Session ordinaire 2018-2019

CC/CE P.V. IR 28

Commission des Institutions et de la Révision constitutionnelle

Procès-verbal de la réunion du 24 septembre 2019

Ordre du jour :

1. Approbation des projets de procès-verbal de la réunion jointe du 22 mai et de la réunion du 17 juillet 2019

2. 6030 Proposition de révision portant instauration d'une nouvelle Constitution
- Rapporteurs : Madame Simone Beissel, Monsieur Alex Bodry, Monsieur Léon Gloden, Monsieur Henri Kox

- Echange de vues sur la continuation des travaux

3. 6961 Projet de loi portant
1. création de l'Autorité nationale de sécurité et
2. modification
1) de la loi modifiée du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité ;
2) du Code pénal
- Rapporteur : Monsieur Eugène Berger

- Présentation et adoption d'une série d'amendements parlementaires

4. Examen de la résolution du Parlement des Jeunes du 11 mai 2019 sur le système électoral au Luxembourg

5. Divers

*

Présents : M. Guy Arendt, M. Marc Baum, Mme Simone Beissel, M. Eugène Berger, M. Alex Bodry, M. Mars Di Bartolomeo, M. Gast Gibéryen, M. Léon Gloden, Mme Martine Hansen, M. Henri Kox, M. Charles Margue, M. Gilles Roth

M. Sven Clement, observateur délégué

Mme Diane Adehm remplaçant M. Michel Wolter

M. Jacques Flies, Mme Anne Greiveldinger, M. Paul Jung, Mme Michèle Schummer, Mme Audrey Heinry, du Ministère d'Etat

Mme Carole Closener, de l'Administration parlementaire

Excusés : M. Marc Angel, M. Claude Wiseler, M. Michel Wolter

*

Présidence : M. Alex Bodry, Président de la Commission

*

1. Approbation des projets de procès-verbal de la réunion jointe du 22 mai et de la réunion du 17 juillet 2019

Les projets de procès-verbal de la réunion jointe du 22 mai et de la réunion du 17 juillet 2019 sont approuvés.

2. 6030 Proposition de révision portant instauration d'une nouvelle Constitution

Ce point est reporté à une réunion ultérieure.

3. 6961 Projet de loi portant
1. création de l'Autorité nationale de sécurité et
2. modification
1) de la loi modifiée du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité ;
2) du Code pénal

La présente réunion s'inscrit dans la suite des réunions du 14 décembre 2018, 15 janvier et 17 juillet 2019, consacrées à la présentation du projet de loi, à l'examen de l'avis du Conseil d'Etat et à la présentation de propositions d'amendements.

Conformément à leur demande, les membres de la Commission ont reçu par courrier électronique les précisions sur le cadre de référence international, au niveau de l'Union européenne et de l'OTAN (cf. textes repris en annexe).
Par ailleurs, les avis des chambres professionnelles et de la Commission consultative des Droits de l'Homme (CCDH) ont été demandés, et l'avis de la Commission nationale pour la protection des données (CNPD) a été reçu en date du 16 juillet 2019 (cf. doc. parl. 6961[7]).

La présentation PowerPoint (pour les détails de laquelle il est prié de se référer à l'annexe), commentée par le représentant du Ministère d'Etat, dresse un état des lieux du cadre légal actuel tel que défini par la loi modifiée du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité, ainsi que du cadre de référence international, et met en avant les objectifs du projet de loi sous rubrique.

Echange de vues

En réponse aux préoccupations exprimées par les membres de la Commission concernant les enquêtes de sécurité, les précisions suivantes sont apportées par les représentants du Ministère d'Etat :

- En ce qui concerne l'extension des enquêtes de sécurité à l'entourage proche du demandeur d'une habilitation, le nouveau paragraphe 6 de l'article 27, introduit par

amendement gouvernemental en 2018 (cf. doc. parl. 6961[2]), vise à conférer une assise légale nationale à une pratique prévue par les engagements internationaux (OTAN et UE) pris par le Luxembourg et consistant à inclure les personnes majeures faisant partie de la communauté de vie du demandeur d'une habilitation de sécurité dans le rayon de l'enquête de sécurité.

- La notion de « personne majeure faisant partie de l'entourage proche du demandeur d'une habilitation de sécurité » n'est pas définie plus en détail afin de laisser à l'ANS le soin de déterminer le cercle des personnes visées en fonction de la situation du demandeur d'une habilitation de sécurité. Alors qu'à l'heure actuelle, l'enquête concernant le demandeur englobe d'office, le cas échéant, les personnes faisant partie du même ménage ou habitant à la même adresse (conjoint, partenaire et enfants), sans qu'ils en soient informés et sans que leur consentement ne soit demandé, force est de constater que les autres personnes fréquentées régulièrement par le demandeur (dans un contexte privé ou professionnel) peuvent tout aussi bien influer sur les garanties que doit présenter le demandeur. De plus, de nouveaux modèles d'habitation ou de communauté de vie se sont développés, comme par exemple la colocation, de sorte que la définition de l'entourage proche s'en trouve modifiée.

- Cette extension est toutefois encadrée par des garde-fous.
  Ainsi le fait de soumettre l'enquête sur ces personnes à leur consentement préalable est de nature à limiter le champ d'action effectif de l'autorité nationale de sécurité en la matière.
  Par ailleurs, ces dispositions ne s'appliquent que dans le cadre des demandes d'habilitation de niveau « SECRET » ou « TRES SECRET ».
  En pratique, actuellement, c'est essentiellement dans le domaine de la défense que des entretiens sont susceptibles d'être tenus avec d'autres personnes que celles qui composent le ménage.

- La délivrance ou le renouvellement d'une habilitation de sécurité à une personne physique sont conditionnés par le fait que celle-ci présente des garanties suffisantes quant à sa discrétion, sa loyauté, sa fiabilité et son intégrité.

- Les critères d'appréciation sont définis au nouvel article 31 de la loi modifiée du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité. Il est précisé que ces critères découlent tous du cadre de référence de l'UE et de l'OTAN. Les critères d'appréciation peuvent également s'avérer utiles pour motiver des décisions de refus.

- L'ANS a accès aux données et aux renseignements listés sous l'article 28, et peut en faire usage pour autant que ces renseignements soient nécessaires pour l'appréciation des garanties précitées.

- Les entretiens menés par l'ANS dans le cadre des enquêtes de sécurité visent certes à recueillir des informations, mais aussi à éclairer les intéressés sur leurs obligations afin de mieux les protéger. S'il existe des trames pouvant servir de base pour les entretiens, il semble toutefois important de conserver un certain degré de flexibilité.

- Le traitement par l'ANS des informations collectées dans le cadre de ses missions est mis en œuvre conformément aux dispositions de la loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale.

- La pratique dans les autres Etats est variable : dans certains Etats, les autorités ont accès aux déclarations fiscales de l'intéressé. En Allemagne, le demandeur d'une

habilitation indique à l'autorité nationale cinq personnes, l'identité du postulant est vérifiée auprès de deux de ces personnes et trois personnes de référence sont interrogées, étant précisé que l'autorité nationale conserve néanmoins le droit d'interroger d'autres personnes.

- L'ANS reçoit, par an, entre 750 et 800 demandes d'octroi ou de renouvellement d'habilitations de sécurité qui concernent en totalité environ 2000 personnes.

- Le Premier Ministre décide de l'octroi ou du retrait d'une habilitation de sécurité, sur la base des résultats de l'enquête de sécurité menée par l'ANS. Toute décision motivée du Premier Ministre de refus ou de retrait d'une habilitation de sécurité est prise suite à un avis motivé d'une commission composée de trois fonctionnaires. La commission se prononce sur base du rapport d'enquête élaboré par l'ANS, le cas échéant du dossier intégral de l'enquête. La personne qui s'est vu refuser ou retirer l'habilitation de sécurité peut solliciter l'accès au dossier sur lequel est fondée sa décision.

- Enfin, la décision de refus ou de retrait peut faire l'objet d'un recours en annulation devant les juridictions administratives.

Il est proposé de continuer l'examen des propositions d'amendements lors d'une prochaine réunion.

4. Examen de la résolution du Parlement des Jeunes du 11 mai 2019 sur le système électoral au Luxembourg

Ce point est reporté à une réunion ultérieure.

5. Divers

Les prochaines réunions auront lieu :

- Le vendredi 11 octobre 2019 à 15h00
  Ordre du jour :
  - Projet de loi n°6961 – Présentation et adoption d'une série d'amendements parlementaires.

- Le mardi 15 octobre 2019 à 15h30
  Ordre du jour :
  - Proposition de révision n°6030 : Echange de vues sur la continuation des travaux
  - Examen de la résolution du Parlement des jeunes du 11 mai 2019 sur le système électoral au Luxembourg

Luxembourg, le 25 septembre 2019

Le Secrétaire-administrateur,
Carole Closener

Le Président de la Commission des Institutions et de la Révision constitutionnelle,
Alex Bodry

Annexes :
Annexe 1 : Textes concernant le cadre de référence international
Annexe 2 : Présentation PowerPoint « Projet de loi n°6961 »

PUBLICLY DISCLOSED - AC/35-WP(2010)0003 - MISE EN LECTURE PUBLIQUE

NATO OTAN
NORTH ATLANTIC COUNCIL
CONSEIL DE L'ATLANTIQUE NORD

NATO UNCLASSIFIED

7 January 2013

DOCUMENT
AC/35-D/2000-REV7

SECURITY COMMITTEE

DIRECTIVE on PERSONNEL SECURITY

Note by the Chairman

1. At Annex is the seventh revision of the Directive on Personnel Security which is published in support of the NATO Security Policy, C-M(2002)49. It is binding and mandatory in nature upon NATO member nations, commands and agencies. This document replaces AC/35-D/2000-REV6 which should be destroyed.

2. This revision reflects approved changes concerning NATO PSC Templates which are contained in Appendices 1 and 2.

3. This document has been approved by the Security Committee in Security Policy Format (AC/35-DS(2012)0005-AS1 (SP) and AC/35-WP(2012)0004-REV1 (SP) refer) and will be subject to periodic review.

(Signed) Stephen F. Smith

Annex: 1

Action Officer: Robert Keil, NOS/POB, Ext. 4084
Originator: [illegible]

NATO HQ - QG OTAN
DMS 1944228
DOCUMENT

PUBLICLY DISCLOSED - AC/35-WP(2010)0003 - MISE EN LECTURE PUBLIQUE

DIRECTIVE ON PERSONNEL SECURITY

INTRODUCTION

1. This Personnel Security directive is published by the Security Committee (AC/35) in support of Enclosure "C" to NATO Security Policy (C-M(2002)49). This directive contains mandatory provisions and also includes information which clarifies the meaning of those provisions. This directive addresses the following aspects :

(a) personnel security clearances:

(i) responsibilities;

(ii) the requirements for identifying positions requiring an appropriate personnel security clearance (PSC);

(iii) the criteria for assessing eligibility for a PSC;

(iv) the investigative requirements for NATO CONFIDENTIAL, NATO SECRET and COSMIC TOP SECRET security clearances;

(v) the requirements for the provision of PSCs to employees of NATO civil and military bodies;

(vi) the requirements for the revalidation of PSCs;

(vii) the procedures for addressing adverse information about an individual holding a PSC; and

(viii) the requirements for maintaining records of PSCs granted to individuals;

(b) security awareness and briefing of individuals;

(c) authorising access to NATO classified information – provisional appointments, one-time access, emergency access, and attendance at conferences and meetings;

(d) personnel security clearances for couriers, guards and escorts; and

(e) access by non-NATO nationals.

PUBLICLY DISCLOSED - AC/35-WP(2010)0003 - MISE EN LECTURE PUBLIQUE

PERSONNEL SECURITY CLEARANCE (PSC)

2. In accordance with the requirements of NATO Security Policy, there shall be an agreed standard of confidence about the loyalty, trustworthiness and reliability of all individuals granted access to, or whose duties or functions may afford access to, NATO classified information. In order to achieve this, individuals authorised to have access to information classified NC or above shall hold an appropriate personnel security clearance (PSC), valid for the duration of the authorised access, and have a need-to-know. Specifically:

(a) individuals hired directly by NATO civil and military bodies shall be granted a NATO Personnel Security Clearance (PSC) by the National Security Authority (NSA) or other competent authority of the individual's parent government;

(b) individuals who are employed by a military or civil agency of their government and who are seconded to a position for employment with a NATO civil or military body shall also be granted a NATO PSC by the NSA or other competent authority of the individual's parent government;

(c) individuals who are employed by a member nation or who are assigned by a member nation to its national delegation at NATO HQ must have been granted an appropriate and valid national and/or NATO PSC; and

(d) individuals who are contractors shall be granted a NATO Personnel Security Clearance (PSC) by the National Security Authority (NSA) or other competent authority. Further guidance concerning contractors can be found within Enclosure "G" to C-M(2002)49, and the supporting Directive on Industrial Security.

Responsibilities

3. NSAs or other competent national authorities are responsible for :

(a) carrying out security investigations on their nationals / citizens[1], and other persons within their jurisdiction, who require access to information classified NC or above, and for determining whether a PSC should be granted, denied or revoked. Standards of investigation shall be in accordance with the national investigative practices of NATO nations, but in no case shall these standards be lower than those prescribed in paragraphs 7 to 10 below;

(b) ensuring that PSC procedures are carried out with the knowledge and consent of the individual being investigated, to the extent that is permitted by national legislation;

(c) revalidating PSCs; and

(d) co-operating with other NSAs or other competent national authorities in carrying out their respective PSC procedures.

[1] There is provision in the industrial security context (Ref.: Directive on Industrial Security, Para: 43, 44) for a NSA/DSA to grant a PSC to an individual holding the nationality / citizenship of another NATO nation.

PUBLICLY DISCLOSED - AC/35-WP(2010)0003 - MISE EN LECTURE PUBLIQUE

4. NATO nations and the Heads of a NATO civil or military body are responsible for :

(a) identifying positions which require a PSC;

(b) authorising access to NATO classified information within their area of responsibility, including the situations described in paragraphs 28 to 37 below;

(c) ensuring that personnel security standards, as set forth herein, are met; and

(d) evaluating continuing eligibility of their staff for access to NATO classified information.

Identifying Positions Requiring a Personnel Security Clearance (PSC)

5. In order to assess whether a position requires a PSC, NATO nations and NATO civil and military bodies shall involve managers who will be the most familiar with the work of their staff and the levels of access to NATO classified information the position requires. It is they who will generally be the best judge of the security clearance level required for the position.

6. Managers shall also be responsible for ensuring that their staffs have the level of PSC appropriate to the access that their work requires and that the principle of need to know is applied. When an individual's PSC is due for its regular revalidation, or when the jobholder changes, the appropriate manager shall be responsible for assessing whether the level of PSC remains necessary for that position.

Criteria for Assessing Eligibility for a Personnel Security Clearance

7. The following paragraphs contain the principal criteria for assessing the loyalty, trustworthiness and reliability of an individual in order for him to be granted and to retain a PSC. These paragraphs consider aspects of character and circumstances which may give rise to potential security concerns.

8. Although the criteria apply to the individual being cleared, where appropriate and in accordance with national legislation, a spouse's, cohabitant's or close family member's character, conduct and circumstances may also be relevant and should be taken into account when considering an individual's eligibility for clearance.

9. The criteria shall be applied to determine if an individual or his spouse, co-habitant, and where appropriate and in accordance with national legislation, close family member :

(a) has committed or attempted to commit, conspired with or aided and abetted another to commit (or attempt to commit) any act of espionage, terrorism, sabotage, treason or sedition;

(b) is, or has been, an associate of spies, terrorists, saboteurs, or of individuals reasonably suspected of being such or an associate of representatives of organisations or foreign nations, including intelligence services of foreign nations, which may threaten the security of NATO and/or NATO nations, unless these associations were authorised in the course of official duty;

PUBLICLY DISCLOSED - AC/35-WP(2010)0003 - MISE EN LECTURE PUBLIQUE

(c) is, or has been, a member of any organisation which by violent, subversive or other unlawful means seeks the overthrow of the government of the member nations, or a change in the form of government of the member nations;

(d) is, or has recently been, a supporter of any organisation described in sub-paragraph (c) above, or who is, or who has recently been closely associated with members of such organisations.

(e) has deliberately withheld, misrepresented or falsified information of significance, particularly of a security nature, or has deliberately lied in completing the personnel security form or during the course of a security interview;

(f) has been convicted of a criminal offence, or offences indicating habitual criminal tendencies; or has serious financial difficulties or unexplained affluence; or has a history of alcohol dependence, use of illegal drugs and/or misuse of legal drugs;

(g) is or has been involved in conduct, including any form of sexual misconduct, which may give rise to the risk of vulnerability to blackmail or pressure;

(h) has demonstrated, by act or through speech, dishonesty, disloyalty, unreliability, untrustworthiness or indiscretion;

(i) has seriously or repeatedly infringed security regulations; or has attempted, or succeeded in, unauthorised activity in respect to communication and information system(s);

(j) is suffering, or has suffered, from any illness or mental or emotional condition which may cause significant defects in his judgement or reliability or may make the individual, unintentionally, a potential security risk. In all such cases competent medical advice should be sought; or

(k) may be liable to pressure through relatives or close associates who could be vulnerable to foreign intelligence services, terrorist groups or other subversive organisations or individuals whose interests may threaten the security interests of NATO and/or NATO nations.

Dual Nationals

10. For individuals holding dual-nationality, one of which may be non-NATO, special attention should be afforded when considering eligibility for a security clearance. Provided that the parent nation NSA[2] granting the clearance is content that there is no actual or potential conflict of loyalty, there is no prima facie reason to deny a clearance.

[2] There is provision in the industrial security context (Ref.: Directive on Industrial Security, Para: 43, 44) for a NSA/DSA to grant a PSC to an individual holding the nationality / citizenship of another NATO nation.

