No. 54309*

Switzerland
and
Singapore

Arrangement between the Ministry of Defence of the Republic of Singapore and the Federal Department of Defence, Civil Protection and Sport of the Swiss Confederation concerning the protection of classified information exchanged in the field of defence. Solothurn, 19 May 2016

Entry into force: *25 July 2016 by notification, in accordance with article 14*

Authentic text: *English*

Registration with the Secretariat of the United Nations: *Switzerland, 28 February 2017*

*No UNTS volume number has yet been determined for this record. The Text(s) reproduced below, if attached, are the authentic texts of the agreement /action attachment as submitted for registration and publication to the Secretariat. For ease of reference they were sequentially paginated. Translations, if attached, are not final and are provided for information only.

Suisse
et
Singapour

Arrangement entre le Ministère de la Défense de la République de Singapour et le Département fédéral de la défense, de la protection de la population et des sports de la Confédération suisse concernant la protection des informations classifiées échangées dans le domaine de la défense. Soleure, 19 mai 2016

Entrée en vigueur : *25 juillet 2016 par notification, conformément à l'article 14*

Texte authentique : *anglais*

Enregistrement auprès du Secrétariat de l'Organisation des Nations Unies : *Suisse, 28 février 2017*

*Aucun numéro de volume n'a encore été attribué à ce dossier. Les textes disponibles qui sont reproduits ci-dessous sont les textes originaux de l'accord ou de l'action tels que soumis pour enregistrement. Par souci de clarté, leurs pages ont été numérotées. Les traductions qui accompagnent ces textes ne sont pas définitives et sont fournies uniquement à titre d'information.

[ENGLISH TEXT – TEXTE ANGLAIS]

Arrangement

between

The Ministry of Defence of the Republic of Singapore

and

The Federal Department of Defence, Civil Protection and Sport of the Swiss Confederation

concerning

The Protection of Classified Information

exchanged

in the

Field of Defence

INTRODUCTION

The Ministry of Defence of the Republic of Singapore and the Federal Department of Defence, Civil Protection and Sport of the Swiss Confederation, hereafter referred to as the Parties,

Recognising the interest and the common necessity to ensure the protection of any Classified Information in the defence and military fields exchanged between the Parties and through government and private entities mutually agreed to by both Parties in connection with cooperation agreements or contracts in the field of defence entered into between their government entities,

Having agreed to hold talks on defence and military related issues and to broaden and tighten mutual cooperation,

Realising that cooperation in the defence and military fields may require the exchange of Classified Information between Parties,

Recognising the need to establish mutually agreed procedures for the safeguarding of Classified Information in accordance with the laws and the regulations of the Parties,

Have agreed as follows

1. DEFINITIONS

The following terms are defined in the interest of clarity:

1.1 "Classified Information" means any classified item, be it in oral or visual communication of classified contents or the electrical or electronic transmission of classified information, or be it material. "Material" includes any letter, note, minute, report, memorandum, signal/message, sketch, photograph, film, map, chart, plan, notebook, stencil, carbon, typewriter ribbon, diskette, etc. or other form of recorded information (e.g. tape recording, magnetic recording, punched card, tape, etc.);

1.2 "Competent Security Authority (CSA) means the government authority responsible for Defence Security in each country.

1.3 "Contractor" means an individual or legal entity possessing the legal capability to undertake contracts.

1.4 "Contract" means an agreement between two or more parties creating and defining enforceable rights and obligations between the parties.

1.5 "Classified Contract" means a contract which contains or involves Classified Information.

1.6 "Facility" means a government establishment, premises of a company or other organisation in which Classified Information is utilised or stored.

1.7 "Security clearance" means a positive determination stemming from a vetting procedure in accordance with national laws and regulations stating that an individual or legal entity is eligible to have access to Classified Information up to a certain classification level.

1.8 "Need-to-know" means the necessity to have access to Classified Information in order to be able to perform official duties and tasks.

1.9 "Originating Party" means the Party that originates and releases the Classified Information to the other Party.

1.10 "Recipient Party" means the Party which receives the Classified Information from the Originating Party.

1.11 "Third Party" means a state, international organisation or any other entity which is not a Party to this Arrangement.

2. SECURITY CLASSIFICATIONS

2.1 The Parties agree that the following classification levels are equivalent and correspond to the security classification levels determined in their national laws and regulations.

IN THE REPUBLIC OF SINGAPORE	IN THE SWISS CONFEDERATION
SECRET	GEHEIM / SECRET / SEGRETO
CONFIDENTIAL	VERTRAULICH / CONFIDENTIEL / CONFIDENZIALE
RESTRICTED	INTERN / INTERNE / AD USO INTERNO

2.2 Classified Information received or generated by one of the Parties shall be granted protection in accordance with the equivalent security classification level, as stated in Article 2.1. In exceptional cases, either Party may ask the other to afford protection at a higher, but not at a lower level than the classification indicated.

2.3 The Originating Party shall notify the Recipient Party of any changes to the security classification of released Classified Information.

3. COMPETENT SECURITY AUTHORITIES

3.1 For the purpose of this Arrangement, the CSAs shall be:

In the Republic of Singapore

Military Security Department
Ministry of Defence
Singapore

In the Swiss Confederation

Federal Department of Defence, Civil Protection and Sport
Defence, Armed Forces Staff / Directorate for Information Security and Facility Protection (DISFP)
3003 Berne

3.2 The CSAs shall inform each other of the national laws and regulations in force for the protection of Classified Information and shall

exchange information about the security standards, procedures and practices for the protection of Classified Information, as well as on any subsequent amendments to the national laws and regulations for the protection of Classified Information.

3.3 The CSAs may hold consultations in order to ensure close cooperation and advise each other on the specific administrative or implementation aspects of the provisions of this Arrangement.

3.4 The respective CSA shall ensure the strict and binding adherence to this Arrangement by the Party and any private entity of the Party in accordance with its national laws and regulations.

4. RESTRICTIONS ON USE AND DISCLOSURE OF CLASSIFIED INFORMATION

4.1 The Recipient Party will not pass, disclose or use, or permit the disclosure or use of, any Classified Information transmitted by the Originating Party except for the purposes and within any limitations stated by or on behalf of the Originating Party, unless prior written consent is given to the contrary by the Originating Party.

4.2 The Recipient Party will take all steps legally available to it to keep Classified Information transmitted to it by the Originating Party free from disclosure under any legislative provision, unless the Originating Party consents to such disclosure. If it becomes probable that the Classified Information may have to be disclosed under any legislative provision, immediate notification will be given to the Originating Party and both Parties will consult about the consequences of such disclosure with a view to identifying and alleviating any likely harm to the Originating Party.

4.3 The Parties shall not use any Classified Information obtained or generated to the detriment or against the interests of the other Party.

4.4 Nothing in this Arrangement will be taken as an authority for or to govern the release, use, exchange or disclosure of information in which intellectual property rights exist, until specific written authorisation of the owner of these rights has first been obtained, whether the owner is one of the Parties or a Third Party.

5. PROTECTION OF CLASSIFIED INFORMATION

5.1 The Originating Party shall:

a) Ensure that released Classified Information is marked with an appropriate national security classification marking according to Article 2.1;

b) Inform the Recipient Party of any conditions of release or limitations on the use of the Classified Information, as applicable.

