligations, to provide an adequate level of protection to classified information within their facilities;

4. the Parties will facilitate visits to their industrial and governmental facilities that are related to contracts, provided that the visit is authorised by both Parties. Visits at the RESTREINT UE/EU RESTRICTED or PROTECTED A or PROTÉGÉ A or PROTECTED B or PROTÉGÉ B information level will be coordinated directly with the respective facility security officer;

5. the security requirements for the provision of classified information to a contractor or prospective contractor will be set out in the Security Aspects Letter for the EU and Security Requirements Check List for Canada and Program/Project Security Instructions, as appropriate.

X. LOSS, COMPROMISE OR DISCLOSURE WITHOUT AUTHORISATION OF CLASSIFIED INFORMATION

The Participants understand that:

1. if the receiving Party knows or has reasonable grounds to believe that classified information received from the providing Party has been compromised, lost, or disclosed without authorisation, the receiving Party will immediately inform the providing Party and, as soon as is practicable, will send the results of the investigation and information regarding measures taken to prevent recurrence as provided for in Article 12 of the Agreement. The report will be sent:

(i) by the GSCDSS, the ECSD or the EEAS DGBA.IBS to Canada, for Canadian classified and protected information;

(ii) by Canada to the GSCDSS, the ECSD or the EEAS DGBA.IBS, as appropriate, for EU classified information;

2. the Parties will deal with any security breach or suspected security breach concerning classified information that is committed by individuals in accordance with the applicable laws, rules and regulations of the receiving Party.

XI. SECURITY CONSULTATIONS AND ASSESSMENT VISITS

1. The Participants will facilitate the reciprocal security consultations and assessment visits referred to in Article 11(2) of the Agreement to ensure that information released under the Agreement is properly protected. Such visits will be subject to prior mutual decision between the Participants.

2. The Participants will implement the standards described in this Arrangement. Each Participant will conduct internally the necessary checks to verify that security measures have been taken in accordance with this Arrangement.

XII. ELECTRONIC HANDLING

Any use of CIS for handling, storing or transmitting classified information exchanged under the Agreement, including stand-alone computers, photocopiers, scanners, electronic storage media and mobile devices, constitutes electronic handling.

XIII. IMPLEMENTATION AND REVIEW

1. The Participants will monitor the release and exchange of classified information under the Agreement.

2. Upon request, each Participant will provide information about its security standards, procedures and practices for safeguarding classified information.

3. This Arrangement will be implemented from the date of the entry into force of the Agreement and in accordance with Article 11(3) of the Agreement.

4. The Participants may review this Arrangement upon the request of one of them. The Participants will review this Arrangement in the event of the Agreement being reviewed in accordance with Article (16)3 of the Agreement.

Signed in duplicate, at ……., on …….. in the English and French languages, both versions being equally valid.

For the Department of Foreign Affairs, Trade and Development of Canada

For the Department of Public Works and Government Services of Canada

For the Directorate of Safety and Security of the General Secretariat of the Council of the European Union

For the Security Directorate of the European Commission

For the European External Action Service Security Department