PUBLICLY DISCLOSED - AC/35-WP(2010)0003 - MISE EN LECTURE PUBLIQUE

Investigative Requirements for NATO CONFIDENTIAL, NATO SECRET and COSMIC TOP SECRET Clearances

11. The initial security clearance for access to information classified NC and NS shall be based on enquiries covering at least the last 5 years, or from age 18 to the present, whichever is the shorter; and shall include the following :

(a) the completion of a **Personnel Security Questionnaire** (which can be either NATO or national);

(b) **identity check / citizenship / nationality status** – the individual's date and place of birth shall be verified and his identity checked. Citizenship status and/or nationality, past and present, of the individual shall be established; this shall include an assessment of any vulnerability to pressure from foreign sources; for example, due to former residence or past associations; and

(c) **national and local records check** – a check shall be made of national security and central criminal records, where these latter exist, and/or other comparable governmental and police records for any officially recorded indication of disloyalty or unreliability. The records of law enforcement agencies with legal jurisdiction where the individual has resided or been employed for at least six months shall be checked.

12. The initial security clearance for access to information classified CTS shall be based on enquiries covering at least the last 10 years, or from age 18 to the present, whichever is the shorter. If interviews are conducted as stated in sub-paragraphs (e)(i) and (ii) below, enquiries shall cover at least the last 7 years, or from age 18 to the present, whichever is the shorter. In addition to the requirements stated in paragraph 11 above, the following are required for clearances for access to information classified CTS; these factors may also be relevant to the assessment of NC and NS clearances, where they are compliant with national rules and legislation :

(a) **financial status**: information shall be sought on the individual's finances in order to assess any vulnerability to foreign or domestic pressure due to serious financial difficulties, or to discover any unexplained affluence;

(b) **education**: information shall be sought on attendance since the 18th birthday, or during an appropriate period as judged by the investigating security authority, at schools, universities and other education establishments;

(c) **employment**: information covering present and former employment shall be sought, reference being made to sources such as employment records, performance or efficiency reports and to employers or supervisors;

(d) **military service**: where applicable, the service of the individual in the armed forces and type of discharge will be verified; and

PUBLICLY DISCLOSED - AC/35-WP(2010)0003 - MISE EN LECTURE PUBLIQUE

(e) **interviews**: where provided and admissible under national law :

(i) interview(s) shall also be conducted with the individual especially if the initial enquiries have revealed potentially adverse information; and

(ii) interviews shall also be conducted with individuals who are in a position to give an unbiased assessment of the individual's background, activities, loyalty, trustworthiness and reliability. When it is the national practice to ask the subject of the investigation for referrals, referees shall be interviewed unless there are good reasons for not doing so. Sufficient additional enquiries shall be conducted to develop all relevant information available on an individual and to substantiate or disprove adverse information.

13. Lack of coverage in any investigative category shall be compensated for through other investigative means, in accordance with National security rules and regulations.

Granting a Personnel Security Clearance

14. The NSA or competent national authority shall consider all available information in order to determine whether a PSC shall be granted or not. It should be noted that indications of potential vulnerability to pressure (e.g. debts or the potential vulnerability of a spouse/cohabitant/close family member) need not be a reason to deny clearance if the subject's loyalty, trustworthiness and reliability are undisputed. The NSA or competent national authority shall assess the risks associated with each case in order to determine whether a clearance may be granted.

Security Clearance Certificate for Employees of NATO Civil and Military Bodies

15. Once a NSA or other competent national authority has granted a PSC to an individual to be employed by, or seconded, to a NATO civil or military body, or an individual assigned by a member nation to its national delegation at NATO HQ, they shall either directly, or upon specific request by the respective NATO body, provide a copy of a PSC certificate to the NATO civil or military body at which the individual is to take up his appointment. An example of this certificate is provided at Appendix 1. In all cases, the date on which the security clearance was granted, and the date of validity of the security clearance shall appear on the personnel security clearance certificate.

16. If an individual's period of service does not commence within 12 months of the issue of a new PSC to fill a post with a NATO civil or military body, or if there is a break of 12 months in an individual's service, during which time he is not employed in a position with a NATO or a NATO member government civil or military body, the PSC shall be referred to the individual's parent NSA for confirmation that it remains valid and appropriate.

Security Clearances for Contractor Personnel Performing Works for NATO Civil or Military Bodies

17. The provision for Personnel Security Clearances or the confirmation of those for contractor personnel performing works on NATO premises and requiring a Personnel Security Clearance is addressed in the Directive on Industrial Security.

PUBLICLY DISCLOSED - AC/35-WP(2010)0003 - MISE EN LECTURE PUBLIQUE

Revalidation of a Personnel Security Clearance

18. After the initial granting of a PSC and provided the individual has had unbroken service with a NATO nation or NATO civil or military body and has a continuing need for access to NATO classified information, the PSC shall be reviewed for revalidation at intervals not exceeding 5 years for a CTS clearance and 10 years for NS and NC clearances, with effect from the date of the last investigative action on which it was based. All investigations for the renewal of a PSC shall cover the period since the previous investigation. Requests for revalidation of a PSC shall be applied for in a timely manner, in accordance with the requirements of the NSA(s).

19. For revalidation of an NC and NS PSC, the procedures outlined below shall, as a minimum, be carried out :

(a) the completion of a personnel security questionnaire by the individual concerned. (The form may be either the NATO supplementary personal particulars form or a similar national form supplied by the relevant national authority);

(b) for individuals employed by a NATO civil or military body, a check of the personnel security questionnaire against the security and personnel records of the NATO body;

(c) when a revalidation is requested by a NATO civil or military body for individuals employed by a NATO body, the completed personnel security questionnaire mentioned at (a) above and the results of the check required at (b) above, shall be sent to the individual's parent and the host nation NSA;

(d) review by the nation in which the NATO body is located (i.e., the host nation) of its national records at the request of the individual's parent NSA;

(e) where applicable, reviews identical with those in (d) above by any other NATO nation in which the staff member has resided if so requested by the parent NSA; and

(f) when the relevant NATO civil or military body requests the individual's parent NSA to re-validate the security clearance, it shall also pass details of the individual's security record during his/her employment for the period under review.

20. The parent NSA shall then review any information arising during the course of these records checks against the background of its own records and send its decision to the requesting NATO civil or military body.

21. The revalidation of a clearance at the CTS level, in addition to the normal review procedures outlined in paragraph 19 above, may include an interview with the individual and shall require the following to cover the 5 years since the last investigation/review :

(a) where character references are required by member nations who have supplied their own personnel security questionnaire, references shall be taken up in consultation with the NSA of the host nation;

(b) in the event that a more detailed investigation is required, interviews should be conducted with at least two persons who are in a position to give an unbiased

PUBLICLY DISCLOSED - AC/35-WP(2010)0003 - MISE EN LECTURE PUBLIQUE

assessment of the individual's background, activities, loyalty, trustworthiness and reliability;

(c) when the PSC of an individual serving abroad has to be revalidated more than once during uninterrupted expatriation, consideration should be given to undertaking the detailed investigation referred to under (b) above;

(d) additional enquiries, where necessary, by the NSA of the host nation on behalf of the parent nation arising from any information which may come to light as a result of any action under paragraph 19 and 21(a) to (c) inclusive above;

(e) the despatch by the NSA of the host nation and of any other member nation in which the subject has resided, of any information developed within the terms of paragraph 19 and 21(a) to (d) inclusive above to the NSA of the parent nation;

(f) a review by the parent NSA against the background of its own records of any information which has been sent to it within the terms of (e) above; and

(g) the despatch of the parent NSA's decision, with regard to the renewal of the personnel security clearance certificate, to the requesting NATO civil or military body.

22. If a NATO personnel security clearance is not revalidated within the life of the clearance, a period of a further 12 months may be allowed for the revalidation to be completed, provided that the responsible NSA has commenced the action necessary to revalidate the clearance. If, at the end of this additional 12-month period, the revalidation has still not been completed, the individual shall be moved to duties which do not require a personnel security clearance. If, exceptionally, enquiries cannot be completed within this period of time, and no adverse information has been found, the NSA/DSA concerned may provide the relevant NATO civil or military body with an extension of the validity of the existing security clearance, indicating a date on which a final decision on the revalidation may be anticipated.

Adverse Information

23. Procedures shall be established to ensure that if adverse information becomes known concerning an individual, a determination shall be made by the individual's parent NSA as to whether he shall continue to hold a PSC. In cases where individuals are considered to represent an unacceptable security risk, their PSC shall be withdrawn and the individuals shall be excluded from access to NATO classified information and from positions where they might endanger security. When the PSC is withdrawn for an individual seconded to, or directly hired by, a NATO civil or military body, a certificate revoking the PSC shall be issued to the NATO body by the parent NSA.

Records of Personnel Security Clearances

24. Records of the PSCs granted to individuals with access to NATO classified information shall be maintained by the NATO member nations and by the employing NATO civil or military body. These records shall contain details of the level, date and validity of the clearance.

PUBLICLY DISCLOSED - AC/35-WP(2010)0003 - MISE EN LECTURE PUBLIQUE

SECURITY AWARENESS AND BRIEFING OF INDIVIDUALS

25. All individuals employed in positions where they have access to NR information, or hold a clearance for access to NC or above, shall be briefed on security procedures and their security obligations. All cleared individuals shall acknowledge that they fully understand their responsibilities and the consequences which the law or administrative or executive order of their nation provides when classified information passes into unauthorised hands either by intent or through negligence. A record of the acknowledgement shall be maintained by the NATO nation or NATO civil or military body authorising access to NATO classified information.

26. All individuals who are authorised access to, or required to handle NATO classified information, shall initially be made aware, and periodically reminded of the dangers to security arising from indiscreet conversation with persons having no need-to-know, their relationship with the media, and the threat presented by the activities of intelligence services which target NATO and its member nations. Individuals shall be thoroughly briefed on these dangers and must report immediately to the appropriate security authorities any approach or manoeuvre which they consider suspicious or unusual.

27. All individuals who cease to be employed in duties requiring access to NATO classified information shall be made aware of, and acknowledge, their responsibilities for the continued safeguarding of NATO classified information.

AUTHORISING ACCESS TO NATO CLASSIFIED INFORMATION

28. An individual shall only be authorised access to NATO classified information after he has been granted the appropriate personnel security clearance, a determination of his need-to-know has been made, and he has been briefed on NATO security procedures and has acknowledged his security obligations.

Exceptional Circumstances

Provisional appointments

29. When an individual is to be assigned in a position that requires a PSC at a level higher than that currently possessed by the individual, the assignment may be made on a provisional basis, provided that :

(a) the individual possesses a current PSC;

(b) action has been initiated to obtain the level of PSC required for the position;

(c) the placement of the individual is approved by the responsible NSA or other competent authority; and

(d) satisfactory checks have been made that the individual has not seriously or repeatedly infringed security regulations.

30. Provisional appointments shall not extend beyond six months from the date the individual takes up the position. An NSA may extend the appointment for another six months if the investigation has been initiated and there is no adverse information.

PUBLICLY DISCLOSED - AC/35-WP(2010)0003 - MISE EN LECTURE PUBLIQUE

One time Access

31. Exceptionally, individuals may be authorised access on a one-time basis to NATO information classified one level higher than that to which they are cleared. The following criteria must be fulfilled :

(a) a compelling mission need for the access shall be justified, in writing, by the individual's supervisor;

(b) access shall be limited to specific items of NATO classified information in support of the mission described by the supervisor;

(c) the individual possesses a current PSC;

(d) satisfactory checks have been made that the individual has not seriously or repeatedly infringed security regulations;

(e) authorisation shall be granted only by an OF6 ("one-star general") or the civilian equivalent, after co-ordination with the appropriate security authority(s); and

(f) a record of the exception, including a description of the information to which access was approved, shall be maintained by the cognisant security office.

32. This procedure shall not be used on a recurring basis for access to NATO classified information. If this is required, or if access is required for more than 6 months, a personnel security clearance for the higher level must be obtained.

Access in Exceptional Circumstances

33. Individuals may, as an exception, be authorised access, to NATO HQ and NATO Civil or Military Bodies' premises and to NATO Classified information, provided that the following criteria are fulfilled:

(a) individuals are nationals of a NATO Member Nation;

(b) access shall be authorised by the Head of NATO HQ Division, or NATO Civil or Military Body based on a compelling written justification;

(c) access shall be limited to specific items of NATO information classified up to and including NATO SECRET in support of the mission described by the Head of a NATO HQ Division, or NATO Civil or Military body;

(d) access shall be authorised on a one time basis or for a limited period of time, in any case not exceeding six months;

(e) access shall be limited to administrative zones, or class 2 security areas;

(f) access to CIS processing NATO classified information shall not be authorised, other than to CIS intended solely to support the activity in which the individual is engaged;

PUBLICLY DISCLOSED - AC/35-WP(2010)0003 - MISE EN LECTURE PUBLIQUE

(g) the responsible parent NSA has granted, in accordance with national legislation, a provisional PSC, or has confirmed that the security clearance process of the individual has already started and that preliminary records checks have not revealed adverse information; and

(h) a record of the exceptions, including a description of the facility and of the information to which access was approved, should be maintained by the responsible Security Office and should be periodically forwarded to the NOS.

34. The procedure described in paragraphs 33 and 35 shall be limited to the following cases:

(a) Short Term employment of an individual whose capacity, with respect to the activity, makes him indispensable;

(b) Employment of interpreters, both from NATO and non-NATO Nations.

The procedure shall not be used on a recurring basis for access to NATO premises, or to NATO classified information. To this end, NOS shall maintain records of the exceptions and inform the NSC accordingly.

Employment of Interpreters from Non-NATO Nations

35. Employment of interpreters who are not nationals of a NATO member nation may be permitted as an exception in the following cases:

(a) the language to be interpreted from/into requires a mother tongue speaker who is not a NATO national; and

(b) the NATO classified information to be interpreted shall have been assessed and authorised for release to the parent nation of the interpreter.

The provisions of paragraphs 33 (b)-(c)-(f)-(h) above shall apply.

Emergency Access

36. In wartime, during periods of mounting international tension, international contingency operations or in peacetime during deployments or on-call/exercise duty when emergency measures require it, member nations and the Heads of NATO civil and military bodies may, in exceptional circumstances, grant by written authorisation, access to NATO classified information to individuals who do not possess the requisite personnel security clearance, provided that such authorisation is absolutely necessary and there are no reasonable doubts as to the loyalty, trustworthiness and reliability of the individual concerned. A record of this authorisation describing the information to which the access was given shall be maintained.

37. In the case of information classified CTS, this emergency access shall be confined wherever possible to those individuals who have been authorised access to either national TOP SECRET or to information classified NS.

PUBLICLY DISCLOSED - AC/35-WP(2010)0003 - MISE EN LECTURE PUBLIQUE

Personnel Security Clearances for Senior Government Officials

38. Access to NATO classified information by Senior government officials (for example, Heads of State and Government, Government Ministers, Members of Parliament, and members of the Judiciary) is determined by national rules and regulations; such SGOs should be briefed on their security obligations in respect to the protection of NATO classified information.

Access by Spouses / Dependents to NATO Classified Information

39. Spouses or dependents of individuals employed by NATO civil and military bodies who are required to have access, on a need-to-know basis, to NATO classified information shall be security cleared, and shall be briefed on their security obligations in respect to the protection of NATO classified information. The security clearance process shall include, as a minimum, the requirements that are established for a personnel security clearance, as stated in paragraphs 11 to 13 above.

ATTENDANCE AT CONFERENCES AND MEETINGS

40. An individual's authorisation for participation in a conference, course, meeting or seminar shall be based on the following:

(a) an identity check and confirmation of the individual's authorisation and security clearance, if required;

(b) the provision of an Attestation of Personnel Security Clearance as provided in Appendix 2;

(c) this form shall be issued by NATO civil or military bodies, NSAs or other competent national authority, and be transmitted to the appropriate authorities, or exceptionally be hand carried by the delegates concerned;

(d) where appropriate and agreed by the receiving and transmitting authorities, a consolidated list of names including the details required in Appendix 2 is acceptable;

(e) at NATO facilities with national diplomatic or military delegations/representations specific arrangements shall be agreed between the Security Office of the NATO facility and the national delegations/representatives stating that the national delegations / representatives provide to the security office of the NATO facility a confirmation of the appropriate clearance of its national when requesting an access badge to the facility; and

(f) visits for any purpose by company representatives, consultants or contractors to NATO facilities or establishments shall follow the provisions of Enclosure "G" to the NATO Security Policy C-M(2002)49 and the latest version of its supporting Directive on Industrial Security AC/35-D/2003.

PUBLICLY DISCLOSED - AC/35-WP(2010)0003 - MISE EN LECTURE PUBLIQUE

COURIERS / GUARDS / ESCORTS

41. Couriers and guards employed to carry documents classified NC and above shall be security cleared, as a minimum, to the NS level by their NSA, unless specific National security rules and regulations are applied. Couriers, guards and escorts shall be briefed on NATO security procedures and shall be instructed on their duties for protecting the NATO classified information entrusted to them. When individuals such as guards and escorts are employed in circumstances where they might have unauthorised access to classified information, they shall be security cleared to the level deemed appropriate by the relevant security authority.

ACCESS BY NON-NATO NATIONALS

42. Non-NATO nationals serving as integrated members of the Armed Forces of NATO member nations may be authorised access up to and including information classified CTS. In the case of such nationals it shall be incumbent upon the NATO member nation NSA to satisfy itself that the conditions for security clearance and access required by this directive and NATO Security Policy are fulfilled.

43. In accordance with the overall provisions of NATO Security Policy, individuals who are nationals[3] of non-NATO nations or who are individuals from an international organisation may be granted access to NATO classified information on a case-by-case basis, provided that :

(a) access is necessary in support of a specified NATO programme, project, contract, operation, or related task;

(b) the individual is granted a NATO Personnel Security Clearance (PSC) based on a clearance procedure no less rigorous than that required for a NATO national in accordance with NATO security policy and supporting directives; noting that a NATO PSC is not required for access to NR information;

(c) the prior written consent of the NATO nation or NATO civil or military body that originated the information is obtained; and

(d) the non-NATO individual in question shall have clearly understood and undertaken, by means of personally undersigning an acknowledgement of responsibilities, that NATO information that he might have access to in the context of a specified NATO programme, project, contract, operation, or related task, shall strictly and solely be used for the purposes of the entrusted task and shall not be shared with or transmitted to third persons, bodies, organisations or governments.

---

3 Nationals of non-NATO nations includes “nationals of a Kingdom”, “citizens of a State”, and ”landed immigrants in Canada”. “Landed immigrants in Canada” are individuals who have gone through a national screening process including residency checks, criminal records and security checks, and who are going to obtain lawful permission to establish permanent residence in the nation.