5.2 The Recipient Party shall:

a) Afford to all Classified Information received from the other Party the same degree of security protection that is afforded to Classified Information of an equivalent classification originated by the Recipient Party, in accordance with its national laws and regulations;

b) Ensure that Classified Information is marked with its own classification in accordance with Article 2.1 above;

c) Ensure that the classifications are not altered, except as authorised in writing by the Originating Party;

d) Return the information to the Originating Party, or destroy the information in accordance with the procedures of the Recipient Party for the destruction of Classified Information, when the information is no longer required;

e) Not pass or disclose any Classified Information received under the provisions of this Arrangement to a Third Party, without the prior written permission of the Originating Party.

6. ACCESS TO CLASSIFIED INFORMATION

6.1 Access to Classified Information will be limited to those persons who have a need-to-know, and who have been security cleared by the Recipient Party's CSA, in accordance with their national standards, to the level appropriate to the classification of information to be accessed.

6.2 Both Parties are committed not to rely on this Arrangement to obtain access to any Classified Information which the other Party has obtained from a Third Party.

7. TRANSFER OF CLASSIFIED INFORMATION

7.1 Information classified CONFIDENTIAL and SECRET will be transmitted between the two Parties in accordance with the national security laws and regulations of the Originating Party. The normal route will be through official diplomatic channels, but other arrangements may be established, if mutually acceptable to both Parties.

7.2 Information classified RESTRICTED will be transmitted in accordance with the national security laws and regulations of the Originating Party which may include the use of commercial couriers.

7.3 Classified Information shall not be transmitted via the internet. Subject to mutual consent, the Parties may agree to permit the transmission of Classified Information by electronic means. The detailed arrangements for the security procedures and/or encryption to be applied to any such transmission for the purpose of secure transmission shall be mutually determined by the CSAs.

8. VISITS

8.1 The prior approval of the CSA of the host Party will be required in respect of visitors, including those on deployment from the other Party's country, where access to Classified Information or a Facility is necessary. Requests for such visits will be submitted in writing to the respective CSA.

8.2 Requests shall include the following information:

8.2.1 Name of proposed visitor, date and place of birth, nationality and passport number/identity card number;

8.2.2 Official position of the visitor together with the name of the Facility which he represents or to which he belongs;

8.2.3 Appropriate security clearance assurance in writing on the basis of the Personnel Security Clearance (PSC),

8.2.4 Name and address of the Facility to be visited;

8.2.5 Name and official position of the person(s) to be visited, if known;

8.2.6 Purpose of visit;

8.2.7 Dates and duration of the visit. In cases of recurring visits, the total period covered by the visits should be stated.

8.3 Visit requests should be submitted to the CSA of the host Party in accordance with normal procedures of the host Party. Short notice visits can be arranged in urgent cases by special mutually determined arrangements.

8.4 In cases involving a specific project or a particular Contract it may, subject to the approval of both Parties, be possible to establish Recurring Visitors Lists. These lists will be valid for an initial period not exceeding 12 months and may be extended for a further period of time (not to exceed 12 months) subject to the prior approval of the CSA of the host Party. They should be submitted in accordance with normal procedures of the host Party. Once the list has been approved, visit arrangements may be made directly between the Facilities involved in respect of listed individuals.

8.5 The Party which requested the visit will ensure that any information which may be provided to visiting personnel will be treated by them as if such information had been furnished pursuant to the provisions of this Arrangement.

8.6 All visitors will comply with the security laws and regulations of the host Party.

9. CLASSIFIED CONTRACTS

9.1 When placing a Classified Contract with a Contractor in the other Party's country, the Originating Party may request assurance in writing from the CSA of the other Party that the proposed Contractor holds the appropriate PSC and Facility Security Clearance (FSC) to the level required for the Contract. The assurance will carry a responsibility that the security conduct by the cleared Contractor will be in accordance with the other Party's national security laws and regulations and this will be monitored by its CSA.

9.2 The respective CSA will ensure that its Contractors, prospective Contractors, sub-Contractors and the Facility(ies) comply with its security procedures. The security procedures will be in accordance with the national laws and regulations of the contracting Party.

9.3 The CSA of the Originating Party will ensure that Contractors which are provided with Classified Information during pre-Contract enquiries and Contractors that receive Classified Contracts placed as a consequence of pre-Contract enquiries are aware of the following:

9.3.1 The definition of the term "Classified Information" and of the equivalent levels of security classification of the two Parties in accordance with the provisions of this Arrangement.

9.3.2 The name(s) of the CSA of each of the two Parties empowered to authorise the release and to coordinate the safeguarding of Classified Information related to the Classified Contract.

9.3.3 The methods or means to be used for the secure transfer of the Classified Information.

9.3.4 The procedures and mechanisms for communicating the changes that may arise in respect of Classified Information.

9.3.5 The procedures for the approval of visits, access or inspection by personnel of one Party to Facilities in the other Party's country that are covered by the Classified Contract.

9.3.6 The obligation that the Contractor will disclose the Classified Information only to a person who has previously been

cleared for access, with a need-to-know, and who is employed on or engaged in the carrying out of the Classified Contract.

9.4 Each Classified Contract will contain guidance on the security requirements and on the classification of each aspect/element of the Classified Contract. The guidance must identify each classified aspect of the Classified Contract, or any classified aspect which is to be generated as a consequence of the Classified Contract, and allocate to it a specific security classification. Changes in the requirements or to the aspects/elements will be notified as and when necessary and the Originating Party will notify the Recipient Party when all the information has been declassified.

10. SECURITY ASSURANCES

10.1 When requested, the CSA will establish the security clearance status of the Facility/individual by forwarding a FSC/PSC assurance if the Facility/individual is already cleared. If the Facility/individual does not have a security clearance, or the clearance is at a lower security level than that which has been requested, notification will be sent that the FSC/PSC assurance cannot be issued immediately, but that action is being taken to process the request. Following successful enquiries, an FSC/PSC will be provided.

10.2 An FSC or PSC is not required for access to information classified RESTRICTED and below.

10.3 A Facility which is deemed by the CSA, in the country in which it is registered, to be under the ownership, control or influence of a third country whose aims are not compatible with that of the host government is not eligible for FSC assurance and the requesting CSA will be notified.

10.4 If either CSA learns of any information which raises doubts about the suitability of an individual for whom a PSC assurance has been issued, it will notify the other CSA of the nature of the information and the action it intends to take, or has taken. Either CSA may request a review of any PSC assurance which has been furnished earlier by the other CSA, provided that the request is accompanied by a reason. The requesting CSA will be notified of the results of the review and any subsequent action.

10.5 If information becomes available which raises doubts about the suitability of a cleared Facility in the Recipient Party's country to continue to have access to Classified Information, then details of this information will be promptly notified to the CSA to allow an investigation to be carried out.

10.6 If either CSA suspends or takes action to revoke a PSC, or suspends or takes action to revoke access which is granted to a national of the other Party's country based upon a security clearance, the other Party will be notified and given reasons for such an action.

10.7 Each CSA may request the other to review any FSC assurances, provided that their request is accompanied by the reasons for seeking the review. Following the review, the requesting Authority will be notified of the results and will be provided with facts supporting any decisions taken.

10.8 If either CSA suspends or takes action to revoke a FSC which it has granted, the other Party would be informed and given the reasons for such a decision.

10.9 If required by the other Party, each CSA will cooperate in reviews and investigations concerning security clearances.

11. LOSS OR COMPROMISE

11.1 In the event of loss or unauthorised disclosure of information classified CONFIDENTIAL or SECRET, or suspicion thereof, the CSA of the Recipient Party shall immediately inform the CSA of the Originating Party in writing.