PUBLICLY DISCLOSED - AC/35-WP(2010)0003 - MISE EN LECTURE PUBLIQUE

44. As an exception to the requirement for originator control in sub-paragraph 43(c) above, NSAs of NATO nations may approve access to NATO classified information by nationals of certain non-NATO nations who are employed by NATO Civil or Military Bodies, the Government of the NATO nation, or by a contractor that is located and incorporated in the NATO nation, provided that all of the following criteria are met, in addition to those in sub-paragraphs 43(a), 43(b) and 43(d) above :

(a) disclosures shall be limited to individuals who are nationals of the following countries - Australia, Austria, Finland, Ireland, New Zealand, Sweden and Switzerland. NSAs may propose changes to the list of countries, for consideration by the NSC;

(b) access shall be limited to information that is classified no higher than NS, and in accordance with any dissemination limitation or administrative marking that has been applied by the originator. Access shall not be provided to CTS information, ATOMAL or other Special Category information;

(c) the non-NATO national shall be granted access to the NATO classified information only for the period of time necessary to provide the specified support to a NATO project, programme, contract, operation or related task. The control of access to the NATO classified information shall be the ultimate responsibility of the security officer of the facility or organisation at which access is provided; the security officer shall be a national of a NATO member nation;

(d) access to the information shall be for the original purpose for which the information was provided to NATO;

(e) there shall be a security of information arrangement or security agreement between the Government of the NATO nation wishing to provide access to the information and the Government of the nation of citizenship of the non-NATO individual. Moreover, the NATO nation that is to provide access to the information shall ensure, within its national legislation, that it has sufficient control and jurisdiction over the non-NATO national to enable it to prosecute the non-NATO national and hold him accountable for the proper handling of NATO classified information. The NATO Nation may act as a Sponsor in respect of non-NATO nationals employed by NATO Civil or Military Bodies, as required; and

(f) the NATO nation that is to provide access to the information shall be willing to provide access to its own classified information of a similar type and classification level to the nation of citizenship of the non-NATO national.

PUBLICLY DISCLOSED - AC/35-WP(2010)0003 - MISE EN LECTURE PUBLIQUE

NATO PERSONNEL SECURITY CLEARANCE CERTIFICATE

1. Certification is hereby given that:

Full Name:

.....

Date and Place of Birth:

.....

has been granted a personnel security clearance by the Government of:

.....

in accordance with current NATO regulations, including the Security Annex to C-M(64)39 in the case of ATOMAL information, and is, therefore, declared suitable to be entrusted with information classified up to and including: [4]

.....
.....

2. The validity of this certificate will expire not later than: [5]

.....

Signed:

Title: Official government stamp

Date of Issue:

Contact details of the issuing authority (Phone, e-mail, fax):
.....

---

4 Insert, as appropriate, one or more of the following:

(a)	COSMIC TOP SECRET	(d)	COSMIC TOP SECRET ATOMAL
(b)	NATO SECRET	(e)	NATO SECRET ATOMAL
(c)	NATO CONFIDENTIAL	(f)	NATO CONFIDENTIAL ATOMAL

5 The date of expiry shall conform with the provisions of paragraph 18 of the Directive on Personnel Security.

(*) The marking is not part of the template.

PUBLICLY DISCLOSED - AC/35-WP(2010)0003 - MISE EN LECTURE PUBLIQUE

ATTESTATION OF NATO PERSONNEL SECURITY CLEARANCE

1. Attestation is hereby given that:

Full Name ……

Date of Birth ……

Place of Birth ……..

Nationality ……

Where employed ……

Purpose and Duration of Visit ……..
……...
……...

Holder of Passport/Identity Card No. .....……
Issued at ..... Dated .....……

Military Rank and Number (where applicable) .....
.....
has been granted access to NATO information classified up to and including
..... in accordance with current NATO security regulations, including the Security Annex to C-M(64)39 in the case of ATOMAL information, and has been briefed accordingly by
.....

Signed:

Title: Official stamp

Date of Issue:

2. The validity of the attestation will expire no later than:
.....……...…...

3. Issued by ……..
(Member nation or NATO civil or military body)

Date and Place of Issue:
.....

Contact details of the issuing authority (Phone, e-mail, fax):
.....

(*) The marking is not part of the template.

DECLASSIFIED/DECLASSIFIEE - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

NATO OTAN
NORTH ATLANTIC COUNCIL
CONSEIL DE L'ATLANTIQUE NORD

NATO UNCLASSIFIED

7 January 2008

DOCUMENT
AC/35-D/2001-REV2

NATO SECURITY COMMITTEE

DIRECTIVE on PHYSICAL SECURITY

Note by the Chairman

1. At Annex is the second revision of the Directive on Physical Security which is published in support of the NATO Security Policy, C-M(2002)49. It is binding and mandatory in nature upon NATO member nations, commands and agencies.

2. This revision reflects approved changes in the area dealing with access to NATO Class I security areas by Individuals from Non-NATO Nations / International Organisations.

3. This document has been approved by the NATO Security Committee under the silence period (AC/35-WP(2007)0008 refers) and will be subject to periodic review.

(Signed) Michael T. Evanoff

Annex: 1

Action Officer: Robert Keil, NOS/POB, Ext. 4084
Original: English

NATO HQ - QG OTAN
DMS 1618429
DOCUMENT

DECLASSIFIED/DECLASSIFIEE - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

DIRECTIVE ON PHYSICAL SECURITY

INTRODUCTION

1. This Physical Security directive is published by the NATO Security Committee (AC/35) in support of Enclosure "D" to the NATO Security Policy (C-M(2002)49). This directive contains mandatory provisions and also includes information which clarifies the meaning of those provisions. This directive addresses the following aspects :

(a) security requirements;

(b) physical security measures;

(c) minimum standards for the storage of NATO classified information;

(d) protection against technical attacks; and

(e) physical security of communication and information systems (CIS).

SECURITY REQUIREMENTS

2. In accordance with the requirements of NATO Security Policy, all premises, buildings, offices, rooms, and other areas in which NATO classified information and material is stored and/or handled shall be protected by appropriate physical security measures. In deciding what degree of physical security protection is necessary, account shall be taken of all relevant factors, such as :

(a) the level of classification and category of information;

(b) the quantity and form of the information (hard copy/computer storage media) held;

(c) the security clearance and need-to-know of the staff;

(d) the locally-assessed threat from intelligence services which target NATO and/or its member nations, sabotage, terrorist, subversive or other criminal activities; and

(e) how the information will be stored.

3. Physical security measures shall be designed to:

(a) deny surreptitious or forced entry by an intruder;

(b) deter, impede and detect actions by disloyal personnel (the spy within);

(c) allow for segregation of personnel in their access to NATO classified information in accordance with the need-to-know principle; and

(d) detect and act upon all security breaches as soon as possible.

DECLASSIFIED/DECLASSIFIEE - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

PHYSICAL SECURITY MEASURES

4. Physical measures represent only one aspect of protective security and shall be supported by sound personnel security, security of information, and INFOSEC measures, details of which will be found respectively in Enclosures "C", "E" and "F" of NATO Security Policy and supporting directives. Sensible management of security risks will involve establishing the most efficient and cost-effective methods of countering the threats and compensating for vulnerabilities by a combination of protective measures from these areas. Such efficiency and cost-effectiveness is best achieved by defining physical security requirements as part of the planning and design of facilities, thereby reducing the need for costly renovations.

5. Physical security programmes shall be based on the principle of "defence in depth", and although physical security measures are site-specific, the following general principles shall apply. It is first necessary to identify the locations that require protection. This is followed by the creation of layered security measures to provide "defence in depth" and delaying factors. The outermost physical security measures shall define the protected area and deter unauthorised access. The next level of measures shall detect unauthorised or attempted access and alert the guard force. The innermost level of measures shall sufficiently delay intruders until they can be detained by the guard force. Consequently, there is an interrelationship between the reaction time of the guard force and the physical security measures designed to delay intruders.

6. Regular maintenance of security systems is necessary to ensure that equipments operate at optimum performance. It is also necessary to periodically re-evaluate the effectiveness of individual security measures and the complete security system. This is particularly important if there is a change in use of the site or elements of the security system. This can be achieved by exercising incident response plans.

Security Areas

7. Areas in which information classified NC and above is handled and stored shall be organised and structured so as to correspond to one of the following:

(a) **NATO Class I Security Area**: an area in which information classified NC and above is handled and stored in such a way that entry into the area constitutes, for all practical purposes, access to classified information. Such an area requires:

(i) a clearly defined and protected perimeter through which all entry and exit is controlled;

(ii) an entry control system which admits only those individuals appropriately cleared and specifically authorised to enter the area;

(iii) specification of the level of classification and the category of the information normally held in the area, i.e. the information to which entry gives access;

DECLASSIFIED/DECLASSIFIEE - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

(b) **NATO Class II Security Area**: an area in which information classified NC and above is handled and stored in such a way that it can be protected from access by unauthorised individuals by controls established internally. Such an area requires:

(i) a clearly defined and protected perimeter through which all entry and exit is controlled;

(ii) an entry control system which admits unescorted access only to those individuals who are security cleared and specifically authorised to enter the area. For all other individuals, provision shall be made for escorts or equivalent controls, to prevent unauthorised access to NATO classified information and uncontrolled entry to areas subject to technical security inspection.

8. Those areas which are not occupied by duty personnel on a 24-hour basis shall be inspected immediately after normal working hours to ensure that NATO classified information is properly secured.

Access to NATO Class I Security Areas by Individuals from Non-NATO Nations / International Organisations

9. Individuals from non-NATO Nations / International Organisations who, because of their assignment and official duties, need regular interface with NATO staffs may be granted access to a NATO Class I Security area. The following criteria shall be applied to those Individuals:

(a) access is only granted on a case-by-case basis;

(b) Individuals must be escorted at all times;

(c) during the time of the access, all classified NATO information inside the Class I security area must be appropriately secured, or protected, as applicable so that the access to the Class I security area does not automatically constitute access to classified NATO information;

(d) the requirements of Appendix 2 to the Directive “Criteria for Access to NATO Class I/II Security Areas by Individuals from Non-NATO Nations and International Organisations” apply; and

(e) access to Open Storage Areas is prohibited.

Access to NATO Class II Security Areas by Individuals from Non-NATO Nations / International Organisations

10. Individuals from non-NATO nations / International Organisations who, because of their assignment and official duties, need regular interface with NATO staffs may be granted unescorted access to a NATO Class II Security Area. Such individuals may also be assigned office space within a NATO Class II Security Area in order to fulfil their assignment and official duties.

DECLASSIFIED/DECLASSIFIEE - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

The granting of unescorted access and/or the assignment of office space shall be handled on a case-by-case basis, and shall be in accordance with the criteria set out in Appendix 2 to this Directive.

Administrative Zones

11. An Administrative Zone may be established around or leading up to NATO Class I or Class II security areas. Such a zone requires a visibly defined perimeter within which the possibility exists for the control of individuals and vehicles. Only information classified up to and including NR shall be handled and stored in Administrative Zones.

Specific Physical Security Measures

12. This section provides information on various physical security measures and how they can contribute to the security framework of an organisation or site.

Perimeter

13. A perimeter fence will form a useful physical barrier and will identify the boundary of an area requiring security protection. The level of protection offered by a fence will depend on its height, construction, the material used and any additional security features used to increase its performance and effectiveness such as topping, Perimeter Intrusion Detection Systems (PIDS), lighting or CCTV.

14. The effectiveness of any security perimeter will depend, to a large extent, on the level of security at the points of access. Gates shall be constructed to the same security standard as the fence; and some form of access control shall be in place, otherwise the security of the fence will be negated.

Security lighting

15. Security lighting can offer a high degree of deterrence to a potential intruder in addition to providing the illumination necessary for effective surveillance either directly by the guards or indirectly through a CCTV system. The standard of lighting should, however, meet the minimum requirement of the CCTV and its installation be appropriate to the site conditions.

Intrusion Detection Systems (IDS)

16. Perimeter Intrusion Detection Systems (PIDS) may be used on perimeters to enhance the level of security offered by the fence. PIDS may be installed as covert devices (although this is usually for aesthetic reasons) or overtly to act as a deterrent. PIDS are inherently prone to false alarm and should therefore normally only be used with an alarm verification system such as CCTV.

DECLASSIFIED/DECLASSIFIEE - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

17. In accordance with the principle of “defence in depth”, IDS may be used in rooms and buildings in place of, or to assist, guards. To be effective, an IDS should have a response force that will react within a reasonable timescale in the event of an alarm being given.

Access Control

18. Control of access may be exercised over a site, a building or buildings on a site or to areas or rooms within a building. The control may be electronic, electro-mechanical, by a guard or receptionist, or physical. A pass or personal recognition system governing the regular staff shall control entry into Class I or II security areas.

Guards

19. The employment of guards can provide a valuable deterrent to individuals who might plan covert intrusion. The guards’ duties and the need for and frequency of patrols shall be decided by considering the level of risk and any other security systems or equipment that might be in place. Guards shall be provided with adequate written guidance to ensure specifically assigned tasks are conducted as required. Guards shall require a means of communication with their control centre.

20. When guards are used to ensure the integrity of security areas and NATO classified information, they shall be appropriately cleared, qualified by training and supervised.

21. The response force is required to provide a minimum of two persons to any point of a security disorder on the site without weakening site protection elsewhere. Guards' response to alarms or emergency signals shall be tested and shall be within a time limit evaluated as capable of preventing an intruder’s access to the NATO classified information being protected.

Closed Circuit Television (CCTV)

22. CCTV is a valuable aid to security guards in verifying incidents and PID alarms on large sites or perimeters. The effectiveness of such a system will, however, depend on the selection of suitable equipment and its installation and on the monitoring of the control centre. Detailed professional advice shall be sought.

Entry and Exit Searches

23. NATO establishments shall undertake random entry and exit searches which are designed to act as a deterrent to the unauthorised introduction of material into, or the unauthorised removal of NATO classified information from a site or building. Entry and exit searches may be made a condition of entry to a site or building. A warning notice shall be displayed to indicate that random entry and exit searches may be undertaken.

DECLASSIFIED/DECLASSIFIEE - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

Visitor Control

24. The nationality of the visitor, his/her clearance and need-to-know, and any special control requirements determine whether the visitor shall be permitted escorted or unescorted access to a NATO establishment. The type of control over visitors is described below:

(a) **Escorted**. Visitors who require an escort within an area shall be accompanied at all times. If they need to visit a number of different departments or other members of staff, they shall be formally handed over from one escort to the next with any accompanying documentation. They may be required to wear a pass that identifies them as a visitor; and

(b) **Unescorted**. Visitors who are permitted unescorted entry to an area, or parts of it shall be required to wear a pass that identifies them as a visitor. It should be noted that a visitor pass system is effective only if all regular staff are required to wear a pass.

Approved Equipment

25. For vaults and open storage areas constructed within a Class I or a Class II security area where information classified NC or higher is stored on open shelves or displayed on charts, maps, etc., the walls, floors, ceilings and door(s) with lock(s) must be approved, under the responsibility of the NSA.

MINIMUM STANDARDS FOR THE STORAGE OF NATO CLASSIFIED INFORMATION

26. NATO security policy sets out the minimum standards for the storage of NATO classified information. This section expands upon the security policy.

27. **COSMIC TOP SECRET (CTS).** CTS information shall be stored within a class I or II security area under one of the following conditions :

(a) in a nationally-approved security container with one of the following supplemental controls:

(i) continuous protection by cleared guard or duty personnel;

(ii) inspection of the security container not less than every two hours, at randomly timed intervals, by cleared guard or duty personnel; or

(iii) a nationally-approved Intrusion Detection System (IDS) in combination with a response force that will, after an alarm annunciation, arrive at the location within the estimated timeframe needed to remove or break open the security container, or overcome the physical security measures in place.

DECLASSIFIED/DECLASSIFIEE - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

(b) an open storage area constructed in accordance with Annex to this directive, which is equipped with an IDS in combination with a response force that will, after an alarm annunciation, arrive at the location within the estimated timeframe needed for forced entry; or

(c) an IDS-equipped vault in combination with a response force that will, after an alarm annunciation, arrive at the location within the estimated timeframe needed for forced entry.

28. **NATO SECRET (NS).** NS information shall be stored within a class I or II security area by one of the following methods :

(a) in the same manner as prescribed for CTS information; or

(b) in a nationally-approved security container or vault without supplemental controls; or

(c) an open storage area, in which case, one of the following supplemental controls is required :

(i) the location that houses the open storage area shall be subject to continuous protection by cleared guard or duty personnel;

(ii) cleared guard or duty personnel shall inspect the open storage area once every four hours; or

(iii) an IDS in combination with a response force that will, after an alarm annunciation, arrive at the location within the estimated timeframe needed for forced entry.

29. **NATO CONFIDENTIAL (NC).** NC information shall be stored in the same manner as prescribed for CTS or NS information except that supplemental controls are not required.

30. **NATO RESTRICTED (NR).** NR information shall be stored in a locked container.

Control of keys and combinations

31. Keys of security containers shall not be taken out of office buildings. Combination settings of security containers shall be committed to memory by individuals needing to know them. Spare keys and a written record of each combination setting for use in an emergency shall be held in sealed opaque envelopes by the government department or NATO civil or military body concerned. Working and spare security keys shall be kept in separate containers. The record of each combination shall be kept in a separate envelope. The keys, combinations and the envelopes shall be given security protection no less stringent than the information to which they give access.

DECLASSIFIED/DECLASSIFIEE - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

32. Knowledge of combination settings of security containers shall be restricted to the smallest possible number of individuals. As a minimum, settings shall be changed :

(a) on first being taken into use;

(b) whenever a change of personnel possessing the combination occurs,

(c) whenever a compromise has occurred or is suspected; and

(d) at intervals not exceeding 12 months.

Physical protection of Copying and Telefax machines

33. Copying and telefax machines shall be physically protected to the extent necessary to ensure that only authorised individuals can use them and that all NATO classified information is controlled in accordance with the requirements of NATO security policy and supporting directives.

PROTECTION AGAINST TECHNICAL ATTACKS

Eavesdropping

34. Offices or areas in which information classified NS and above is regularly discussed shall be protected against passive and active eavesdropping attacks, by means of sound physical security measures and access control, where the risk warrants it. The responsibility for determining the risk shall be co-ordinated with technical specialists and decided by the appropriate security authority.