11.2 An immediate investigation will be carried out by the Recipient Party (with assistance from the Originating Party if required) in accordance with its national laws and regulations for the protection of Classified Information. The Recipient Party will inform the Originating Party about the circumstances, measures adopted and outcome of the investigation as soon as is practicable.

11.3 In the event of loss or unauthorised disclosure of information classified RESTRICTED, or suspicion thereof, the CSA of the Recipient

shall inform the CSA of the Originating Party in writing after the investigations are complete.

11.4 When an actual or suspected loss or unauthorised disclosure of Classified Information has occurred in a third country, the CSA of the Recipient Party shall take the actions referred to in Articles 11.1, 11.2 and 11.3, if possible.

12. COSTS

Any costs incurred in the application of the security provisions of this Arrangement will be borne by the Party providing the services.

13. DISPUTES

Any disputes regarding the interpretation or implementation of this Arrangement shall be resolved by negotiations between the Parties and not be referred to a national or international tribunal or third party for resolution. Meanwhile, the Parties shall continue to fulfil the provisions set forth in this Arrangement.

14. FINAL PROVISIONS

14.1 The Parties shall notify each other in writing of the completion of the national measures necessary for the entry into force of this Arrangement. This Arrangement shall enter into force on the date of the receipt of the latest written notification.

14.2 This Arrangement is concluded for an indefinite period of time. It may be amended by mutual written consent of the Parties. Amendments shall enter into force in accordance with the provisions of Article 14.1.

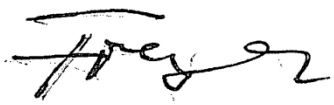
14.3 Either Party may terminate this Arrangement by written notification delivered to the other Party through diplomatic channels, observing a period of notice of six (6) months. If this Arrangement is terminated, all Classified Information provided or generated under this Arrangement shall continue to be handled and protected by the Parties in

accordance with the provisions of this Arrangement, notwithstanding its termination. In the event of termination, solutions to any outstanding problems will be sought via consultation.

14.4 This Arrangement shall supersede and replace all protection of classified information provisions in other agreements in the field of defence previously entered into between the Parties.

Signed in duplicate in the English Language.

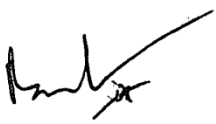
For the Federal Department of Defence, Civil Protection and Sport of the Swiss Confederation



Urs Freiburghaus

Head of Directorate for Information Security and Facility Protection

For the Ministry of Defence of the Republic of Singapore



Brigadier General Paul Chew

Director Military Security

Place and Date: Solothurn, 19.5.16

[TRANSLATION – TRADUCTION][1]

Accord

entre le Département fédéral de la défense, de la protection de la population et des sports de la Confédération suisse et le Ministère de la Défense de la République de Singapour concernant la protection des informations classifiées échangées dans le domaine de la défense

Conclu le 19 mai 2016
Entré en vigueur par échange de notes le 25 juillet 2016

Introduction

Le Département fédéral de la défense, de la protection de la population et des sports de la Confédération suisse et le Ministère de la Défense de la République de Singapour,
ci-après dénommés «Parties contractantes»,

reconnaissant l'intérêt et la nécessité commune d'assurer la protection de toute information classifiée concernant la défense et les affaires militaires échangée entre les Parties contractantes et par l'intermédiaire d'organismes gouvernementaux ou privés mutuellement reconnus dans le cadre d'accords de coopération ou de contrats concernant la défense conclus par leurs instances gouvernementales,

ayant convenu de s'entretenir sur des sujets concernant la défense et les affaires militaires et d'élargir et de renforcer leur coopération mutuelle,

sachant que la coopération en matière de défense et d'affaires militaires peut nécessiter l'échange d'informations classifiées entre les Parties contractantes,

reconnaissant la nécessité d'établir des procédures mutuellement reconnues pour la sauvegarde des informations classifiées conformément aux lois et réglementations des Parties contractantes,

ont convenu des dispositions suivantes:

[1] Translation provided by by the Government of Switzerland – Traduction fournie par par le Gouvernement suisse.

1. Définitions

La terminologie suivante est utilisée aux fins du présent Accord:

1.1 «Information classifiée» désigne tout objet classifié, qu'il s'agisse d'une communication orale ou visuelle au contenu classifié ou de la transmission électrique ou électronique d'un message classifié, ou d'un objet matériel. Par «objet matériel», on entend toute lettre, note, procès-verbal, rapport, mémorandum, signal ou message, croquis, photo, film, carte, schéma, plan, carnet de notes, stencil, carbone, ruban de machine à écrire, disquette, etc., ou autre forme d'information enregistrée (par ex., enregistrement sur bande, enregistrement magnétique, carte perforée, bande, etc.);

1.2 «Autorité de sécurité compétente» (ASC) désigne l'autorité gouvernementale responsable de la sécurité liée à la défense dans chaque pays;

1.3 «Entrepreneur» désigne une personne physique ou morale ayant la capacité juridique de conclure des contrats;

1.4 «Contrat» désigne tout accord entre au moins deux parties, qui crée ou définit des droits et obligations exécutoires entre celles-ci;

1.5 «Contrat classifié» désigne un contrat qui contient ou qui se rapporte à des informations classifiées;

1.6 «Etablissement» désigne soit une installation gouvernementale, soit les locaux d'une entreprise ou d'une autre organisation dans lesquels des informations classifiées sont utilisées ou entreposées;

1.7 «Habilitation de sécurité» désigne une décision positive faisant suite à une enquête de sécurité, conduite conformément aux lois et aux réglementations nationales, qui reconnaît à un individu ou à une personne morale le droit d'accéder à des informations classifiées d'un niveau déterminé;

1.8 «Besoin d'en connaître» désigne la nécessité d'avoir accès à des informations classifiées pour pouvoir accomplir des tâches et des devoirs officiels;

1.9 «Partie d'origine» désigne la Partie contractante qui émet les informations classifiées et les transmet à l'autre Partie contractante;

1.10 «Partie destinataire» désigne la Partie contractante à laquelle une information classifiée est transmise par la partie d'origine;

1.11 «Tierce partie» désigne tout Etat, organisation internationale ou autre instance qui n'est pas partie au présent Accord.

2. Echelons de classification

2.1 Les Parties contractantes conviennent de l'équivalence des échelons de classification suivants et de leur correspondance avec les échelons de classification définis dans leurs lois et réglementations nationales.

Pour la Confédération suisse	Pour la République de Singapour
GEHEIM / SECRET / SEGRETO	SECRET
VERTRAULICH / CONFIDENTIEL / CONFIDENZIALE	CONFIDENTIAL
INTERN / INTERNE / AD USO INTERNO	RESTRICTED

2.2 Les informations classifiées reçues ou émises par l'une ou l'autre des Parties contractantes se voient attribuer des échelons de classification équivalents conformément aux dispositions du ch. 2.1. Dans des cas exceptionnels, une Partie contractante peut demander à l'autre Partie contractante d'accorder une protection correspondant à l'échelon de classification supérieur, mais pas inférieur, à celui indiqué.

2.3 La partie d'origine informe la partie destinataire de toute modification de l'échelon de classification des informations classifiées transmises.

3. Autorités de sécurité compétentes

3.1 Pour le présent Accord, les autorités de sécurité compétentes (ASC) sont:

Pour la Confédération suisse

Le Département fédéral de la défense, de la protection de la population et des sports
Etat-major de l'armée / Sécurité des informations et des objets (SIO)
3003 Berne

Pour la République de Singapour

Département de la sécurité militaire
Ministère de la Défense
Singapour

3.2 Les ASC s'informent mutuellement des lois et réglementations nationales en vigueur en matière de protection des informations classifiées. De même, elles se tiennent mutuellement informées de leurs normes, procédures et pratiques nationales en matière de sécurité relatives à la protection des informations classifiées ainsi que de tout changement apporté ultérieurement au lois et réglementations nationales correspondantes.

3.3 Les ASC peuvent se consulter afin d'assurer leur étroite coopération et se conseiller mutuellement sur les aspects administratifs ou exécutoires spécifiques des dispositions du présent Accord.

3.4 Les ASC de chaque Partie contractante veillent à ce que la Partie contractante et tout organe privé en faisant partie adhèrent obligatoirement et rigoureusement au présent Accord conformément à leurs lois et réglementations nationales.

4. Restrictions d'utilisation et de transmission des informations classifiées

4.1 La partie destinataire ne transmet, ni ne divulgue, ni n'utilise, ni ne permet la divulgation ou l'utilisation des informations classifiées transmises par la partie d'origine, excepté aux fins et dans les limites définies par ou au nom de la partie d'origine, sans le consentement préalable et écrit de la partie d'origine.

4.2 La partie destinataire prend toutes les mesures légalement à sa disposition pour que les informations classifiées qui lui sont transmises ne soient pas divulguées en vertu d'une quelconque disposition législative, sauf si la partie d'origine y consent. S'il s'avère probable que les informations classifiées doivent être communiquées dans le cadre d'une disposition législative, une notification immédiate est envoyée à la partie d'origine et les deux Parties contractantes se consultent à propos des conséquences d'une telle divulgation en vue d'identifier et d'atténuer tout préjudice que pourrait subir la partie d'origine.

4.3 Aucune information classifiée, reçue ou émise, n'est utilisée par l'une des Parties contractantes au détriment de l'autre Partie contractante ou de ses intérêts.

4.4 Aucune disposition du présent Accord ne doit être considérée comme autorisant ou permettant d'autoriser la transmission, l'utilisation, l'échange ou la divulgation d'informations protégées par des droits de propriété intellectuelle sans le consentement préalable et écrit du propriétaire de ces droits, que ce dernier soit l'une des Parties contractantes ou une tierce partie.

5. Protection des informations classifiées

5.1 La partie d'origine:

a) garantit que les informations classifiées transmises portent le marquage de sécurité correspondant à l'échelon de classification approprié selon le droit national et conforme aux dispositions du ch. 2.1;

b) informe la partie destinataire de toute condition relative à la divulgation ou aux restrictions d'utilisation des informations classifiées, selon les cas.

5.2 La partie destinataire:

a) accorde à toutes les informations classifiées qu'elle reçoit de l'autre partie une protection équivalente à celle accordée à ses propres informations classifiées du même échelon, conformément à ses lois et réglementations nationales;

b) garantit que les informations classifiées portent un marquage approprié selon sa propre classification et conforme aux dispositions du ch. 2.1 ci-dessus;

c) garantit que les échelons de classification ne soient pas modifiés, à moins que la partie d'origine n'ait autorisé cette modification par écrit;

d) renvoie les informations classifiées à la partie d'origine, ou les détruit conformément aux pratiques adoptées par la partie destinataire pour la destruction d'informations classifiées, lorsque les informations ne sont plus nécessaires;

e) ne transmet ni ne communique à une tierce partie les informations classifiées qu'elle reçoit selon les termes du présent Accord sans l'accord préalable et écrit de la partie d'origine.

6. Accès aux informations classifiées

6.1 Seules ont accès aux informations classifiées les personnes ayant besoin d'en connaître, et à qui l'ASC de la partie destinataire a délivré, en conformité avec ses normes nationales, une habilitation de sécurité suffisante pour autoriser l'accès aux informations classifiées en question.

6.2 Les deux Parties contractantes s'engagent à ne pas utiliser le présent Accord pour obtenir l'accès à des informations classifiées que l'autre partie a obtenues d'une tierce partie.

7. Transmission d'informations classifiées

7.1 Les informations classifiées CONFIDENTIEL ou SECRET sont transmises entre les deux Parties contractantes conformément aux lois et réglementations nationales de la partie d'origine. La transmission s'effectue normalement par la voie diplomatique. D'autres arrangements sont possibles avec le consentement mutuel des deux Parties contractantes.

7.2 Les informations classifiées INTERNE sont transmises conformément aux lois et réglementations nationales de la partie d'origine, ce qui peut inclure l'utilisation de messageries commerciales.

7.3 Les informations classifiées ne doivent pas être transmises sur l'internet. Les informations classifiées peuvent être communiquées par voie électronique d'un commun accord entre les Parties contractantes. Les ASC déterminent d'un commun accord les modalités relatives aux procédures de sécurité et/ou de cryptage applicables à de telles transmissions.

8. Visites

8.1 Les visiteurs, y compris ceux qui sont détachés par l'autre Partie contractante, doivent avoir reçu l'autorisation préalable de l'ASC de la partie destinataire lorsqu'il leur est nécessaire d'avoir accès à des informations classifiées ou à un établissement. Les demandes d'autorisation de visite sont présentées par écrit à l'ASC concernée.

8.2 La demande de visite contient les renseignements suivants:

8.2.1 nom, date et lieu de naissance, nationalité et numéro du passeport ou de la carte d'identité du visiteur;

8.2.2 fonction officielle du visiteur et nom de l'établissement qu'il représente ou auquel il appartient;

8.2.3 habilitation de sécurité appropriée établie par écrit sur la base de l'habilitation de sécurité du personnel (HSP);

8.2.4 nom et adresse de l'établissement objet de la visite;

8.2.5 nom et fonction officielle des personnes auxquelles on rend visite, si c'est possible;

8.2.6 but de la visite;

8.2.7 dates et durée de la visite. En cas de visites répétées, la période totale couverte par les visites doit être indiquée, si c'est possible.

8.3 Les demandes de visite sont soumises à l'ASC de la partie destinataire conformément aux procédures normales de la partie destinataire. En cas d'urgence, un délai plus court peut être convenu mutuellement par accord spécial.

8.4 S'agissant d'un projet spécifique ou d'un contrat particulier, il est possible, sous réserve de l'approbation des deux Parties contractantes, de dresser des listes de visiteurs qui reviennent souvent. Ces listes sont valables pour une période initiale ne dépassant pas douze mois et qui peut être renouvelée pour une période supplémentaire ne dépassant pas douze mois, sous réserve de l'approbation préalable de l'ASC de la partie destinataire. Ces listes sont soumises conformément aux procédures normales de la partie destinataire. Une fois la liste approuvée, les établissements concernées règlent directement entre elles les modalités pratiques des visites pour ce qui concerne les personnes figurant sur la liste.

8.5 La Partie contractante qui a demandé la visite veille à ce que toutes les informations qui peuvent être fournies aux visiteurs soient traitées par ceux-ci comme des informations reçues conformément aux dispositions du présent Accord.

8.6 Tous les visiteurs respectent les lois et réglementations de sécurité de la partie destinataire.

9. Contrats classifiés

9.1 Lors de la conclusion d'un contrat classifié avec un entrepreneur dans le pays de l'autre partie, la partie d'origine peut obtenir de l'ASC de l'autre partie la garantie écrite que l'entrepreneur proposé détient les HSP et les habilitations de sécurité d'établissement (HSE) de l'échelon requis pour le contrat en question. L'habilitation de sécurité doit garantir que la conduite en matière de sécurité de l'entrepreneur habilité sera conforme aux lois et

règlementations de sécurité nationales de l'autre partie et que cela sera supervisé par son ASC.