35. **Protection against passive eavesdropping attacks** - the leakage of NATO classified information via insecure communications or by overhearing directly or by unintentional electromagnetic emissions - may involve seeking technical security advice as described in paragraph 36 below and may involve soundproofing walls, doors, floors and ceilings of designated sensitive areas.

36. **Protection against active eavesdropping** - the leakage of NATO classified information by wired microphones, radio microphones or other implanted devices - requires a technical and/or physical security inspection of the fabric of the room, its furnishings and fittings and its office equipment, including office machines (mechanical and electrical) and communications. These inspections shall be undertaken by trained security staff authorised by the appropriate security authority.

Technically Secure Areas

37. Areas which have been specifically identified as requiring protection against audio eavesdropping are to be designated as technically secure areas and entry to them shall be specially controlled. Rooms must be locked and /or guarded in accordance with physical security standards when not occupied and any keys treated as security keys. Such areas shall be subject

DECLASSIFIED/DECLASSIFIEE - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

to regular physical and/or technical inspections; the periodicity of inspections shall be determined by the appropriate security authority. Inspections shall also be undertaken following any unauthorised entry or suspicion of such and entry by external personnel for maintenance work or redecoration.

38. No item of furnishings or equipment shall be allowed into these areas until it has been thoroughly examined physically for eavesdropping devices by trained security staff. A record of the type, serial and inventory numbers shall be maintained of equipment and furniture moved into and out of these technically secure areas. The areas shall be kept locked by an approved method when not occupied, and keys, if used, shall be treated as security keys.

39. Telephones shall not normally be installed in areas which are technically secure. However, where their installation is unavoidable, they shall be provided with a positive disconnect device or shall be physically disconnected when classified discussions take place.

40. The presence of mobile telephones and other electronic items equipped with electro-acoustic parts shall be prohibited in technically secure areas.

41. Regular technical security inspections may need to be carried out in areas where exceptionally sensitive conversations are held in order to supplement physical searches for quick plant devices and to investigate a telephone system or an electrical or other service which could be used as an attack medium. They may also be necessary to determine the vulnerabilities of sensitive areas, including vulnerabilities arising from the local threat from intelligence services which target the Alliance and/or its member nations.

Examination of electrical / electronic equipment

42. Before being used in those areas where meetings are held or work is being performed which involves information classified NS and above, and in circumstances where the threat is assessed as high, communications equipment and electrical or electronic equipment of any kind shall be examined by technical or communications security experts to ensure that no intelligible information is inadvertently or illicitly transmitted by such equipment beyond the perimeter of the appropriate security area.

Overlooking

43. When NATO classified information is at risk from overlooking, appropriate measures shall be taken to counter this risk under daylight as well as artificial light conditions.

PHYSICAL SECURITY FOR COMMUNICATION AND INFORMATION SYSTEMS (CIS)

44. Specific consideration should be given to the physical security of CIS areas and the appropriate directives and guidance should be consulted.

DECLASSIFIED/DECLASSIFIEE - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

OPEN STORAGE AREAS

1. Open Storage Areas are those authorised by the Head of the civil or military body for open storage of classified information. These areas shall be constructed in accordance with the following standards:

(a) **Construction** - the perimeter walls, floors, and ceiling shall be permanently constructed and attached to each other. All construction must be done in a manner so as to provide visual evidence of unauthorized penetration;

(b) **Doors** - doors shall be constructed of wood, metal or other solid material. Entrance doors shall be secured with a built-in nationally approved three-position combination lock. When special circumstances exist, the Head of the civil or military body may authorise other locks on entrance doors for NS and NC storage. Doors other than those secured with the aforementioned locks shall be secured from the inside with either deadbolt emergency egress hardware, a deadbolt, or a rigid wood or metal bar which extends across the width of the door, or by other means approved by the agency head;

(c) **Vents, Ducts, and Miscellaneous Openings** - all vents, ducts, and similar openings in excess of 96 square inches / 620 square centimetres (and over 6 inches / 15 centimetres in its smallest dimension) that enter or pass through an open storage area shall be protected with either bars, expanded metal grills, commercial metal sounds baffles, or an intrusion detection system;

(d) **Windows** -

(i) all windows that might reasonably afford visual observation of classified activities within the facility shall be made opaque or equipped with blinds, drapes, or other coverings;

(ii) Windows at ground level, or other easily reachable windows (for example, from roofs, verandas, and building annexes) will be constructed from or covered with materials that provide protection from forced entry. The protection provided to the windows need be no stronger than the strength of the contiguous walls. Open storage areas that are located within a controlled compound or equivalent may eliminate the requirement for forced entry protection if the windows are made inoperable, either by permanently sealing them or equipping them on the inside with a locking mechanism and they are covered by an IDS (either independently or by the motion detection sensors within the area).

DECLASSIFIED/DECLASSIFIEE - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

CRITERIA for ACCESS to NATO CLASS I/II SECURITY AREAS by INDIVIDUALS from Non-NATO NATIONS and INTERNATIONAL ORGANISATIONS

1. The granting of access as set out in paragraphs 9 and 10 of this directive will increase the risk of compromise of NATO classified information. In order to mitigate some of the increased risk, the following criteria shall be applied prior to granting access to a NATO Class I Security Area, unescorted access to NATO Class II Security Areas, or assigning office space within a NATO Class II Security Area :

(a) access is necessary in support of a specified NATO programme, project, contract, operation, or related task;

(b) individuals shall only belong to a non-NATO nation / international organisation which has signed a Security Agreement with NATO and has been certified by the NATO Office of Security (NOS) as being able to appropriately protect released NATO classified information;

(c) the individual is in possession of an appropriate and valid NATO Personnel Security Clearance (PSC) based on a clearance procedure no less rigorous than that required for a NATO national in accordance with NATO security policy and supporting directives;

(d) for access to NATO classified information, the established release procedures (the latest version of AC/35-D/2002 refers) shall be observed;

(e) the approval of access rights is reserved to the NOS and shall take place in accordance with the requirements of paragraph 3 below;

(f) non-NATO individuals who have been granted access shall be clearly recognisable by unique access passes or badges. The access pass or badge shall not provide access to any other NATO Security Area;

(g) non-NATO individuals have signed the "Certificate of Acknowledgement of Responsibilities" associated with the security protection of NATO classified information;

(h) non-NATO individuals shall not have escorting privileges, exchange pass arrangements with other NATO civil or military bodies, or access to NATO registries / sub-registries; and

(i) where office space is allocated within a NATO Class II Security Area, effective measures shall be implemented to prevent the unauthorised disclosure of NATO classified information, whether in hard-copy form or associated with a NATO communication and information system (CIS).

2. The successful implementation of the above measures rests on the continuing development of sound security education and awareness for all staffs working in areas to which non-NATO individuals are granted access. It is, therefore, imperative that Security

DECLASSIFIED/DECLASSIFIEE - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

Officers develop appropriate security education programmes and oversee the implementation of these measures.

3. The procedure to obtain approval for access rights is as follows :

(a) Heads of Division / Office shall confirm in writing to the Director, NOS (through the appropriate chain of command) that the non-NATO individual has a requirement for access to a particular area within a NATO Class II Security Area;

(b) the request shall be supported by documentation specifying the duration of the requirement, the full identifying particulars of the individual and the rationale for seeking access rights;

(c) the NOS shall approve an individual's suitability for access on a case-by-case basis. Approval shall be based on confirmation that :

- a Security Agreement and a Code of Conduct has been signed between NATO and the non-NATO nation / international organisation;

- the NOS has certified the non-NATO nation / international organisation as being able to appropriately protect released NATO classified information;

- the individual is in possession of an appropriate and valid NATO Personnel Security Clearance (PSC);

- the individual has signed a "Certificate of Acknowledgement of Responsibilities" associated with the security protection of NATO classified information;

(d) approved individuals shall receive a unique access pass or badge which indicates that the individual is permitted unescorted access to a specific zone in the NATO Class II Security Area;

(e) NATO staffs and non-NATO individuals from the Divisions / Offices involved in these arrangements shall be briefed by the appropriate local security authority / staffs.

4. On completion of the requirement to support a specified NATO programme, project, contract, operation, or related task, the granting of unescorted access to a NATO Class II Security Area shall be withdrawn. Non-NATO individuals who cease to be employed in the Divisions / Offices involved in these arrangements shall be made aware of, and acknowledge in writing, their responsibilities for the continued safeguarding of NATO classified information.

5. The implementation of the arrangements shall be subject to periodic security inspection by the appropriate Security Authority (NOS, SHAPE J2 for ACO, or ACT Office of Security for ACT).

DECLASSIFIED/DECLASSIFIÉ - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

NATO OTAN
NORTH ATLANTIC COUNCIL
CONSEIL DE L'ATLANTIQUE NORD

NATO UNCLASSIFIED

17 January 2012

DOCUMENT
AC/35-D/2002-REV4

SECURITY COMMITTEE

DIRECTIVE on the SECURITY of INFORMATION

Note by the Chairman

1. At Annex is the fourth revision of the Directive on the Security of Information which is published in support of the NATO Security Policy, C-M(2002)49. It is binding and mandatory in nature upon NATO member nations, commands and agencies.

2. This revision reflects approved changes to the following areas :

(a) Deletion of Appendix 5 - Security Arrangements for the Release of NATO Classified Information to the Western European Union (WEU);

(b) Appendix 8 - Security Assurance;

(c) Appendix 9 - Personnel Security Certificate (for non-NATO national); and

(d) Appendix10 - Attestation of Personnel Security Clearance (for non-NATO national)

3. This document has been approved by the Security Committee (AC/35-WP(2010)0001, AC/35-WP(2011)0009 and AC/35-WP(2011)0011 refer) and will be subject to periodic review.

(Signed) Stephen F. Smith

Annex: 1

Action officer: Robert Keil, NOS/[illegible], ext. [illegible]
Original: English
DMS 1889086

NATO HQ - QG OTAN DOCUMENT

DECLASSIFIED/DECLASSIFIÉ - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

DIRECTIVE ON THE SECURITY OF INFORMATION

INTRODUCTION

1. This Security of Information directive is published by the NATO Security Committee (AC/35) in support of Enclosure "E" to the NATO Security Policy (C-M(2002)49). This directive contains mandatory provisions and also includes information which clarifies the meaning of those provisions. This directive addresses the following aspects :

(a) classification and markings of information;

(b) control and handling of information;

(c) reproductions, translations and extracts of information;

(d) dissemination and transmission of information by physical means ;

(e) receipts and records;

(f) disposal and destruction;

(g) security infractions, breaches and compromises; and

(h) security arrangements for the release of NATO classified information to non-NATO nations and international organisations.

CLASSIFICATION and MARKINGS

2. Security classifications indicate the sensitivity of NATO information and are applied in order to alert recipients to the need to ensure protection in proportion to the degree of damage that would occur from unauthorised access or disclosure. NATO security classifications and their significance are :

(a) COSMIC TOP SECRET (CTS) - unauthorised disclosure would result in exceptionally grave damage to NATO;

(b) NATO SECRET (NS) – unauthorised disclosure would result in grave damage to NATO;

(c) NATO CONFIDENTIAL (NC) - unauthorised disclosure would be damaging to NATO; and

(d) NATO RESTRICTED (NR) - unauthorised disclosure would be detrimental to the interests or effectiveness of NATO.

DECLASSIFIED/DECLASSIFIÉ - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

3. NATO nations and NATO civil and military bodies shall introduce measures to ensure that information created by, or provided to NATO is assigned the correct security classification. For NATO civil and military bodies, these measures shall include:

(a) restricting the authority to decide on a security classification for information to a limited number of designated positions;

(b) limiting the information that requires a security classification, encouraging the placing of more sensitive information into appendices to texts so that the main text can be distributed more widely and with less stringent security measures; and

(c) emphasising that documents shall not necessarily be given the same security classification as those to which they are attached, refer or respond.

4. Each NATO civil or military body shall establish a system to ensure that CTS information which it has originated is reviewed no less frequently than every five years to ascertain whether the CTS classification still applies. Such a review is not necessary in those instances where the originator has predetermined that specific CTS information shall be automatically downgraded after two years and the information has been so marked.

5. The top and bottom of each page of a document shall be marked with the overall security classification of the document, noting that individual annexes / appendices / attachments / enclosures may be marked with a classification level lower than the overall security classification of the document.

6. The overall security classification of a document shall be at least as high as that of its most highly classified component. Component parts of documents classified NC and above shall, where possible, be classified (including by paragraph) by the originator to facilitate decisions on further dissemination of appropriate sections. Covering documents shall be marked with the security classification of the information contained therein when they are separated from the information they accompany.

7. When information from various sources is collated, the product shall be reviewed for overall security classification since it may warrant a higher classification than its component parts. Original security classification caveats must be retained when information is used to prepare composite documents.

8. Cases of apparent over-classification or under-classification shall be brought to the attention of the originator by the recipient. If the originator changes the classification of the document, he shall inform all addressees.

9. An originator of classified information that is collated into a new product by a NATO civil or military body who, when consulted in the course of a review for the declassification of NATO classified information, objects to the declassification of specific information, will indicate the earliest date or event on or around which he shall either agree to its declassification or review it again for declassification.

DECLASSIFIED/DECLASSIFIÉ - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

Changing Classifications

10. The classification level of NATO classified information may be changed only by, or with the consent of, the originator. However, if the originator cannot be determined, the successor organisation or higher authority shall assume the responsibility of the originator. In such cases, changes in classification may occur only after the NATO nations or NATO civil or military bodies that have an interest in the subject matter have been consulted.

11. The originator, or if the originator cannot be determined, the successor organisation or higher authority, is responsible for ensuring that recipients are promptly notified when the classification level of information is changed.

Dissemination Limitation Markings

12. As an additional marking to further limit the dissemination of NATO classified information, a Dissemination Limitation Marking may be applied by the originator.

CONTROL AND HANDLING

The Registry System

13. There shall be a Registry System which is responsible for the receipt, accounting, handling, distribution and destruction of accountable information. Such a responsibility may be fulfilled either within a single registry system, in which case strict compartmentalisation of CTS information shall be maintained at all times, or by establishing separate registries and control points:

(a) each NATO member nation may establish up to two Central Registries for CTS, which act as the main receiving and dispatching authority for the nation or body within which it has been established. Central Registries may also act as registries for other accountable information; and

(b) registries and control points shall act as the responsible organisation for the internal distribution of CTS and NS information and for keeping records of each document held in that registry's or control point's charge; they may be established at ministry, department, or command levels.

14. Registry personnel handling national classified information in NATO nations may, if properly cleared and briefed for access to NATO classified information, also be responsible for NATO classified information.

15. Regardless of the type of registry organisation, those that handle information classified CTS shall appoint a "COSMIC Control Officer" (CCO). CCOs shall be designated as necessary. A Deputy COSMIC Control Officer (DCCO) may perform some of the duties of the COSMIC Control Officer on a permanent basis and shall assume all authority and responsibility during the latter's absence.

DECLASSIFIED/DECLASSIFIÉ - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

16. The CCO is responsible for the following tasks, which may be delegated to the Head of a COSMIC Registry :

(a) the physical safeguarding of all information classified CTS held by the Central Registry, registry or control point to which he is assigned;

(b) maintaining an up-to-date record of all information classified CTS held or circulating within the registry or control point or passed to other registries or control points, and maintaining records of disclosure and destruction sheets for his registry;

(c) maintaining up-to-date records, by name, of all individuals authorised access to information classified CTS held by his registry or control point;

(d) maintaining up-to-date records of all other registries and control points with which he is authorised to exchange information classified CTS, together with the names of the associated CCOs and their sample signatures;

(e) distribution of information classified CTS to only those addressees authorised to have access to information classified CTS;

(f) transmission of information classified CTS;

(g) obtaining receipts for all information classified CTS distributed or transmitted;

(h) ensuring that documents classified CTS are returned to the responsible registry when no longer required, either for retention or destruction; and

(i) in the case of Heads of COSMIC Central Registries, notifying NOS of organisational changes regarding any of the registries or control points for which he is responsible.

Registry System Handling

Information Classified COSMIC TOP SECRET (CTS)

17. Documents classified CTS consigned to an addressee in another member nation or NATO civil or military body may be transmitted direct from one registry or control point to another when authorised by the appropriate authority of the member nation or NATO civil or military body.

18. The Registry System shall exercise continuous control of individual documents classified CTS, which includes such items as microfiche and computer storage media, and shall maintain records of document receipt, distribution and destruction. Records shall identify the COSMIC Central Registry, registry, control point or individual holding the document.

19. At least annually, each registry shall carry out an inventory of all information classified CTS for which it is accountable. A document classified CTS is deemed to have been accounted for, if:

(a) it is physically accounted for and contains the correct number of pages;

(b) a receipt is held from the registry or control point to which it has been transferred; or

DECLASSIFIED/DECLASSIFIÉ - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

(c) a change in classification or declassification notice or a destruction certificate for the document is held.

20. Registries and control points shall report the results of the annual inventory to the responsible COSMIC Central Registry.

21. Results of annual inventories of all COSMIC Central Registries shall be reported by the responsible security authority to the NOS by the 31st March of each year.

22. The dissemination of information classified CTS shall be through COSMIC registry channels. Registries may transmit information classified CTS directly to other registries provided that the transmission and receipt is recorded in the originating and receiving registries. Documents classified CTS may be issued outside a registry or control point to an individual who is responsible for its custody, but they shall be returned when no longer required. The individual custody of documents classified CTS shall not be transferred except through the responsible registry.

Information Classified NATO SECRET (NS)

23. The handling requirements for information classified NS are as follows :

(a) up-to-date records of the receipt, disposition, and dispatch of information classified NS shall be maintained; and

(b) periodic spot-checks shall be conducted of registry and divisional/personal holdings to verify their continued control.

Information Classified NATO CONFIDENTIAL (NC) and NATO RESTRICTED (NR)

24. Unless specifically required by national security rules and regulations, NC and NR material is not required to go through the Registry System. Measures shall be in place to prevent unauthorised access to NC and NR material.