9.2 Les ASC garantissent que leurs entrepreneurs, entrepreneurs potentiels, sous-traitants et établissements respectent leurs procédures de sécurité. Les procédures de sécurité doivent être conformes aux lois et réglementations nationales des Parties contractantes.

9.3 L'ASC de la partie d'origine garantit que les entrepreneurs qui reçoivent des informations classifiées lors des vérifications précontractuelles et les entrepreneurs qui obtiennent des contrats classifiés suite aux vérifications précontractuelles sont au courant des éléments suivants:

9.3.1 la définition du terme «information classifiée» et les échelons de classification équivalents des deux Parties contractantes conformément aux dispositions du présent Accord;

9.3.2 le(s) nom(s) de l'ASC de chacune des deux Parties contractantes habilitées à autoriser la diffusion de l'information et de coordonner la sauvegarde des informations classifiées liées au contrat classifié;

9.3.3 les méthodes et moyens utilisés pour la transmission sûre des informations classifiées;

9.3.4 Les procédures et mécanismes prévus pour la communication des changements susceptibles d'intervenir en relation avec les informations classifiées.

9.3.5 Les procédures d'approbation des visites, d'accès ou d'inspection par le personnel d'une Partie contractante dans le pays de l'autre Partie contractante qui sont prévues dans le contrat classifié.

9.3.6 l'obligation faite à l'entrepreneur de divulguer des informations classifiées seulement à une personne qui est habilitée à y accéder, qui a le besoin d'en connaître et qui est employée ou engagée pour l'exécution du contrat classifié.

9.4 Dans chaque contrat classifié figurent des directives sur les exigences de sécurité et sur la classification de chaque aspect ou élément du contrat classifié. Les directives identifient chacun des aspects classifiés du contrat ou tout autre aspect qui pourrait en découler et lui attribuent un échelon de classification spécifique. Les changements apportés aux exigences ou aux aspects/éléments doivent être notifiés, si nécessaire et au moment voulu. La partie d'origine avise la partie destinataire lorsque toutes les informations sont déclassifiées.

10. Garanties de sécurité

10.1 Sur demande, l'ASC établit l'état de sécurité de l'établissement ou de la personne en transmettant une HSE ou une HSP si l'établissement ou la personne est déjà habilité. Si l'habilitation de sécurité correspond à un échelon inférieur à celui qui a été demandé ou si l'habilitation de sécurité fait défaut,

il est notifié qu'une HSE ou une HSP ne peut pas être délivrée immédiatement et que des mesures sont prises à cet égard. Si les vérifications s'avèrent positives, une HSE ou une HSP sera délivrée.

10.2 Aucune HSE ou HSP n'est requise pour accéder à des informations classifiées INTERNE ou d'un échelon inférieur.

10.3 Aucune HSE n'est délivrée si l'ASC du pays selon les lois duquel un établissement est organisé estime que cet établissement est propriété, sous le contrôle ou l'influence d'un pays tiers poursuivant des buts incompatibles avec ceux du gouvernement hôte. L'ASC qui a présenté la demande d'HSE doit en être notifiée.

10.4 Si l'une ou l'autre des ASC prend connaissance de renseignements qui suscitent des doutes au sujet de l'aptitude d'un individu ayant reçu une HSP, elle avise l'autre ASC de la nature desdits renseignements ainsi que des mesures qu'elle entend prendre ou qu'elle a déjà prises. Chacune des ASC peut demander le réexamen de toute HSP délivrée précédemment par l'autre ASC, sous réserve que la requête soit motivée. L'ASC qui fait la demande est informée des résultats du réexamen ainsi que de toute mesure en découlant.

10.5 Si des renseignements nouvellement disponibles suscitent des doutes quant à l'opportunité qu'un établissement habilité du pays destinataire continue d'avoir accès à des informations classifiées, les détails de ces renseignements sont portés sans délai à la connaissance de l'ASC afin de lui permettre de faire une enquête.

10.6 Si l'une ou l'autre des ASC suspend ou prend des mesures pour révoquer une HSP, ou si elle suspend ou prend des mesures pour révoquer l'accès accordé à un citoyen du pays de l'autre Partie contractante sur la base d'une habilitation de sécurité, cette mesure et ses motifs sont portés à la connaissance de l'autre Partie contractante.

10.7 Chacune des ASC peut demander à l'autre ASC de réexaminer toute HSE, sous réserve que la requête soit motivée. L'ASC qui fait la demande est informée des résultats du réexamen ainsi que des faits servant de base à la décision prise.

10.8 Si l'une ou l'autre des ASC suspend ou prend des mesures pour révoquer une HSE qu'elle a délivrée, l'autre Partie contractante doit être informée de cette décision ainsi que de ses motifs.

10.9 Si l'autre Partie contractante le demande, chacune des ASC peut coopérer aux enquêtes et à l'examen concernant les habilitations.

11. Perte ou compromission

11.1 L'ASC de la partie destinataire informe immédiatement et par écrit l'ASC de la partie d'origine en cas de perte ou de compromission, ou de suspicion de perte ou de compromission, d'informations classifiées CONFIDENTIEL ou SECRET.

11.2 Une enquête immédiate est déclenchée par la partie destinataire (avec la participation de la partie d'origine si elle est demandée) conformément à ses lois et règlementations nationales en matière de protection des informations classifiées. La partie destinataire informe le plus tôt possible la partie d'origine des circonstances et des mesures adoptées ainsi que des résultats de l'enquête.

11.3 En cas de perte ou de compromission d'informations classifiées INTERNE, ou de doute à ce sujet, l'ASC de la partie destinataire informe l'ASC de la partie d'origine par écrit lorsque les investigations sont terminées.

11.4 En cas de perte avérée ou suspectée ou de compromission d'informations classifiées dans un pays tiers, l'ASC de la partie destinataire prend les mesures conformément aux dispositions contenues aux ch. 11.1, 11.2 et 11.3, si c'est possible.

12. Frais

Tous les frais exposés pour la mise en œuvre des dispositions de sécurité du présent Accord sont pris en charge par la Partie contractante qui fournit les services.

13. Différends

Tout différend relatif à l'interprétation et à l'application du présent Accord est résolu à l'amiable entre les Parties contractantes et n'est pas renvoyé devant un tribunal national ou international ou une tierce partie pour résolution. Entretemps, les Parties contractantes continuent à respecter les dispositions du présent Accord.

14. Dispositions finales

14.1 Chacune des Parties contractantes notifie à l'autre Partie contractante l'accomplissement des formalités nationales nécessaires à l'entrée en vigueur du présent Accord. La date de réception de la dernière notification écrite détermine l'entrée en vigueur du présent Accord.

14.2 Le présent Accord est conclu pour une durée indéterminée. Il peut être modifié sur la base d'un accord commun adopté par écrit par les Parties contractantes. Les modifications entrent en vigueur conformément aux dispositions du ch. 14.1.

14.3 Chaque Partie contractante peut résilier le présent Accord en notifiant sa décision de résiliation à l'autre Partie contractante par la voie diplomatique, moyennant un préavis de six (6) mois. Nonobstant la résiliation, les Parties contractantes continuent à traiter et à protéger toutes les informations classifiées échangées ou produites conformément au présent Accord. En cas de résiliation, la résolution des problèmes en suspens est opérée par le biais de consultations entre les parties.

14.4 Le présent Accord remplace toutes les dispositions concernant la protection des informations classifiées convenues précédemment dans un accord signé par les Parties contractantes dans le domaine de la défense.

Signé en deux exemplaires en langue anglaise.

Pour le Département fédéral de la défense,
de la protection de la population et des sports
de la Confédération suisse:

Urs Freiburghaus
Chef Protection des informations et des objets

Pour le
Ministère de la Défense
de la République de Singapour:

Brigadier Paul Chew
Chef Sécurité militaire

ARRANGEMENT ENTRE LE MINISTÈRE DE LA DÉFENSE DE LA RÉPUBLIQUE DE SINGAPOUR ET LE DÉPARTEMENT FÉDÉRAL DE LA DÉFENSE, DE LA PROTECTION DE LA POPULATION ET DES SPORTS DE LA CONFÉDÉRATION SUISSE CONCERNANT LA PROTECTION DES INFORMATIONS CLASSIFIÉES ÉCHANGÉES DANS LE DOMAINE DE LA DÉFENSE

INTRODUCTION

Le Ministère de la défense de la République de Singapour et le Département fédéral de la défense, de la protection de la population et des sports de la Confédération suisse, ci-après dénommés les Parties,

Reconnaissant l'intérêt et la nécessité commune d'assurer la protection de toute information classifiée dans les domaines de la défense et militaire échangée entre les Parties et par l'intermédiaire d'entités gouvernementales et privées mutuellement agréées par les deux Parties dans le cadre d'accords de coopération ou de contrats dans le domaine de la défense conclus entre leurs entités gouvernementales,

Ayant convenu de tenir des discussions sur les questions militaires et les questions liées à la défense et d'élargir et de renforcer la coopération mutuelle,

Conscients que la coopération dans les domaines de la défense et militaire peut nécessiter l'échange d'informations classifiées entre les Parties,

Reconnaissant la nécessité d'établir des procédures mutuellement convenues pour la sauvegarde des informations classifiées, conformément aux lois et aux règlements des Parties,

Sont convenus de ce qui suit :

1. DÉFINITIONS

Les termes suivants sont définis dans un souci de clarté :

1. 1Le terme « information classifiée » désigne tout article classifié, qu'il s'agisse de la communication orale ou visuelle de contenus classifiés ou de la transmission électrique ou électronique d'informations classifiées, ou de matière. Le terme « matière » désigne toute lettre, note, photographie, carte, disquette et tout procès-verbal, rapport, mémorandum, signal/message, croquis, film, graphique, plan, carnet, pochoir, carbone, ruban de machine à écrire, etc. ou toute autre forme d'information enregistrée (par exemple, enregistrement sur bande, enregistrement magnétique, carte perforée, ruban, etc.).

1. 2Le terme « agence de sécurité compétente » désigne l'autorité gouvernementale responsable de la sécurité de la défense dans chaque pays.

1. 3Le terme « contractant » désigne toute personne physique ou morale possédant la capacité juridique de conclure des contrats.

1. 4Le terme « contrat » désigne un accord entre deux ou plusieurs parties qui crée et définit des droits et des obligations exécutoires entre elles.

1. 5Le terme « contrat classifié » désigne un contrat qui prévoit des dispositions pour l'utilisation d'informations classifiées.

1. 6Le terme « installations » désigne un établissement gouvernemental, les locaux d'une société ou d'une autre organisation dans lesquels des informations classifiées sont utilisées ou stockées.

1. 7Le terme « habilitation de sécurité » désigne la détermination positive résultant d'une procédure d'agrément diligentée conformément aux lois et réglementations nationales, qui garantit qu'une personne physique ou morale peut avoir accès à des informations classifiées jusqu'à un certain niveau de classification.

1. 8Le terme « besoin d'en connaître » désigne la nécessité d'accéder à des informations classifiées afin de pouvoir accomplir des fonctions et des tâches officielles.

1. 9Le terme « Partie d'origine » désigne la Partie qui communique ou transmet l'information classifiée à l'autre Partie.

1. 10Le terme « Partie destinataire » désigne la Partie qui reçoit des informations classifiées de la Partie d'origine.

1. 11Le terme « tierce partie » désigne un État, une organisation internationale ou toute autre entité qui n'est pas partie au présent Arrangement.

2. CLASSIFICATIONS DE SÉCURITÉ

2. 1Les Parties conviennent que les niveaux de classification de sécurité suivants sont équivalents et correspondent aux niveaux de classification de sécurité spécifiés dans leur droit interne. POUR LA RÉPUBLIQUE DE SINGAPOUR	POUR LA CONFÉDÉRATION SUISSE
SECRET	GEHEIM / SECRET / SEGRETO
CONFIDENTIAL	VERTRAULICH / CONFIDENTIEL / CONFIDENZIALE
RESTRICTED	INTERN / INTERNE / AD USO INTERNO

2. 2Les informations classifiées reçues ou générées par l'une des Parties bénéficient d'une protection conformément au niveau de classification de sécurité équivalent, comme indiqué à l'article 2.1. Dans des cas exceptionnels, chaque Partie peut demander à l'autre d'accorder une protection à un niveau supérieur, mais non inférieur, au niveau de classification indiqué.

2. 3La Partie d'origine informe la Partie destinataire de toute modification apportée au niveau de classification de sécurité de l'information classifiée transmise.

3. AUTORITÉS DE SÉCURITÉ COMPÉTENTES

3. 1.Aux fins du présent Arrangement, les autorités de sécurité compétentes sont :

Pour la République de Singapour

Le Département de la sécurité militaire du Ministère de la défense de Singapour

Pour la Confédération suisse

Le Département fédéral de la défense, de la protection de la population et des sports, État-major de l'armée / la Direction de la sécurité de l'information et de la protection des installations 3003 Berne

3. 2.Les autorités de sécurité compétentes s'informent mutuellement des lois et des réglementations nationales en vigueur pour la protection des informations classifiées et s'échangent des informations sur les normes, procédures et pratiques de sécurité pour la protection des informations classifiées, ainsi que sur toute modification ultérieure des lois et de la réglementation nationales pour la protection des informations classifiées.

3. 3.Les autorités de sécurité compétentes peuvent organiser des consultations en vue d'assurer une coopération étroite et de se conseiller mutuellement sur les aspects administratifs ou de mise en œuvre spécifiques des dispositions du présent Arrangement.

3. 4.Les autorités de sécurité compétentes veillent au respect strict et contraignant du présent Arrangement par la Partie et toute entité privée de la Partie, conformément à ses lois et réglementations nationales.

4. RESTRICTIONS À L'EXPLOITATION ET À LA DIVULGATION DES INFORMATIONS CLASSIFIÉES

4. 1 La Partie destinataire ne peut transmettre, divulguer ou utiliser, ni permettre la divulgation ou l'utilisation de toute information classifiée transmise par la Partie d'origine sans le consentement écrit préalable de cette dernière, à des fins autres que celles indiquées par la Partie d'origine ou en son nom, et dans les limites énoncées par la Partie d'origine.

4. 2 La Partie destinataire prend toutes les mesures qui lui sont légalement accessibles pour que les informations classifiées qui lui sont transmises par la Partie d'origine ne soient pas divulguées en vertu d'une disposition législative quelconque, à moins que la Partie d'origine n'y consente. S'il devient probable que les informations classifiées doivent être divulguées en vertu d'une disposition législative quelconque, la Partie d'origine en est immédiatement informée et les deux Parties se consultent sur les conséquences de cette divulgation en vue d'identifier et d'atténuer tout préjudice probable pour la Partie d'origine.

4. 3 Les Parties n'utilisent aucune information classifiée obtenue ou générée au détriment ou contre les intérêts de l'autre Partie.