STORAGE

25. NATO classified information shall be stored in accordance with NATO Security Policy (Enclosure “D”) and the supporting physical security directive requirements. NATO classified information may be stored as microfilm, on computer storage media, provided the collections or media are afforded the same security protection as the original information and any collections or media containing more than one classification shall be afforded the security protection of the highest classification appearing in the collection or on the microfilm, or computer storage media. Information classified NR shall be stored in a manner that deters unauthorised access; for example, in a locked desk, cabinet or room to which access is controlled.

DECLASSIFIED/DECLASSIFIÉ - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

REPRODUCTIONS, TRANSLATIONS, AND EXTRACTS

26. Reproductions and translations of documents classified NS and below may be produced by the addressee under strict observation of the need-to-know principle. Security measures laid down for the original document shall be applied to such reproductions and/or translations. If classified NS, they shall be marked with identifying copy numbers. The number of reproductions and/or translations of NS documents and their copy numbers shall be recorded.

27. Extracts of NATO classified documents may be included, if necessary, in documents which need to be seen by individuals in member nations or NATO civil or military bodies who have not been authorised access to NATO classified information, provided they hold a national personnel security clearance to the level of the classification of the extracted information. In order to ensure that the extracts are properly protected, such papers shall be given an appropriate security classification and shall be distributed on a need-to-know basis. An extract from a classified document shall bear the classification of the document or component thereof (if individually classified) from which it is taken unless it is obvious that it justifies another classification. If so, it shall be referred to the original or higher classification authority for determination of the correct classification.

28. If, however, in exceptional circumstances, the originator of a classified document desires to control the further dissemination of information contained therein, the originator shall indicate these special limitations with a prominent and suitable note to the effect, for example: “Reproduction of this document in whole or in part, is prohibited unless authorised by the originator” or “Reproduction of paragraphs ….to….annexes….and….is prohibited unless authorised by the originator”. These special restrictions should be applied with discrimination and as infrequently as possible.

29. Notwithstanding originator control prohibitions, addressees whose national language is not that of a document may translate the document, provided the requirements for copying have been met and the translation includes all classifications markings and caveats of the original document. In addition, translations of documents classified CTS shall be reported to the originator.

30. Information classified CTS shall not, except in exceptional cases, be copied. Extra paper copies of information classified CTS shall normally be obtained from the originating NATO nation or NATO civil or military body. In exceptional cases, paper copies or translations of information CTS, including extracts and copies to or from machine readable media may be made for urgent mission purposes, provided that the copies or translations :

(a) are authorised by the CCO of a COSMIC Central Registry or, if authority has been delegated, by the CCO of a registry or control point;

(b) are reported to the COSMIC Central Registry or accountable registry or control point, which shall maintain a record of the number of copies made;

(c) bear the reference and copy number of the original information together with the name of the originating authority and that of the reproducing COSMIC Central Registry, registry or control point;

(d) are marked with an identifying reproduction copy number locally assigned by the element making the reproduction or translation;

DECLASSIFIED/DECLASSIFIÉ - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

(e) display the CTS marking and classification and all other markings of the original information; and

(f) are brought under COSMIC registry control, distributed through COSMIC registry channels and reported in the annual inventory along with other CTS information.

31. As an exception to the above, the officer in charge of a communications centre may authorise the production of those copies and translations necessary to make initial distribution of signals/messages classified CTS. A record shall be made of the number of copies made. Thereafter, the authority for reproduction and translation of the signal/message will be the CCO of the COSMIC Central Registry.

32. Reproductions, extracts and translations of information classified NS, including copies to or from machine readable media, may be reproduced by the addressee when necessary for mission purposes, provided that the reproductions and/or translations are marked with identifying reproduction copy numbers and the number of reproductions and/or translations, including reproduction copy numbers, are recorded.

33. Reproductions, extracts, and translations of information classified NC and NR may be reproduced by the addressee provided they are controlled in a manner to deter unauthorised access.

34. Equipment, such as copiers, facsimile equipment and IT systems, used to reproduce classified information, shall be physically protected to ensure that only authorised individuals can use them.

DISSEMINATION AND TRANSMISSION BY PHYSICAL MEANS

35. The purpose of security during dissemination and physical transmission is to ensure appropriate protection against unauthorised observation, modification, or disclosure (deliberate or inadvertent).

Dissemination

36. The dissemination of NATO classified information shall be on a need-to-know basis. The dissemination of information classified NC and above shall be restricted to individuals who have the appropriate level of personnel security clearance, who have been briefed on their security responsibilities, and who are authorised to have access to such information. The dissemination of information classified CTS shall be in compliance with paragraph 22 above. Information classified NR may be disseminated to individuals who have been informed of the prescribed control measures, have been briefed and have a need-to-know for official purposes.

Transmission

Transmission within Sites or Establishments

37. Classified information carried within the perimeter of the site or establishment shall be covered in order to prevent observation of its contents.

DECLASSIFIED/DECLASSIFIÉ - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

Transmission outside Sites/Establishments within a NATO Nation

38. Whenever a courier service is used for the transmission of NATO classified information outside the confines of a site or establishment, the packaging requirements of paragraphs 39 and 40 and the receipt requirements of paragraphs 47 to 50 shall be complied with. The physical transmission of classified information within a NATO nation shall be by the following means:

(a) **Military or government courier service**;

(b) **National postal services/**
NATO information classified up to and including NS may be transmitted by a national postal service under conditions fixed by national regulations;

(c) **Authorised commercial courier service/**
Where appropriate, such services may be used for NATO information classified up to and including NS if permitted by national regulations, provided their use is approved by the relevant NSA/DSA;

(d) **Personal Carriage**
The personal carriage of NATO classified information may be permitted within a NATO nation under conditions no less stringent than the national regulations for the personal carriage of national information of equivalent classification, provided that:

(i) a record shall be kept in the appropriate registry, control point or office of all accountable information carried;

(ii) classified information shall be packaged in accordance with the requirements of paragraphs 39 to 40, and the locked briefcase or similar approved container shall be of such size and weight that it can be retained in the personal possession of the courier;

(iii) classified information shall not leave the possession of the bearer unless it is stored in accordance with the prescribed security requirements, it shall not be left unattended, and it shall not be opened en route;

(iv) classified information shall not be read in public places; and

(v) the individual shall be briefed on his security responsibilities and be provided with either a formal written authorisation, in accordance with national rules and regulations; and, when carrying information classified NC and above, be provided with a NATO courier certificate (Appendix 1 contains an example of a courier certificate).

39. Information classified NC and above transmitted between sites or establishments shall be packaged so that it is protected from unauthorised disclosure. The following standards shall apply :

(a) it shall be enclosed in two opaque and strong covers. A locked pouch, locked box or a sealed diplomatic pouch may be considered as the outer cover;

DECLASSIFIED/DECLASSIFIÉ - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

(b) the inner cover shall be secured, bear the appropriate NATO classification, as well as other prescribed markings and warning terms, and bear the full designation and address of the addressee;

(c) the outer cover shall bear the designation and address of the addressee and a package number for receipting purposes;

(d) the outer cover shall not indicate the classification of the contents or reveal that it contains classified information; and

(e) if the classified information is transmitted by courier, the outer cover shall be clearly marked with the notice, “By Courier Only”.

40. Information classified NR shall, as a minimum, be transmitted in a single opaque envelope or wrapping. The markings on the package shall not reveal that it contains information classified NR.

International Transmission

41. The international transmission of information classified CTS shall be by diplomatic pouch or military courier. Personal carriage internationally of information classified CTS is prohibited.

42. The international transmission of NATO classified information up to and including NS shall be by diplomatic pouch, military courier, registered mail or personal carriage as set out below. Information classified NR may also be transmitted by other postal or commercial services.

43. Information classified up to and including NS that cannot be transmitted by one of the foregoing methods and that is relevant to the industrial domain may be transmitted by other means in accordance with the relevant provisions in Enclosure “G” of the NATO security policy and its supporting industrial security directive.

44. The following requirements shall be met for the international transmission of packages containing information classified NC and above :

(a) the package shall bear an official seal, or be packaged in a manner to indicate that it is an official consignment, and should not undergo customs or security scrutiny. Official NATO Seals shall be handled as accountable documents, and as such, they shall be protected as though they were NS material;

(b) the courier shall carry a courier certificate recognised by all NATO nations (see example at Appendix 1) identifying the package and authorising him to carry the package; and

(c) the courier’s travel arrangements shall be in accordance with the following restrictions on destinations, routes and means of transportation or, if national regulations are more stringent, in accordance with national regulations :

(i) the courier shall not travel to, through or over non-NATO nations nor use any means of transportation or any transportation carrier registered in

DECLASSIFIED/DECLASSIFIÉ - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

a non-NATO nation, to which any of the criteria listed below apply :

(1) the government of the nation :

(a) has given evidence by word or deed of an attitude hostile to NATO and/or NATO nations;

(b) is not able to give a generally agreed level of protection to the life and/or personal belongings of its residents and/or visiting foreigners; or

(c) has given evidence that it does not respect at all times the immunity of a diplomatic seal;

(2) the intelligence services of the nation target NATO and/or NATO nations; or

(3) the nation is at war, or subject to serious civil strife.

45. In exceptional cases, the restrictions at paragraph 44(c) above may be waived by the NSAs or the Heads of NATO civil or military bodies, or their designated representatives, if urgent operational requirements cannot be otherwise met.

DISSEMINATION AND TRANSMISSION BY ELECTROMAGNETIC MEANS

46. Information classified NR and above shall be disseminated and transmitted in accordance with the requirements of Enclosure “F” of NATO security policy and its supporting directives.

RECEIPTS AND RECORDS

47. Receipts are required for packages containing accountable information that are transmitted between sites / establishments, within national borders or internationally. Receipts shall be obtained against package numbers. Receipts are not required for packages containing information classified NC or NR unless required by the originator or specifically required by national security rules and regulations. Receipts shall be unclassified, shall quote the reference number, copy number, and language of the documents, and a short title, if it is unclassified.

48. A receipt shall be enclosed in the inner cover of packages containing CTS and NS documents. The receipt and disposition of CTS and NS documents shall be recorded as prescribed herein.

49. The receipt, listing the documents, shall be immediately returned to the sender after having been dated and signed. Documents that contain accountable information shall be signed for only by the CCO or other registry system individual. The inner cover of a package containing a CTS document may contain a marking indicating that it is to be opened only by a specific individual or office. However, the cover shall be opened in the presence of the CCO, DCCO or other authorised registry system individual, and a copy of the external receipt or other identifying information shall be provided so that the document may be entered into the registry system.

DECLASSIFIED/DECLASSIFIÉ - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

50. A continuous receipt system is required for the distribution of information classified CTS. For the distribution of information classified NS within member nations and NATO civil and military bodies, each member nation or NATO civil and military body concerned shall establish internal procedures, to ensure that information classified NS is controlled and its receipt, disposition and dispatch is recorded.

51. Users of a CTS document shall sign and date a disclosure record, which shall remain affixed to the document, or file of documents, until it is destroyed. The record shall be retained for 10 years after destruction of the document.

DISPOSAL AND DESTRUCTION

52. Proper management of NATO classified information extends throughout the life cycle of the information, including those aspects related to the disposal and destruction of the information. At the end of the life cycle, information shall be reviewed for retention, archival storage, downgrading, declassification or destruction.

53. Any such actions need to meet not only security requirements, but also need to meet NATO information management and archival requirements.

Destruction

54. Classified information which is no longer required for official purposes, including surplus or superseded information and waste, shall be destroyed in such a manner as to ensure that it cannot be reconstructed. It is not necessary to await destruction instructions. Registries and other offices that hold NATO classified information shall maintain a continuous review of the information to determine whether it can be destroyed.

55. The following are additional requirements for the destruction of accountable information :

(a) all information classified CTS shall be returned to the registry holding them on charge for destruction. Information classified CTS shall be listed on a destruction certificate which shall be signed by the COSMIC Control Officer and by an independent witnessing official, who shall be appropriately cleared and authorised to have access to information classified CTS;

(b) the NSA may authorise the responsible Control Officer of any deployed or isolated military unit to destroy information classified CTS which is no longer needed, provided properly executed destruction certificates are furnished to the registry which holds them on charge;

(c) destruction certificates and control records for information classified CTS shall be retained for a minimum period of 10 years in a registry, as they may assist in the conduct of investigations. Copies of destruction certificates need not be forwarded to the originator or the appropriate COSMIC Central Registry unless specifically requested;

DECLASSIFIED/DECLASSIFIÉ - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

(d) the destruction of information classified NS shall be recorded and the record shall be signed by the destruction official and independent witness, both of whom shall be appropriately cleared and authorised to have access to NS information; and

(e) destruction certificates and control records for information classified NS shall be retained in the registry or office performing the destruction for a period specified by individual NATO nations and NATO civil or military bodies, but for not less than 5 years.

56. The control records to be retained should be sufficient to undertake a damage assessment or conduct a security investigation into the compromise or loss of accountable information.

57. The recording of the destruction and the retention of control records of information classified NC and NR is not required; unless required by the originator or specifically required by national security rules and regulations.

SECURITY INFRACTIONS, BREACHES AND COMPROMISES

Action on Breaches of Security

58. All breaches of security shall be reported immediately to the appropriate security authority. Each reported breach of security shall be investigated by individuals who have security, investigative and, where appropriate, counterintelligence experience, and who are independent of those individuals immediately concerned with the breach, to determine :

(a) whether NATO classified information has been compromised[1];

(b) if so, whether all the unauthorised individuals who have or could have had access to the information have at least either a national or a NATO personnel security clearance and are known from existing records to be of such reliability and trustworthiness that no harm to NATO will result from the compromise; and

(c) what remedial, corrective or disciplinary (including legal) action is recommended.

59. Where the investigation yields positive answers to both 58(a) and (b), the administrative authority shall take steps to brief and/or indoctrinate the individuals concerned, as appropriate, to the classification and category of the information to which they have had inadvertent access. The administrative authority can close such cases without reporting to the NOS. Where the investigation yields a positive answer to 58(a) and a negative answer to either part of 58(b) the compromise is reportable to the NOS as described below.

[1] Classified information lost, even temporarily, outside a security area is to be presumed compromised. Classified information lost, even temporarily, inside a security area, including that in documents which cannot be located at periodic inventories, is to be presumed compromised until investigation proves otherwise.

DECLASSIFIED/DECLASSIFIÉ - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

Records of Breaches of Security

60. Heads of NATO civil and military bodies shall arrange for records of breaches of security regulations, including reports of investigation and remedial and corrective actions, to be kept for three years and to be available during security inspections.

Reporting of Compromises

61. When a compromise of NATO classified information has to be reported under the terms of paragraph 59, the report shall be forwarded through the NSA or the Head of the NATO civil or military bodies concerned to the NOS. Where possible, the reporting authority should inform the originating NATO component at the same time as the NOS, but the latter may be requested to do this when the originator is difficult to identify. The timing of the reports depends on the sensitivity of the information and the circumstances. Initial reports shall be forwarded immediately to the NOS in cases where it has been determined that :

(a) CTS or NS information is involved; or

(b) there are indications or suspicions of espionage (provided the report would not hamper the investigations in hand); or

(c) unauthorised disclosure to the press/media has occurred.

62. Initial reports shall contain the following information:

(a) a description of the information involved, including its classification and marking reference and copy number, date, originator, subject and scope;

(b) a very brief description of the circumstances of the compromise, including the date, the period during which the information was exposed to compromise and, if known, the number and/or category of unauthorised individuals who have or could have had access; and

(c) whether the originator has been informed.

63. Further reports shall follow as developments warrant. Reports on compromise of information classified NC shall be forwarded when the investigation has been completed and should contain information as requested in paragraph 62(a), (b) and (c). There is no requirement to report compromises involving information classified NR unless they meet the criteria set out paragraph 61(b) or (c) or specifically required under national security rules and regulations. In all cases of reportable compromise the final report, or a progress report, of the investigation shall be with the NOS within 90 days of the initial report.

Relief From Accountability for Lost Accountable Documents

64. When the final report of investigation shows that an accountable document has been irretrievably lost rather than mislaid, the NSAs or the Head of the NATO civil or military body may grant relief from accountability.

DECLASSIFIED/DECLASSIFIÉ - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

Action by the Originating NATO Component

65. The main purpose of reporting compromises of NATO classified information is to enable the originating NATO component to assess the resulting damage to NATO and to take whatever action is desirable or practicable to minimise the damage. Reports of the damage assessment and minimising action taken shall be forwarded to the NOS.

Action by the NATO Office of Security (NOS)

66. The NOS shall :

(a) coordinate enquiries where security authorities from more than one NATO nations are concerned;

(b) coordinate, if necessary, with the originators and the security authorities concerned the final assessment of the damage done to NATO and any minimising action to be taken;

(c) recommend to, and/or conduct in agreement with the security authority concerned, further investigations whenever it considers them necessary; and

(d) inform the Secretary General of NATO, whenever the gravity of damage to the Alliance so warrants.

Action by the Secretary General of NATO

67. The Secretary General of NATO may request the appropriate authorities to make further investigations and to report.

SECURITY ARRANGEMENTS FOR THE RELEASE OF NATO CLASSIFIED INFORMATION TO NON-NATO NATIONS AND INTERNATIONAL ORGANISATIONS

68. Enclosure "E" to NATO security policy sets out the principles for authorising the release of NATO classified information to non-NATO nations and international organisations, and the release authority conditions. The following Appendices to this directive address the specific procedures and arrangements :

(a) APPENDIX 2
Procedures for the Release of NATO classified information to non-NATO Recipients;

(b) APPENDIX 3
NATO Production and Logistic Organisations (NPLOs) - Procedures to be Followed for the Release of NATO Classified Information Belonging to an NPLO or other Organisation Granted a Charter under the Terms of C-M(62)18;

(c) APPENDIX 4
Security Provisions for the Exchange of Classified Information Between NATO and the European Union (EU);

DECLASSIFIED/DECLASSIFIÉ - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

(d) APPENDIX 5 - *Cancelled*;

(e) APPENDIX 6
Security Arrangements for the Release and Protection of NATO Classified Information to a NATO-led Combined Joint Task Force (CJTF) or Similar Formation and the Exchange and Protection of Classified Information with non-NATO Nations / Organisations Participating in a NATO-led CJTF or Similar Formation;

(f) APPENDIX 7
Minimum Standards for the Handling and Protection of NATO Classified Information (NATO SECRET and Below) to be Met by Non-NATO Recipients;

(g) APPENDIX 8
Security Assurance;

(h) APPENDIX 9
Personnel Security Clearance Certificate (for non-NATO national); and

(i) APPENDIX 10
Attestation of Personnel Security Clearance (for non-NATO national).

DECLASSIFIED/DECLASSIFIÉ - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

COURIER CERTIFICATE
(Example)

Valid until ….....……..

1. This is to certify that the bearer ….....……, holder of Passport/
(name and rank where applicable)
Identity Card No. …..... is a member of ……. (parent organisation).

2. On the journeys detailed overleaf, the bearer is travelling in the execution of his official functions and is designated as an official NATO courier. He is authorised to carry …..... (number) of packages of official NATO documents, the seals on which correspond to the specimen seal appearing against the appropriate journey.

3. All customs and immigration officials concerned are, therefore, requested to extend to the official correspondence and documents being carried under official seal by the bearer, the immunity from search or examination conferred by the Agreement on the Status of the North Atlantic Treaty Organization National Representatives and International Staff, and the Agreement between the Parties to the North Atlantic Treaty regarding the Status of their Forces.

Signature of Authorising Official:

Designation:
(Name and rank in capitals)

Official stamp of NATO member
Nation or NATO civil or military body

Date:

DETAILS OF ITINERARY		**SPECIMENS OF SEAL USED**
From	To	See note below
From	To	See note below

NOTE: In addition to an impression of the seal, the officer affixing the seal must print his name, rank and the name and address of his department, command, agency or facility.

DECLASSIFIED/DECLASSIFIÉ - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

PROCEDURES FOR THE RELEASE OF NATO CLASSIFIED INFORMATION TO NON-NATO RECIPIENTS

REQUESTS FOR RELEASE OF NATO INFORMATION

1. Release authorisation shall be based on the principles stated in Enclosure "E" of NATO security policy.

2. Requests for release shall be sent to the relevant addressee as follows:

   (a) the Council Secretariat, NATO International Staff, for NATO classified information issued by the NAC;

   (b) to the Secretary of the appropriate subject-matter committee for information classified up to and including NS which has been originated by that committee and/or bodies subordinate to it;

   (c) the Director, International Military Staff, for NATO classified information issued by the NAMILCOM and/or bodies subordinate to it;

   (d) to SACEUR or D/SACEUR for information classified up to and including NS which is identified as being releasable to xFOR, or is classified NATO/xFOR SECRET (mission SECRET);

   (e) to the Mission Commander for a NAC-approved operation involving non-NATO Troop Contributing Nations, for information classified up to and including NS that has already been determined as releasable to the mission (xFOR); and

   (f) the Head of an NPLO, for NATO classified information originated by and belonging to one or more of the nations participating in the NPLO.

3. Requests for release shall include the following information:

   (a) for NAC-approved cooperative activities, where potential non-NATO participants to that activity have also been endorsed by the NAC on a case-by-case basis:

      (i) reference to the relevant subject in the overall work plan or the OPLAN for the cooperative activity;

      (ii) purpose and justification for the release (initiating cooperation, progress in cooperation, exercise, etc);

      (iii) identification of document(s) containing the NATO classified information (reference number, date and NATO classification);

      (iv) description of the NATO classified information which should be released (the whole document(s), part of the document or excerpt from the document);

DECLASSIFIED/DECLASSIFIÉ - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

(v) if appropriate, a request for generic release (i.e. specific subject areas, defined series of documents, anticipated future documents or series of documents, etc., stating maximum classification and any other limitations regarding the possible future release).

(b) for release outside cooperative activities approved by the NAC, the document containing the NATO classified information must be identified and the information requested in (a) (ii), (iii) and (iv) above must be given. Generic release is not authorised.

Actions upon the Receipt of a Release Request

4. Addressees receiving a request for release of NATO classified information shall ensure that :

(a) the justification given in the release request is adequate; and

(b) the NATO classified information concerned is properly identified and described; and

(c) in accordance with the requirements of Enclosure "E" to NATO Security Policy, a Security Agreement has been concluded between NATO and the non-NATO recipient and that the required security survey has been carried out by the NOS with a positive result;

or

in exceptional circumstances, in order to support specific operational requirements endorsed by the NAMILCOM / NAC (for example, in support of force protection, and the exchange of intelligence information), a Security Assurance from the non-NATO recipient has been provided;

or

the non-NATO recipient has provided, through its NATO Sponsor, a written Security Assurance to NATO that it will protect NATO classified information to a degree no less stringent than the provisions contained in the bilateral Security Agreement / Arrangement for the protection of the Sponsor's classified information of an equivalent classification;

or

the NATO sponsor has provided the necessary assurance that the appropriate security system is in place in the non-NATO recipient for the protection of released information;

and

DECLASSIFIED/DECLASSIFIÉ - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

(d) the request is sent to the appropriate committee or delegated authority for a decision; and

(e) any international organisation which requests release has a Security Agreement in force with NATO and the release of information to its non-NATO members is in accordance with relevant provisions of the Security Agreement as well as other established rules concerning their participation in NATO activities.

5. In cases where the NATO classified information requested for release has been issued by two or more bodies (e.g. a military document prepared by NAMILCOM and approved by the Defence Planning Committee (DPC) and issued under the latter's reference), it is the responsibility of the initial addressee to coordinate the response to the request.

Actions by the Release Authority

6. Based on the information contained in the request, the Release Authority will approve or refuse the release.

7. National members of the Release Authority are responsible for obtaining any approval which may be required from national authorities.

8. The Release Authority is responsible for ensuring that any information released to a non-NATO recipient has been reviewed / sanitised so that the non-NATO recipient is only given information for which he has a requirement / need-to-know.

9. Approval, whether obtained in committee or under the silence procedure, will be recorded in writing.

10. In the context of NAC-approved cooperative activities, the Release Authority may approve generic release of NATO classified information issued under its authority. Such approval must state the specific subject areas or series of documents of the NATO classified information and the level of classification authorised for release and may stipulate any other limitations regarding possible future release.

11. Should a request for release of NATO classified information not be approved by a delegated Release Authority, the request, together with the latter's reason for not approving it, may be presented to the next level and ultimately to the NAC for final decision. This action will only be taken in cases when sought by the requesting NATO member nation(s) or NATO body or when the delegated Release Authority decides that such action is appropriate.

DECLASSIFIED/DECLASSIFIÉ - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

Marking Information to be Released

12. The following procedures shall be used for marking NATO classified information:

(a) **for existing NATO information**: classified information originating from NATO which is released to non-NATO recipients shall retain its NATO classification. In addition, the cover or first page of the copy of any document released, and the archive copy, shall be marked with the name of the Release Authority, the date the release decision was taken and any related terms or conditions;

(b) **for NATO information created within NAC-approved activities**:

(i) NATO classified information originated in the context of a NAC co-operative activity shall bear the marking "NATO" followed by the designation of the activity or by the name(s) of the international organisation(s) or participating nation(s) and the classification level;

Example:

NATO/EAPC RESTRICTED

NATO/RUSSIA CONFIDENTIAL

NATO/ISAF CONFIDENTIAL

NATO/OAE CONFIDENTIAL

(ii) the dissemination of information generated within a NATO co-operative activity may be restricted by the originator to some of the non-NATO recipients. In this case, a caveat showing the non-NATO recipients permitted access shall be added below the classification line:

Example:

NATO/PfP RESTRICTED
SWEDEN AND SWITZERLAND ONLY

(iii) information created by a NATO civil or military body that is intended to be further disseminated outside the environment within which it was created shall bear the caveat "Releasable to":

Example:

NATO CONFIDENTIAL
RELEASABLE TO CHILE

NATO/EAPC RESTRICTED
RELEASABLE TO AUSTRALIA

DECLASSIFIED/DECLASSIFIÉ - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

NATO CONFIDENTIAL
RELEASABLE to KFOR

NATO CONFIDENTIAL
RELEASABLE to OAE

Transmission of Information to be Released

13. All NATO classified information released to non-NATO recipients shall be forwarded via physical or electromagnetic means, in accordance with the requirements of NATO Security Policy and supporting directives.

Records of Information to be Released

14. NATO civil and military bodies shall keep control records of all information classified CONFIDENTIAL and above which they have released to non-NATO recipients and shall, at least every six months (or as directed by the appropriate Security Authority), report details of the reference number, title and release date to the NATO Central Registry, Brussels. The report sent to the NATO Central Registry identifies the details of the information released since the previous report. On request, national authorities can obtain details through the NATO Central Registry, Brussels.

DECLASSIFIED/DECLASSIFIÉ - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

NATO PRODUCTION AND LOGISTICS ORGANISATIONS (NPLOs)

PROCEDURES TO BE FOLLOWED FOR THE RELEASE OF NATO CLASSIFIED INFORMATION BELONGING TO AN NPLO OR OTHER ORGANISATION GRANTED A CHARTER UNDER THE TERMS OF C-M(62)18

1. NATO classified information originated by one or more of the nations participating in an NPLO or other organisation granted a charter under the terms of C-M(62)18, or generated within such an organisation and pertaining to it, may be the subject of an application for release to a non-NATO recipient by any member nation, or NATO body considering that it would be advantageous to NATO.

2. The provisions of Appendix 2 shall apply, except that the application shall be submitted to the Head of the NATO organisation concerned, who will pass it on to the Board of Directors (or its delegated representative) for a decision. It must specify the document(s) or the class of information to be released, the proposed recipient's need for access to the information, and the purpose for which it will be used. The Board shall take into account already concluded Security Agreements and other arrangements with international organisations that govern the participation of their non-NATO members in NATO-related activities.

3. Provided that the Board (or its delegated representative) agrees that the NATO classified information should be released, it shall ask the NSA of the nations participating in the NATO organisation's programme to satisfy themselves that adequate security arrangements for the protection of the NATO classified information intended to be released exist or are created.

4. For NR information, a Project / Programme Security Group involving the NSAs of the participating nations may delegate authority for release to the Security Officer of the NPLO, in consultation with the appropriate management within the NPLO.

5. The security arrangements shall include a Security Agreement / Arrangement accepted by the nations participating in the NPLO and, on behalf of the intended recipient(s), by an authority competent to commit them to undertake to provide the NATO classified information released a level of security protection no less stringent than that afforded to it within NATO as set out in Appendices 7 and 8. A copy of these Appendices shall be provided to the intended recipient(s). Where a Security Agreement is in force with an international organisation, the release of information to its non-NATO members shall be in accordance with relevant provisions of the Security Agreement as well as other established rules concerning their participation in NATO activities.

6. NSAs shall also take whatever steps they consider appropriate to ensure that the intended recipient(s) are competent to comply with the provisions of the Security Agreement.

7. Release shall be administered on behalf of the Board of Directors of the NATO organisation concerned, by its Security Office. Records shall be kept of all information classified NC or NS passed under these procedures. These records shall be subject to examination by the NOS during its periodic inspections of the organisation.

DECLASSIFIED/DECLASSIFIÉ - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

SECURITY PROVISIONS FOR THE EXCHANGE OF CLASSIFIED INFORMATION BETWEEN NATO AND THE EUROPEAN UNION (EU)

GENERAL

1. The release and exchange of information classified RESTRICTED and above between NATO and the EU is regulated by the Agreement between the North Atlantic Treaty Organisation and the European Union on the Security of Information. This Appendix sets out the policy, procedures and minimum requirements for the handling of NATO classified information to be released to the EU. Attachment 1 contains the "NATO Procedures for Requesting Classified Information from the EU". Attachment 2 contains the "Security Standards Between the NATO Office of Security (NOS), the EU Council General Secretariat Security Office (GSCSO) and the European Commission Security Office (ECSO) for the Protection of Classified Information Exchanged Between NATO and the EU".

RELEASE AUTHORITY

2. The North Atlantic Council (NAC) is the ultimate authority for the release of NATO classified information to the EU except for information classified up to and including COSMIC TOP SECRET which has been originated by the NATO Military Committee (NAMILCOM) (see paragraph 3(b) below). The release of other information classified COSMIC TOP SECRET will always require approval by the NAC. NAC approval is also required for the release to the EU of NATO SECRET information originated by Committees subordinated to the NAC.

3. The NAC has delegated release authority to :

(a) the relevant committee for information classified up to and including NATO CONFIDENTIAL;

(b) the NAMILCOM for information classified up to and including COSMIC TOP SECRET which has been originated by the NAMILCOM and bodies subordinate to it; and

(c) the Board of Directors of a NATO Production and Logistics (NPLO), or other organisations granted a charter under the terms of C-M(62)18, for information classified up to and including NATO SECRET, which has been originated by one or more nations participating in the NPLO or other organisations.

4. Authority for release will only be delegated to a committee on which the originator(s) is/are represented. If the originator(s) cannot be established, the relevant committee will assume the responsibility of the originator(s).

DECLASSIFIED/DECLASSIFIÉ - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

REQUESTS FOR RELEASE

5. Requests from the EU for the release of NATO classified information (which must explain their requirement and provide details of intended recipients) will be sent to the relevant addressee, as follows :

(a) the Executive Secretary, NATO International Staff, for NATO classified information issued by the NAC and committees subordinate to it;

(b) the Director, International Military Staff, for NATO classified information issued by the NAMILCOM and bodies subordinate to it; and

(c) the Head of an NPLO, or other organisation granted a charter under the terms of C-M(62)18, for classified information originated by one or more nations participating in the NPLO or other organisation.

ACTIONS UPON RECEIPT OF A RELEASE REQUEST

6. The addressee will task relevant NATO staffs to prepare the required documents for the appropriate committee (or, in the case of an NATO Production and Logistics Organisation (NPLO), for the Board of Directors) for a decision on release. These documents will contain the following information :

(a) identification of document(s) containing the NATO classified information (reference number, date and NATO security classification);

(b) description of the NATO classified information which could be released (the whole document(s), part of the document(s) or excerpts from the document(s));

(c) in the case of requests for release to non NATO EU Member State(s), confirmation that the EU Member State(s) have subscribed to the "Partnership for Peace" framework document and, in that context, have a valid security agreement with NATO; and

(d) in the case of requests for release to non-EU Member States, a written confirmation that the EU has completed security formalities and a Security Agreement is in place to ensure implementation of security procedures in the non-EU Member states. This confirmation will be provided to the NATO Office of Security (NOS).

REQUESTS FOR GENERIC RELEASE

7. Requests for generic release (e.g. NATO SECRET planning information pertaining to NATO/EU joint CMX exercises) will also include, following the agreement of the appropriate committee, details of specific subject areas, defined series of documents, anticipated future documents or series of documents and anticipated requirements for internal release, etc., stating maximum classification. Upon approval, the appropriate committee (or Board of Directors) will state any other limitations regarding future release.

DECLASSIFIED/DECLASSIFIÉ - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

PROCESSING RELEASE REQUESTS

8. The request will be sent to the appropriate committee (or Board of Directors) for a decision, which will entail obtaining the approval of the originator(s). National members of the relevant committee are responsible for obtaining any approval which may be required from their national authorities. The Board of Directors of an NPLO, having agreed on the release of classified information originated by and belonging to one or more of the states participating in the NATO Production and Logistics Organisation (NPLO)**,** will seek prior to dissemination, the approval of the national security authorities**.**

9. In cases where the NATO classified information requested for release has been issued by two or more bodies (e.g., a military document prepared by NAMILCOM and approved by Defence Planning Committee (DPC), it is the responsibility of the originating authority to coordinate the response to the request.

CLASSIFICATION MARKINGS

10. Classified information originating from NATO which is released to the EU will retain its NATO ownership label and security classification. A caveat will be added below the line to denote releasability :

E.g.: NATO (Security Classification)
RELEASABLE TO EU

Or: NATO (Security Classification)
RELEASABLE TO EU COUNCIL AND/OR (NAMED DIVISION) ONLY

Or: NATO (Security Classification)
RELEASABLE TO EU COUNCIL AND/OR EU COMMISSION

Or: NATO (Security Classification)
RELEASABLE TO EU **AND** NAME(S) OF THIRD COUNTRY(IES) ONLY

11. In addition, the cover or first page of any document released will be marked with the name of the committee (or Board of Directors) which has authorised the release, the date the release decision was taken and any limitation caveats.

RECORDS

12. NATO bodies will keep complete, separate records of all NATO accountable information which they have released to the EU and will send details of the reference number, title, classification, and release date to the NATO Central Registry, Brussels.

13. NATO Central Registry shall maintain a master record of accountable information released to the EU. This record shall be accessible by NATO Member States.

DECLASSIFIED/DECLASSIFIÉ - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

MINIMUM REQUIREMENTS FOR THE HANDLING OF NATO CLASSIFIED INFORMATION RELEASED TO THE EU

14. Within the EU, in accordance with Articles 6, 11 and 12 of the Agreement between the North Atlantic Treaty Organisation and the European Union on the Security of Information, NATO classified information will be handled in accordance with EU security regulations. All NATO classified information which is released to the EU is for official use only. It will, therefore, only be disseminated to individuals in the EU with a need-to-know, an appropriate security clearance for NATO CONFIDENTIAL information and above only, and in accordance with stipulated release caveats.

CLASSIFICATION SYSTEM

15. Classification markings will be used to indicate the sensitivity of the NATO classified information and thus the security procedures and regulations which will apply for its protection. The classifications are as follows: RESTRICTED, CONFIDENTIAL, SECRET and COSMIC TOP SECRET. These correspond to :

NATO	UE COUNCIL / COMMISSION
NATO RESTRICTED	RESTREINT UE
NATO CONFIDENTIAL	CONFIDENTIEL UE
NATO SECRET	SECRET UE
COSMIC TOP SECRET	TRÈS SECRET UE

REGISTRIES AND THE CONTROL OF CLASSIFIED INFORMATION

16. All NATO classified information released to the EU (or to the EU recipients) shall be transferred through a NATO registry to a separate registry established for NATO information in the EU.

ELECTROMAGNETIC TRANSMISSION

17. The electromagnetic transmission of classified information between NATO and the EU shall be conducted in accordance with agreed NATO/EU mechanisms / procedures to be agreed, which assure its protection.

NOS RESPONSIBILITIES

18. The NOS shall:

(a) ensure that the Security Arrangements for the protection of released classified information meet the minimum requirements as laid down in this Appendix;

(b) coordinate inspections with the EU counterpart; and

(c) keep records on all CTS documents held by EU, based on a calendar year report received annually by the 31st March.