4. 4 Aucune des dispositions du présent Arrangement n'est considérée comme autorisant la communication, l'utilisation, l'échange ou la divulgation d'informations sur lesquelles il existe des droits de propriété intellectuelle, ou comme régissant de telles activités, sans l'autorisation préalable et spécifique, donnée par écrit, du propriétaire de ces droits, que ledit propriétaire soit l'une des Parties ou une tierce partie.

5. PROTECTION DES INFORMATIONS CLASSIFIÉES

5. 1La Partie d'origine est tenue :

a) de veiller à ce que soient apposées sur les informations classifiées les marques de classification de sécurité nationale appropriées conformément aux dispositions de l'article 2.1 ;

b) d'informer la Partie destinataire de toute condition de divulgation ou de toute limitation à l'utilisation des informations classifiées, le cas échéant.

5. 2La Partie destinataire est tenue :

a) d'accorder à toutes les informations classifiées reçues de l'autre Partie le même niveau de protection que celui accordé à ses propres informations classifiées équivalentes, conformément à sa législation nationale ;

b) de veiller à ce que sa propre classification équivalente soit indiquée sur les informations classifiées, conformément à l'article 2.1 ci-dessus ;

c) d'assurer que les classifications ne sont pas modifiées, sauf sur autorisation écrite de la Partie d'origine ;

d) de renvoyer les informations à la Partie d'origine ou de les détruire conformément aux procédures de la Partie destinataire pour la destruction des informations classifiées, lorsque les informations ne sont plus nécessaires ;

e) de ne pas transmettre ni divulguer à un tiers les informations classifiées reçues en vertu des dispositions du présent Arrangement, sans l'autorisation écrite préalable de la Partie d'origine.

6. ACCÈS AUX INFORMATIONS CLASSIFIÉES

6. 1L'accès aux informations classifiées est limité aux personnes dont les fonctions exigent ledit accès et auxquelles une habilitation de sécurité du niveau correspondant à la classification des informations a été octroyée par l'autorité de sécurité compétente de la Partie destinataire désignée pour la sécurité, conformément à ses normes nationales.

6. 2Les deux Parties s'engagent à ne pas se fonder sur le présent Arrangement pour obtenir l'accès à toute information classifiée que l'autre Partie a obtenue d'un tiers.

7. TRANSFERT DES INFORMATIONS CLASSIFIÉES

7. 1Les informations classifiées CONFIDENTIAL et SECRET seront transmises entre les deux Parties conformément aux lois et réglementations nationales de sécurité de la Partie d'origine. La transmission se fait normalement par la voie diplomatique, mais d'autres dispositions peuvent être prises si elles sont mutuellement acceptables pour les deux Parties.

7. 2Les informations classifiées RESTRICTED sont transmises conformément aux lois et réglementations nationales de sécurité de la Partie d'origine, en ayant recours à des courriers commerciaux.

7. 3Les informations classifiées ne doivent pas être transmises via l'Internet. Sous réserve de consentement mutuel, les Parties peuvent autoriser la transmission d'informations classifiées par voie électronique. Les modalités détaillées des procédures de sécurité ou de cryptage à appliquer à toute transmission de ce type à des fins de transmission sécurisée sont déterminées d'un commun accord par les autorités de sécurité compétentes.

8. VISITES

8. 1Les visites devant être effectuées, y compris les visites des personnes détachées de l'autre pays, sont subordonnées à l'approbation préalable de l'autorité de sécurité compétente du pays d'accueil, lorsque l'accès est demandé aux informations classifiées ou aux installations. Les demandes d'autorisation pour ces visites sont soumises par écrit à l'autorité de sécurité concernée.

8. 2 Les demandes d'autorisation doivent comporter les informations suivantes :

8. 2.1le nom du visiteur proposé, la date et le lieu de naissance, la nationalité, le numéro de son passeport ou de sa carte d'identité ;

8. 2.2la fonction officielle du visiteur ainsi que le nom de l'établissement qu'il représente ou auquel il appartient ;

8. 2.3l'assurance d'habilitation de sécurité appropriée par écrit sur la base de l'habilitation personnelle de sécurité ;

8. 2.4le nom et l'adresse des installations à visiter ;

8. 2.5le nom et la fonction officielle de la ou des personnes à visiter, s'ils sont connus ;

8. 2.6l'objet de la visite ;

8. 2.7la date et la durée de la visite. Dans le cas de visites répétées, la période totale durant laquelle les visites sont effectuées doit être indiquée.

8. 3Les demandes de visite doivent être soumises à l'autorité de sécurité compétente de la Partie hôte conformément aux procédures normales de cette dernière. En cas d'urgence, des visites peuvent être organisées à court terme en vertu d'arrangements spéciaux convenus d'un commun accord.

8. 4Lorsqu'il s'agit d'un projet spécifique ou d'un contrat particulier, il est possible, sous réserve de l'approbation des deux Parties, d'établir la liste des visiteurs périodiques. Cette liste est valide pour une période initiale ne dépassant pas douze mois et peut être prorogée pour une autre période (ne dépassant pas douze mois), sous réserve de l'approbation préalable de l'autorité de sécurité compétente de la Partie hôte. Ces listes sont présentées conformément aux procédures de la Partie hôte. Une fois la liste approuvée, les modalités relatives à la visite peuvent être convenues directement entre les responsables des établissements concernés en fonction des personnes inscrites.

8. 5La Partie qui a demandé la visite veille à ce que toute information fournie aux visiteurs soit traitée par ces derniers comme ayant été fournie conformément aux dispositions du présent Arrangement.

8. 6Tous les visiteurs se conforment aux lois et réglementations nationales de sécurité de la Partie hôte.

9. CONTRATS CLASSIFIÉS

9. 1Lorsqu'elle conclut un contrat classifié avec un contractant situé dans le pays de l'autre Partie, la Partie d'origine peut demander à l'autorité de sécurité compétente de l'autre Partie l'assurance écrite que le contractant proposé détient l'habilitation de sécurité et l'habilitation de sécurité des installations appropriées au niveau requis pour le contrat. L'assurance atteste que le contractant habilité applique des mesures de sécurité conformes aux lois et réglementations nationales de sécurité de l'autre Partie, sous la surveillance de son autorité de sécurité compétente.

9. 2L'autorité de sécurité compétente veille à ce que ses contractants, ses contractants potentiels, ses sous-traitants et les installations se conforment à ses procédures de sécurité. Les procédures de sécurité sont conformes aux lois et réglementations nationales de la partie contractante.

9. 3L'autorité de sécurité compétente de la Partie d'origine veille à ce que les contractants qui reçoivent des informations classifiées au cours des enquêtes précontractuelles et les contractants qui reçoivent des contrats classifiés à la suite d'enquêtes précontractuelles soient informés des points suivants :

9. 3.1La définition du terme « informations classifiées » et des niveaux équivalents de classification de sécurité des deux Parties, conformément aux dispositions du présent Arrangement.

9. 3.2Le nom de l'autorité de sécurité compétente de chacune des deux Parties habilitée à autoriser la divulgation des informations classifiées ainsi qu'à coordonner la sauvegarde des informations classifiées faisant l'objet du contrat classifié.

9. 3.3Les méthodes ou les moyens à utiliser pour le transfert sécurisé des informations classifiées.

9. 3.4Les procédures et mécanismes de communication des changements qui peuvent survenir à l'égard des informations classifiées.