DECLASSIFIED/DECLASSIFIÉ - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

NATO PROCEDURES FOR REQUESTING CLASSIFIED INFORMATION FROM THE EUROPEAN UNION

GENERAL

1. NATO, NATO Commands and Agencies shall use the attached form for requesting classified information from the EU.

PROCEDURES FOR REQUESTING

2. A request for EU classified information shall contain the following :

(a) identification and description of the EU classified information that is requested;

(b) if appropriate, a request for generic release (i.e. specific subject areas, defined series of documents, anticipated future documents or series of documents etc.);

(c) intended recipients in NATO; and indication of possible further release outside NATO; and

(d) rationale and justification of the request**;** if appropriate, reference to the relevant NATO activity/mission and/or NATO/EU joint activity or co-operation.

DECLASSIFIED/DECLASSIFIÉ - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

	NATO RESTRICTED
	NATO CONFIDENTIAL
	NATO SECRET
	COSMIC TOP SECRET

NORTH ATLANTIC TREATY ORGANIZATION

FROM: (DIVISION/OFFICE)

REQUEST FOR RELEASE OF EU CLASSIFIED INFORMATION

TO : EU (COUNCIL OR COMMISSION, AS APPROPRIATE) INFO. : REFS. :	FILE : NO :
1. IDENTIFICATION OF DOCUMENT(S) (WHERE KNOWN)	

DECLASSIFIED/DECLASSIFIÉ - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

2. RATIONALE FOR THE REQUEST
3. INTENDED RECIPIENTS IN NATO AND, IF APPROPRIATE, OUTSIDE NATO
4. (Describe here if the whole document is needed or which part or extract is requested)

Date: Signature:

DECLASSIFIED/DECLASSIFIÉ - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

SECURITY STANDARDS BETWEEN THE NATO OFFICE OF SECURITY (NOS), THE EU COUNCIL GENERAL SECRETARIAT SECURITY OFFICE (GSCSO) AND THE EUROPEAN COMMISSION SECURITY OFFICE (ECSO) FOR THE PROTECTION OF CLASSIFIED INFORMATION EXCHANGED BETWEEN NATO AND THE EU

INTRODUCTION

1. Pursuant to Article 12 of the NATO-EU Security Agreement, reciprocal standards for the protection of classified information exchanged between NATO and the EU are hereby agreed. NOS, the GSCSO and the ECSO are responsible for the implementation and oversight of these standards.

PERSONNEL SECURITY CLEARANCE AND AUTHORISATION FOR ACCESS

2. Subject to Article 5(a) of the NATO/EU Security Agreement, positions which require access to NATO or EU classified information (respectively NCI and EUCI) must be identified. Access to EUCI and NCI will be authorised only for individuals who have a "need-to-know". Furthermore, individuals occupying such positions which require access to information classified at or above NATO CONFIDENTIAL or CONFIDENTIAL UE level must have a 'need-to-know' as well as a valid Personal Security Clearance (PSC) issued in accordance with the relevant provisions contained in the respective security rules of NATO, the General Secretariat of the Council and/or the European Commission.

3. The parent National Security Authority (NSA) of the individual concerned is the competent authority responsible for seeing that the necessary security investigations on their nationals/citizens have been carried out in accordance with the respective NATO/EU minimum security standards.

4. Before being given access to classified information, all individuals who require access to classified information must be briefed on the protective security regulations relevant to the classification of the information they are to access. Those individuals accessing classified information must be made aware that any breach of the security regulations will result in disciplinary action and/or possible further legal action in accordance with their respective security regulations or provisions.

DECLASSIFIED/DECLASSIFIÉ - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

CLASSIFICATION SYSTEM

5. Classification markings will be used to indicate the sensitivity of the classified information and thus the security procedures and regulations which will apply for its protection. The classifications and their equivalence are as follows :

NATO	EU
NATO RESTRICTED	RESTREINT UE
NATO CONFIDENTIAL	CONFIDENTIEL UE
NATO SECRET	SECRET UE
COSMIC TOP SECRET	EU TOP SECRET/TRES SECRET UE

The NATO or EU marking in the classification line indicates ownership of the information and defines, inter alia, originator rights.

All information originated by one of the Parties and provided to the other(s) shall include an express releasability marking, such as:

NATO SECRET
RELEASABLE TO THE EU

SECRET UE
RELEASABLE TO NATO

REGISTRIES AND THE CONTROL OF CLASSIFIED INFORMATION

6. A registry system is established at NATO, the General Secretariat of the Council and the European Commission for the receipt, dispatch, control and storage of classified information. The EU Council General Secretariat will be the Central Registry for NATO classified information provided to the EU. At each organisation a designated registry will act as the main point of entry and /exit for information classified NATO CONFIDENTIAL above or CONFIDENTIEL UE and above, as defined per the respective rules of NATO and the EU. Such registries are established as follows :

(a) for NATO: at NATO HQ and SHAPE (for information to be distributed within Allied Command Europe); and

(b) for the EU: at the EU Council General Secretariat.

7. Central and sub-Registries will be responsible for :

(a) distribution and control of classified information within their respective organisation(s);

(b) storage of classified information; and

DECLASSIFIED/DECLASSIFIÉ - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

(c) final disposal and/or downgrading and/or declassification of classified information, including the maintenance of destruction certificates for NATO accountable or EU classified information.

8. The NOS, the GSCSO and the ECSO will be responsible for the oversight and control of registries within their respective organisation(s) and will inform their counterparts of the establishment/disestablishment of registries containing each other's classified information.

9. When exchanging classified information, appropriately cleared couriers will be used by both sides and will be granted, upon presentation of the appropriate security clearance certificate, access badges to the building(s) they need to visit to deliver and collect the documents.

ELECTROMAGNETIC TRANSMISSION

10. The electromagnetic transmission of classified information between NATO and the EU and between the EU and NATO shall be encrypted in accordance with the sender's requirements as outlined in its Security Policies or Regulations.

11. Crypto equipment employed for communications between NATO and the EU must have been certified by the appropriate authority of one of the States designated under Article 5a of the Security Agreement if the level of the information is CONFIDENTIAL or below. When the equipment is intended for the transmission of information classified SECRET and above, it must have been evaluated and approved in accordance with NATO or EU policies or regulations.

BREACHES OR COMPROMISES OF SECURITY

12. Whenever a breach/compromise of security affecting information classified NATO CONFIDENTIAL/CONFIDENTIEL UE or above is discovered or suspected:

(a) a report giving details of the breach/compromise must be sent :

(i) by the GSCSO or ECSO to the NOS, for NCI;

(ii) by the NOS to the GSCSO or ECSO, as appropriate, for EUCI;

(b) an investigation into the circumstances of the breach/compromise must be made. When completed, a full report must be submitted to the office to which the initial report was addressed. At the conclusion of the investigation, remedial or corrective action, where appropriate, must be taken.

13. For information classified NATO RESTRICTED or RESTREINT UE breach/compromises of security need to be reported only when they present unusual features and/or when it is assessed that actual damage resulted from the breach/compromise is in accordance with the respective NATO and UE security regulations.

DECLASSIFIED/DECLASSIFIÉ - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

INSPECTIONS / LIAISON

14. The three Security Offices will facilitate reciprocal inspections to ensure that information originated by their parent organisation is properly protected. In this respect, a joint GSCSO-ECSO team will inspect NATO Headquarters and SHAPE**,** while the NOS will conduct separate inspections to the General Secretariat of the Council and the European Commission.

REVIEW

15. The three Security Offices will facilitate, as appropriate, the presence of observers on their respective inspections. NOS may observe with respect to inspections of EU Member States relative to the protection of NATO classified information releasable to the EU, and GSCSO ECSO may observe with respect to inspections of NATO Member States relative to the protection of EU classified information releasable to NATO.

LIAISON

16. The NOS, the GSCSO and the ECSO will maintain constant liaison to oversee the release and exchange of classified information under the terms of the NATO-EU Security Agreement. These Offices will meet to discuss and review matters of common interest and assess the implementation of these standards. Any modifications to this Security Standards document shall be subject to agreement between the NOS, the GSCSO and the ECSO and the approval by the NATO Security Committee and the EU Council Security Committee respectively.

DECLASSIFIED/DECLASSIFIÉ - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

This Page Intentionally Left Blank

DECLASSIFIED/DECLASSIFIÉ - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

SECURITY ARRANGEMENTS FOR THE RELEASE AND PROTECTION OF NATO CLASSIFIED INFORMATION TO A NATO-LED COMBINED JOINT TASK FORCE (CJTF) OR SIMILAR FORMATION AND THE EXCHANGE AND PROTECTION OF CLASSIFIED INFORMATION WITH NON-NATO NATIONS/ORGANISATIONS PARTICIPATING IN A NATO-LED CJTF OR SIMILAR FORMATION

1. The CJTF concept of deployable multinational, multi-service formations involving NATO and non-NATO nations/organisations generated and tailored for specific contingency operations was endorsed at the NATO Summit of January 1994 and is being implemented through PO(96)63 and the latest version of MC 389. It reflects NATO's determination to give full and practical effect to its new roles, to strengthen the European defence capability of the Alliance and to enhance the development of the Partnership for Peace (PfP) programme. Similar formations may include specific operations that have been approved by the NAC.

2. Participation in a NATO-led CJTF presumes that NATO and non-NATO nations will release/exchange and protect classified information required for the conduct of the CJTF, principally to maintain force protection and the effectiveness of the mission.

3. This Appendix sets out the security requirements for the release and protection of NATO classified information to a NATO-led CJTF and the exchange and protection of classified information with non-NATO nations/organisations participating in a NATO-led CJTF; it draws on existing NATO Security Policy and procedures for the release and protection of NATO classified information outside NATO.

4. The following principles shall apply:

(a) political and military endorsement of the CJTF mission shall have been obtained and any legal requirements satisfied before classified information can be released to/exchanged within a CJTF;

(b) the non-NATO nation shall have signed a Security Agreement with, or provided a Security Assurance to, NATO. The international organisation shall have concluded a Security Agreement with NATO to enable the former to receive NATO classified information.

(c) the release of information to a non-NATO nation on the basis of a Security Assurance shall be limited to NC. However, in exceptional circumstances, in order to support specific operational requirements endorsed by the NAMILCOM / NAC (for example, in support of force protection, and the exchange of intelligence information), NS information may be released to non-NATO troop contributing nations (NNTCN);

(d) NATO security policy and procedures for the handling and protection of NATO classified information shall apply to all nations/organisations participating in the CJTF;

DECLASSIFIED/DECLASSIFIÉ - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

(e) the originator is responsible for determining the security classification and initial dissemination of information; the release of NATO classified information to non-NATO recipients shall be in accordance with the requirements of Enclosure "E" to NATO Security policy;

(f) non-NATO members participating in the CJTF shall be eligible to receive information classified up to and including NS released to the CJTF in accordance with NATO procedures, and in accordance with the understanding in sub-paragraph (c) above;

(g) all classified information released/exchanged will be disseminated under strict observance of the need-to-know principle and shall only be used for the accomplishment of the CJTF mission;

(h) the CJTF Mission Commander shall balance the requirement to protect classified information with the need to maintain force protection and the effectiveness of the CJTF mission. Any classified information of an operational nature that has the potential to affect the lives of CJTF personnel, shall be withheld only in the most exceptional circumstances;

(i) following the decision on which non-NATO nations shall join the CJTF, and in order to ensure force protection and the effectiveness of the mission, authority for the release/exchange of all classified information of an urgent operational nature, such as support of combined combat operations, may be delegated by the NATO Military Committee (NAMILCOM) to the level best suited to evaluate the importance of that information and the need for its immediate release. This shall be specified in the promulgating NATO Operations Order (OPORD). The guiding principle shall be that classified information of an operational nature that has the potential to affect the lives of CJTF personnel shall be withheld only in the most exceptional circumstances. Such release of information not marked by the originator as releasable to the CJTF shall be reported promptly to the NAMILCOM which will decide what limitations should be imposed on the continuing release of such information and inform the appropriate commander(s).

5. As stated at paragraph 4, a political and military mandate for the mission shall be required, any legal requirements satisfied, and security formalities completed before any classified information can be released to or exchanged within a CJTF.

6. A security organisation shall be established in the promulgating NATO Operations Order at the inception of the CJTF. The security organisation shall be directed by a Security Authority who, as a rule, will be the ACOS Intelligence (or equivalent) of the CJTF HQ. Security responsibilities shall also be clearly identified and defined in that OPORD. These shall include :

(a) regulating and coordinating all physical, personnel, information and INFOSEC issues;

(b) clearly identifying release authorities for classified information which shall be established in accordance with agreed NATO security policy;

(c) overseeing and monitoring the security regime, to include the provision of advice and guidance to non-NATO participants on the protection of NATO classified information; and

DECLASSIFIED/DECLASSIFIÉ - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

(d) contingency planning for emergency access and destruction of classified information.

SECURITY REGULATIONS - GENERAL

7. NATO civil and military bodies participating in the CJTF shall comply with NATO security regulations and procedures for the handling and protection of NATO classified information. National/other organisation classified information released to the CJTF shall be handled and protected to the same standard as NATO classified information unless other procedures are required by the originator.

8. Non-NATO personnel shall be denied access to any NATO or national classified information that has not been authorised for release by the appropriate authority. Physical controls and security procedures shall be established in order to maintain separation between NATO classified information which is not releasable to the CJTF and NATO classified information released to the CJTF.

9. This regime shall be achieved by:

(a) establishing separate NATO facilities for the collation and screening of NATO classified information prior to release. These facilities shall be at the lowest level consistent with the security and effectiveness of the CJTF;

(b) permitting access to NATO secure areas by non-NATO personnel only when escorted;

(c) prohibiting access by non-NATO personnel to primary sources of NATO classified information or to IT systems and networks processing NATO classified information;

(d) permitting access by non-NATO personnel to meetings/briefings only after NATO classified information to be used in them has been approved for release;

(e) providing non-NATO nations with copies of this Annex and its Appendices and any other relevant NATO security documents to enable them to handle and protect classified information to NATO standards.

SECURITY REGULATIONS - DETAIL

10. The following addresses the requirements for physical security, personnel security, security of information and INFOSEC :

(a) **Physical Security**

(i) areas containing NATO and other classified information must be selected to provide both effective security and for operational efficiency;

(ii) NATO classified information shall be stored and controlled separately from other classified information;

(iii) NATO-only and CJTF areas must be separated and clearly identified;

DECLASSIFIED/DECLASSIFIÉ - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

(iv) access to these areas shall be permitted to authorised personnel only, who have a valid and appropriate security clearance and possess a pass issued by the authorities controlling these areas;

(b) **Personnel Security**

(i) access to classified information shall only be permitted to individuals who have a valid and appropriate personnel security clearance issued by their national security authority or other competent national body;

(ii) it is the CJTF commander's responsibility to ensure :

- that all individuals participating in the CJTF are informed of the security regime and of current security regulations and procedures;
- that these individuals are aware of their personal responsibility for the protection of classified information to which they have access; and
- that these individuals receive appropriate security education and training, particularly with regard to the protection of NATO classified information.

(c) **Security of Information**

(i) **COSMIC TOP SECRET (CTS)** - CTS shall not be released to non-NATO members of the CJTF. CTS information is only to be handled by appropriately security cleared NATO and NATO member nation personnel with authorised access to the subject matter. Regulations and procedures for handling and protecting information classified CTS are to be found in the relevant Enclosures of NATO Security Policy. In case of actual release, the CJTF commander shall develop an annex summarising the appropriate provisions.

(ii) **SECRET information** is to be handled by appropriately security cleared personnel with authorised access to the subject matter. When not in use, SECRET information is to be stored in security containers. The area in which the container is located is to be under guard at all times and a control of entry system is to be established which only permits authorised individuals to enter the area. Displays of SECRET information shall only take place within appropriately controlled areas. SECRET information is to be transmitted by diplomatic courier, secure messenger services or approved secure telecommunications. Copies may only be made after receipt of written approval from the originator. All copies are to be registered and controlled in the same manner as the original. All transactions involving SECRET information are to be covered by a continuous chain of receipts;

(iii) **CONFIDENTIAL information** is to be handled by appropriately security cleared personnel with authorised access to the subject matter. When not in use, CONFIDENTIAL information is to be stored in security containers located in controlled areas. Displays of CONFIDENTIAL information shall only take place within appropriately controlled areas. Transmission is to be via diplomatic couriers or military messenger services or approved secure telecommunications. Copies may be reproduced by recipients provided that dissemination is made under the need-to-know principle;

DECLASSIFIED/DECLASSIFIÉ - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

(iv) **RESTRICTED information** is to be handled, displayed and stored in areas to which unauthorised individuals are denied access. Transmission is to be achieved through secure means. Transmission by public telecommunications is to be avoided unless speed of delivery is essential to CJTF force security and mission success. Copies may be reproduced by recipients;

(v) **Recipients** are to maintain records of all information classified NATO CONFIDENTIAL and above or that is classified CONFIDENTIAL and above by a member nation, non-NATO nation or another organisation released to the CJTF. Information no longer required is to be destroyed by secure means and, for information classified NATO SECRET and above, a destruction certificate completed containing the signatures of two appropriately security cleared individuals having witnessed the destruction.

(vi) **Should** a compromise of information classified CONFIDENTIAL or above take place, an investigation of the circumstances shall be carried out by the appropriate security authority and the originator informed. CJTF participants, whether NATO or non-NATO, shall cooperate in the investigation as required. Remedial or corrective action shall be taken to correct any deficiency in procedures that caused the compromise. A report on the compromise and on action taken will be forwarded to the NATO Office of Security (NOS) by the investigating security authority.

(d) **INFOSEC**

(i) **identification and authentication/access control** - only authorised users, who have been uniquely and reliably identified and authenticated, shall have access to relevant classified information, whether this is national, other organisation, NATO or CJTF;

(ii) **accounting/audit** - authorised users shall be individually **accountable** for their access (read, write, modify and delete) and actions (transmit/receive) with regard to classified information within the CJTF. Measures will be implemented by the CJTF security authority/ies (as specified in the OPORD) to detect and prevent users or bodies (inside or outside the CJTF) from breaching or attempting to breach the security environment;

(iii) **confidentiality** - measures shall be taken to prevent the interception or redirection of data communications that carry classified information within the CJTF;

(iv) **integrity** - the integrity of all classified information stored, processed or transmitted within the CJTF shall be maintained; and

(v) **availability** - classified information within the CJTF shall be available to authorised users when required.