9. 3.5Les procédures d'approbation des visites, de l'accès ou de l'inspection par le personnel d'une Partie des installations de l'autre Partie qui sont couvertes par le contrat classifié.

9. 3.6L'obligation pour le contractant de ne divulguer les informations classifiées qu'aux personnes dûment autorisées à accéder à ces informations, qui ont « besoin de connaître » et qui sont employées ou engagées dans l'exécution du contrat classifié.

9. 4 Chaque contrat classifié contient des dispositions concernant les exigences de sécurité et la classification de chacun de ses aspects ou éléments. Les dispositions doivent identifier chaque aspect classifié du contrat classifié, ou tout aspect classifié qui doit être généré en conséquence du contrat classifié, et lui attribuer une classification de sécurité spécifique. Les modifications apportées aux exigences ou aux aspects et éléments sont notifiées si nécessaire et la Partie d'origine notifie la Partie destinataire lorsque toutes les informations ont été déclassifiées.

10. ASSURANCES DE SÉCURITÉ

10. 1Sur demande, l'autorité de sécurité compétente établit le statut d'habilitation de sécurité de l'installation ou de la personne en transmettant une assurance d'habilitation de sécurité si l'installation ou la personne est déjà habilitée. Si tel n'est pas le cas ou si l'habilitation est d'un niveau de sécurité inférieur à celui qui a été demandé, l'autorité de sécurité compétente ayant demandé l'information est informée que l'assurance d'habilitation de sécurité ne peut être octroyée immédiatement mais que la procédure est en cours. Si la procédure aboutit, une habilitation personnelle de sécurité ou de sécurité des installations est délivrée.

10. 2Une habilitation personnelle de sécurité ou de sécurité des installations n'est pas nécessaire pour accéder à des informations classifiées RESTRICTED et inférieures.

10. 3Une installation, dans le pays où elle est enregistrée, considérée par l'autorité de sécurité compétente comme étant sous la propriété, le contrôle ou l'influence d'un pays tiers dont les objectifs ne sont pas compatibles avec ceux du gouvernement hôte n'est pas éligible à l'assurance d'habilitation de sécurité des installations et l'autorité de sécurité compétente ayant demandé l'information en est informée.

10. 4Si l'une des deux autorités de sécurité compétentes a connaissance d'une information qui soulève des doutes quant à l'aptitude d'une personne pour laquelle une assurance d'habilitation de sécurité a été délivrée, elle informe son homologue de la teneur de cette information et des mesures qu'elle entend prendre ou a prises. L'une ou l'autre des autorités de sécurité compétentes peut demander que toute habilitation de sécurité personnelle octroyée précédemment par l'autre autorité compétente soit réexaminée, à condition que cette demande soit accompagnée de motifs recevables. L'autorité de sécurité compétente qui en a fait la demande est informée des résultats de l'examen et de toute action subséquente.

10. 5Si l'on dispose d'informations qui soulèvent des doutes quant à l'aptitude d'une installation autorisée dans le pays de la Partie destinataire à continuer à avoir accès à des

informations classifiées, les détails de ces informations sont notifiés sans délai à l'autorité de sécurité compétente afin qu'une enquête soit menée.

10. 6Lorsque l'une ou l'autre autorité de sécurité compétente révoque une habilitation personnelle de sécurité ou prend des mesures en vue de la révoquer ou révoque l'autorisation d'accès accordée à un ressortissant de l'autre Partie bénéficiant d'une habilitation de sécurité ou prend des mesures pour révoquer cette autorisation, l'autre Partie est informée des mesures prises et des raisons qui les ont inspirées.

10. 7Chaque autorité de sécurité compétente peut demander à l'autre de réexaminer toute assurance d'habilitation de sécurité des installations, à condition que cette demande soit accompagnée de motifs recevables. À la suite de l'examen, l'autorité à l'origine de la demande est informée des résultats et des faits à l'appui de toute décision prise.

10. 8Si l'une ou l'autre des autorités de sécurité compétentes révoque une habilitation de sécurité des installations qu'elle a accordée ou prend des mesures en vue de la révoquer, l'autre Partie est informée des mesures prises et des raisons qui les ont inspirées.

10. 9Si l'autre Partie l'exige, chaque autorité de sécurité compétente coopérera aux examens et enquêtes concernant les habilitations de sécurité.

11. PERTE DES RENSEIGNEMENTS OU COMPROMISSION

11. 1En cas de perte ou de divulgation non autorisée d'informations classifiées CONFIDENTIAL ou SECRET, ou de soupçons à cet égard, l'autorité de sécurité compétente de la Partie destinataire en informe immédiatement par écrit l'autorité de sécurité compétente de la Partie d'origine.

11. 2La Partie destinataire ouvre immédiatement une enquête, le cas échéant avec l'assistance de la Partie d'origine, conformément à ses lois et réglementations nationales applicables à la protection des informations classifiées. La Partie destinataire informe dès que possible la Partie d'origine des circonstances de l'incident, des mesures prises et du résultat de l'enquête.

11. 3En cas de perte ou de divulgation non autorisée d'informations classifiées RESTRICTED, ou de soupçons à cet égard, l'autorité de sécurité compétente de la Partie destinataire en informe par écrit l'autorité de sécurité compétente de la Partie d'origine une fois l'enquête terminée.

11. 4 Lorsqu'une perte ou une divulgation non autorisée d'informations classifiées, réelle ou présumée, s'est produite dans un pays tiers, l'autorité de sécurité compétente de la Partie destinataire prend les mesures visées aux articles 11.1, 11.2 et 11.3, si possible.

12. COÛTS

Tous les coûts encourus en application des dispositions de sécurité du présent Arrangement sont à la charge de la Partie qui fournit les services.

13. DIFFÉRENDS

Tout différend relatif à l'interprétation ou à la mise en œuvre du présent Arrangement est résolu par voie de négociations entre les Parties et n'est soumis à un tribunal national ou international, ni à une tierce partie pour règlement. Entre-temps, les Parties continuent d'appliquer les dispositions énoncées dans le présent Arrangement.

14. DISPOSITIONS FINALES

14. 1Les Parties se notifient par écrit de l'accomplissement des procédures internes nécessaires à l'entrée en vigueur du présent Arrangement. Celui-ci entre en vigueur à la date de réception de la dernière notification écrite.

14. 2Le présent Arrangement est conclu pour une durée indéterminée. Il peut être modifié à tout moment sur accord écrit des Parties. Ces modifications entrent en vigueur conformément aux dispositions de l'article 14.1.

14. 3L'une ou l'autre des Parties peut dénoncer le présent Arrangement moyennant une notification écrite adressée à l'autre Partie par la voie diplomatique et en respectant une période de préavis de six mois. En cas de dénonciation du présent Arrangement, toutes les informations classifiées fournies ou générées dans le cadre de cet Arrangement continuent d'être traitées et protégées par les Parties conformément aux dispositions du présent Arrangement, nonobstant sa dénonciation. En cas de dénonciation, des solutions aux problèmes en suspens sont recherchées par voie de consultation.

14. 4 Le présent Arrangement annule et remplace toutes les dispositions relatives à la protection des informations classifiées figurant dans d'autres accords dans le domaine de la défense conclus précédemment entre les Parties.

FAIT en double exemplaire, en langue anglaise.

Pour le Département fédéral de la défense, de la protection de la population et des sports de la Confédération suisse :

URS FREIBURGHAUS,

Chef de la Direction de la sécurité de l'information et de la protection des installations

Pour le Ministère de la défense de la République de Singapour :

PAUL CHAUW,

Général de brigade

Directeur du département de la sécurité militaire