DECLASSIFIED/DECLASSIFIÉ - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

MARKING AND CLASSIFICATION

11. The following are the marking and classification requirements :

(a) there will be a requirement to release/disseminate classified information from the planning/preparatory stages of the CJTF onwards. Originators should designate as much classified information as possible as releasable to the CJTF. CJTF commanders and others involved in the CJTF should seek to anticipate classified information requirements at the earliest possible stage and seek approval for its release/dissemination as outlined in paragraph 12 below. Separate compartments for **NATO only** and for **NATO classified information released to the CJTF** must be created in order to provide a mechanism to control the circulation of classified information within the CJTF.

(b) information shall be marked and classified as follows :

(i) with an identifying marking - NATO, NATO nation, non-NATO nation or another organisation;

(ii) classified according to NATO Security Policy - RESTRICTED, CONFIDENTIAL, SECRET;

(iii) carry a release designator where appropriate:

Either: NATO SECRET
Releasable to (name of CJTF)

or:

(cite NATO nation, non-NATO nation or other organisation)SECRET
Releasable to (cite NATO only or name of the CJTF);

and

(iv) contain any caveats regarding further dissemination :

NATO SECRET
Releasable (cite the name of the CJTF and/or
the name or names of nations) Only

(c) information originated in the theatre of operations by a CJTF component and intended for dissemination throughout the CJTF shall be marked as NATO/CJTF. As a rule, all information of an operational nature originated in theatre shall bear this marking;

(d) component parts of documents classified CONFIDENTIAL and above shall be marked and classified (including by paragraph) by the originator to allow further dissemination of appropriate sections. Original security classifications markings / caveats shall be retained when information is used to prepare composite documents or briefings.

DECLASSIFIED/DECLASSIFIÉ - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

RELEASE AUTHORITY

12. The release authorities are as follows, based on the source/originator of the classified information :

(a) **NATO Nation, Non-NATO Nation or Other Organisation**: Classified information originated by a NATO nation, a non-NATO nation or another organisation may be provided to NATO and/or to the CJTF. Classified information provided exclusively to NATO can only be further released on the authority of the providing nation/organisation.

(b) **NATO**: The NAC is the ultimate authority for the release of NATO classified information to non-NATO recipients. This authority adheres to the principle of originator consent and is delegated in accordance with the requirements of NATO Security Policy (Enclosure "E"). This shall also apply to all NATO classified information previously contributed by NATO nations where the national originator cannot be determined. Classified information originated within elements of the CJTF as NATO-only may subsequently be authorised for release to the CJTF by the originator;

(c) **CJTF**: classified information generated within the CJTF shall generally be marked as NATO/CJTF and may therefore be disseminated, when necessary, throughout the CJTF based on the security clearance and on the need-to-know of the recipient(s). Classified information generated within the CJTF which cannot be disseminated, for whatever reason, to the CJTF as such, shall be handled as either national or NATO classified, and is subject to release as described above. CJTF commanders of OF-6 rank or above may authorise the release of information originated by the CJTF or already released to it to individuals or organisations beyond the CJTF on a need-to-know basis for CJTF force protection and the effectiveness of the CJTF mission.

DECLASSIFIED/DECLASSIFIÉ - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

MINIMUM STANDARDS FOR THE HANDLING AND PROTECTION OF NATO CLASSIFIED INFORMATION (NATO SECRET and Below) TO BE MET BY NON-NATO RECIPIENTS

INTRODUCTION

1. All NATO classified information which is released to a non-NATO recipient is for official use only. It shall, therefore, only be disseminated to individuals with a need-to-know. The recipient shall agree that the minimum standards provided in this document will be met. These security measures only address information classified NS and below. Should it be determined that it is necessary to release information classified CTS to a non-NATO recipient, additional security measures will be required; these additional measures shall be extracted from the pertinent Enclosures of NATO Security Policy and its supporting directives.

PERSONNEL SECURITY CLEARANCE AND AUTHORISATION FOR ACCESS

2. Before an individual is granted access to information classified CONFIDENTIAL or SECRET, he shall be subject to a personnel security clearance procedure which meets the minimum standards below to determine whether he is trustworthy and reliable. When the result of such a procedure is positive, a Personnel Security Clearance shall be granted to the individual by his Security Authority in accordance with the format at Appendix 9.

3. Before an individual is authorised access to classified information, he shall be briefed on the security regulations relevant to the level of classification of the information released and the legal and disciplinary consequences of infractions/breaches of these regulations.

4. When an individual who has been personnel security cleared is designated as a representative of his organisation to a meeting in which classified information is involved or the venue for the meeting is within a secure area, his Security Authority, when requested, will send an Attestation of Security Clearance, in accordance with the format at Appendix 10 to the organisation convening the meeting. The requirements for escorting individuals who do not hold a NATO Personnel Security Clearance remain valid if the meeting takes place in a NATO secure area.

Criteria for Assessing Eligibility for a Personnel Security Clearance

5. The following paragraphs contain the principal criteria for assessing the loyalty, trustworthiness and reliability of an individual in order for him to be granted and to retain a PSC. These paragraphs consider aspects of character and circumstances which may give rise to potential security concerns.

6. Although the criteria apply to the individual being cleared, where appropriate and in accordance with national legislation, a spouse's, cohabitant's or close family member’s character, conduct and circumstances may also be relevant and should be taken into account when considering an individual's eligibility for clearance.

DECLASSIFIED/DECLASSIFIÉ - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

7. The criteria shall be applied to determine if an individual or his spouse, co-habitant, and where appropriate and in accordance with national legislation, close family member :

(a) has committed or attempted to commit, conspired with or aided and abetted another to commit (or attempt to commit) any act of espionage, terrorism, sabotage, treason or sedition;

(b) is, or has been, an associate of spies, terrorists, saboteurs, or of individuals reasonably suspected of being such, unless these associations were authorised in the course of official duty;

(c) is, or has been, a member of any organisation which by violent, subversive or other unlawful means seeks the overthrow of the government of a nation(s), or a change in the form of government of a nation(s);

(d) is, or has recently been, a supporter of any organisation described in sub-paragraph (c) above, or who is, or who has recently been closely associated with members of such organisations.

(e) has deliberately withheld, misrepresented or falsified information of significance, particularly of a security nature, or has deliberately lied in completing the personnel security form or during the course of a security interview;

(f) has been convicted of a criminal offence, or offences indicating habitual criminal tendencies; or has serious financial difficulties or unexplained affluence; or has a history of alcohol dependence, use of illegal drugs and/or misuse of legal drugs;

(g) is or has been involved in conduct, including any form of sexual misconduct, which may give rise to the risk of vulnerability to blackmail or pressure;

(h) has demonstrated, by act or through speech, dishonesty, disloyalty, unreliability, untrustworthiness or indiscretion;

(i) has seriously or repeatedly infringed security regulations; or has attempted, or succeeded in, unauthorised activity in respect to communication and information system(s);

(j) is suffering, or has suffered, from any illness or mental or emotional condition which may cause significant defects in his judgement or reliability or may make the individual, unintentionally, a potential security risk. In all such cases competent medical advice should be sought; or

(k) may be liable to pressure through relatives or close associates who could be vulnerable to foreign intelligence services, terrorist groups or other subversive organisations or individuals.

DECLASSIFIED/DECLASSIFIÉ - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

Investigative Requirements for NATO CONFIDENTIAL and NATO SECRET Clearances

8. The initial security clearance for access to information classified NC and NS shall be based on enquiries covering at least the last 5 years, or from age 18 to the present, whichever is the shorter; and shall include the following :

(a) the completion of a **Personnel Security Questionnaire** (which can be either NATO or national);

(b) **identity check / citizenship / nationality status** – the individual's date and place of birth shall be verified and his identity checked. Citizenship status and/or nationality, past and present, of the individual shall be established; this shall include an assessment of any vulnerability to pressure from foreign sources; for example, due to former residence or past associations; and

(c) **national and local records check** – a check shall be made of national security and central criminal records, where these latter exist, and/or other comparable governmental and police records for any officially recorded indication of disloyalty or unreliability. The records of law enforcement agencies with legal jurisdiction where the individual has resided or been employed for at least six months shall be checked.

REGISTRIES AND THE CONTROL OF CLASSIFIED INFORMATION

9. A registry system shall be established by the recipient for the receipt, dispatch, control and storage of classified information. This shall include a Central Registry and other registries as necessary. Registries shall be responsible for :

(a) the recording of the receipt and dispatch of all classified information;

(b) the distribution and control of all classified information within the nation/organisation served;

(c) the storage of the classified information; and

(d) the final disposal of the classified information, including the maintenance of:

(i) destruction certificates for all information classified SECRET;

(ii) log books or document registers for information classified RESTRICTED or CONFIDENTIAL.

DECLASSIFIED/DECLASSIFIÉ - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

REQUIREMENTS FOR THE HANDLING, STORAGE, AND TRANSMISSION OF NATO CLASSIFIED INFORMATION

10. These are as follows :

(a) **NATO SECRET** information shall be handled, displayed, processed and stored in areas to which access is strictly controlled. Access shall be limited to designated appropriately cleared individuals with an established need-to-know for official purposes. NATO SECRET information shall be stored in security containers with nationally-approved locks, the keys or combinations to which shall be held only by designated security cleared personnel needing access to the stored information to fulfil their official duties. Transmission of documents must be made by official courier or diplomatic bag.

Only cryptographic systems specifically authorised by the NAMILCOM shall be used for the encryption of information, however transmitted (e.g. electromagnetic), which is classified NATO SECRET. Reproductions and translations of documents classified NATO SECRET may be produced by the addressee under strict observation of the need-to-know principle. Copies of documents classified NATO SECRET must be marked with identifying reproduction copy numbers. The number of reproductions and/or translations of NATO SECRET documents and their copy numbers must be recorded by the registry (or sub-registry);

(b) **NATO CONFIDENTIAL** information shall be handled, displayed, processed and stored in areas to which access is strictly controlled. Access shall be restricted to designated individuals who have been appropriately cleared and have an established need-to-know for official purposes. Information shall be stored in security containers with nationally-approved locks, the keys or combinations to which shall be held by designated security personnel. Transmission of documents must be by official courier or diplomatic bag. Cryptographic systems approved by a NATO member nation or by the NAMILCOM shall be used for the encryption of NATO CONFIDENTIAL information transmitted by electromagnetic means. Reproductions and translations of documents classified NATO CONFIDENTIAL may be produced by the addressee under strict observation of the need-to-know principle;

(c) **NATO RESTRICTED information** shall be handled, displayed, processed and stored in a manner that deters unauthorised access; for example, in a locked desk, cabinet or room to which access is controlled. Documents may be sent through postal channels by such means as are authorised by the appropriate NSA. Cryptographic systems approved by a NATO member nation or by the NAMILCOM shall be used for the encryption of NATO RESTRICTED information transmitted by electromagnetic means. In exceptional circumstances, when speed is of paramount importance and means of encryption are not available, information classified NATO RESTRICTED may be transmitted electromagnetically in clear text over public systems. Reproductions and translations of documents classified NATO RESTRICTED may be produced by the addressee under strict observation of the need-to-know principle.

DECLASSIFIED/DECLASSIFIÉ - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

COMMUNICATION AND INFORMATION SYSTEMS

11. Non-NATO communication and information systems used for the processing/storage/transmission of NATO classified information shall meet the standards required by NATO Security Policy and supporting directives.

BREACHES OR COMPROMISES OF SECURITY

12. Whenever a breach/compromise of security affecting classified information is discovered:

(a) a report giving details of the breach/compromise shall be sent immediately to the NOS; and

(b) an investigation into the circumstances of the breach/compromise must be made. When completed, a full report must be submitted to the NOS. At the conclusion of this investigation, remedial or corrective action, where appropriate, shall be taken and the NOS notified. In all cases the originator shall be informed.

13. Reports shall contain the following information:

(a) a description of the information involved, including its classification and marking reference and copy number, date, originator, subject and scope;

(b) a very brief description of the circumstances of the compromise, including the date, the period during which the information was exposed to compromise and, if known, the number and/or category of unauthorised individuals who have or could have had access; and

(c) whether the originator has been informed.

INSPECTIONS

14. A non-NATO recipient participating in a NAC approved activity shall facilitate periodic inspections by the NOS to ensure that the security arrangements for the protection of released information meet the minimum standards dictated in this Annex.

ADMINISTRATIVE ARRANGEMENTS TO BE IMPLEMENTED BY NON-NATO RECIPIENTS

15. Non-NATO recipients shall appoint a Security Authority responsible for the implementation of security arrangements and procedures under the Security Agreement and shall identify this authority to NOS which is the equivalent security authority for NATO. The NOS shall establish liaison with the Security Authority of the non-NATO recipient to facilitate implementation of these security arrangements and procedures.

DECLASSIFIED/DECLASSIFIÉ - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

16. In accordance with the provisions contained in the Security Agreement, the NOS and the Security Authority of a non-NATO recipient must establish to their satisfaction that the recipient party will protect the classified information it receives as required by the originator.

17. The administrative arrangements shall cover, as required, the establishment of:

(a) a Security Authority which shall implement and oversee the security measures for the protection of classified information released and classified information exchanged in the cooperative activity;

(b) a registry system, including a Central Registry and other registries as required by the non-NATO recipient;

(c) procedures for the recording, control and destruction of classified information;

(d) standards of security containers used for the storage of classified information;

(e) channels of transmission;

(f) personnel security clearance procedures; and

(g) a system and procedures for the investigation of compromises/breaches of security.

18. After signature of the Security Agreement and the completion of the administrative arrangements, and before the exchange of classified information begins, the NOS shall, and non NATO recipients may, carry out a survey of the preparations made by an intended non-NATO recipient or NATO respectively for the handling and storage of the classified information to be exchanged. A copy of the NOS survey report shall be provided to the intended non-NATO recipient.

DECLASSIFIED/DECLASSIFIÉ - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

SECURITY ASSURANCE

A Security Assurance provided by a non-NATO recipient of NATO classified information shall contain the following certification:

The government of the

…….
(cite the applicable nation or organisation)

represented by

…….
(cite the signatory's name and position) [1]

in furtherance of participation in

……...
(cite the name of the NAC approved activity, e.g., CJTF or other programme or operation)

hereby agrees:

(a) to protect classified information provided to it by (name of the CJTF or other programme or operation) in accordance with the Annex to this Assurance;

(b) to provide such classified information only to appropriately cleared individuals under its jurisdiction with a need-to-know;

(c) to use such information only for the purposes for which it was provided;

(d) not to transfer such information to a third party without the prior written approval of the originator of the information; and

(e) to continue to abide by these security requirements of the Annex to this Assurance even after completion of (name of the CJTF or other programme or operation).

[1] The signatory is an officially authorised representative who is either the direct recipient of released information or is a senior representative responsible for ensuring the protection of information released in support of a co-operative activity.

DECLASSIFIED/DECLASSIFIÉ - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

MINIMUM STANDARDS FOR THE PROTECTION OF NATO/ (1) CLASSIFIED INFORMATION

(applicable Nation or Organisation)

Security Clearance and Authorisation for Access

1. Before an individual is granted access to NATO/ (1) classified information, he will be subject to a security clearance procedure designed to determine whether the individual is loyal and trustworthy. When the result of such a procedure is positive, the recipient nation/organisation is to produce an Attestation of Personnel Security Clearance in accordance with the format at Attachment 2 to this Annex, which is to be forwarded to the (2) Security Office.

2. Upon receipt of the Attestation of Personnel Security Clearance, the (2) Security office will authorize access to information and areas, in accordance with the individual's need-to-know.

3. The individual shall be briefed by the (2) Security Office on the security regulations relevant to the classification of the information he is going to have access to.

Definitions of Classification Markings

4. The following principles apply to the classification of NATO/ (1) information:

(a) NATO/(1) SECRET
The unauthorised disclosure of which would result in grave damage to the NATO and (2) mission.

(b) NATO/(1) CONFIDENTIAL
The unauthorised disclosure of which would be damaging to the NATO and (2) mission.

(c) NATO/(1) RESTRICTED
The unauthorised disclosure of which would be detrimental to the interests or effectiveness of the NATO and (2) mission.

Requirements for Receipt, Handling, Storage and passing on of NATO/ (1) Classified Information

5. **Receipt/Registration**. A Registry system shall be established by the recipient for the receipt, dispatch, control and storage of classified information. Sub-registries may be established as necessary. Registries shall be responsible for:

(a) The recording of the receipt and dispatch of all NATO/(1) classified information;

(b) The distribution and control of all NATO/(1) classified information within the nation/organisation served;

DECLASSIFIED/DECLASSIFIÉ - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

(c) The storage and final disposal of all NATO/(1) classified information which must include:

(1) Destruction certificates for all information classified NATO/ (1) SECRET;

(2) Logbooks and registers for all information classified NATO/ (1) RESTRICTED or CONFIDENTIAL.

6. **Handling, Storage and passing on**. The following rules and regulations apply for the handling, storage and passing on of NATO/ (1) classified information:

(a) **NATO/(1) SECRET**
NATO/ (1) SECRET information shall be handled, displayed, processed and stored in areas to which access is strictly controlled. Access shall be limited to designated, appropriately cleared individuals with an established need-to-know for official purposes. NATO/ (1) SECRET information shall be stored in security containers with nationally-approved locks, the keys or combinations to which shall be held only by designated, security cleared personnel, who require access to the stored information in order to fulfil their official duties. Transmission of documents must be made by official courier or diplomatic bag.

(b) Copies of classified information are not to be made without prior authorisation from (2) HQ J2 Chief/Head of Security Office. If authorised, copies of NATO/ (1) SECRET may only be released to appropriately cleared individuals and only on strict observation of the need-to-know principle. Copies of documents classified NATO/ (1) SECRET must be marked with identifying reproduction copy numbers and must be recorded by the registry (or sub-registry).

(c) **NATO/(1) CONFIDENTIAL**
NATO/ (1) CONFIDENTIAL information shall be handled, displayed, processed and stored in areas to which access is strictly controlled. Access shall be restricted to designated individuals who have been appropriately cleared and have an established need-to-know for official purposes. Information shall be stored in security containers with nationally approved locks, the keys or combinations to which shall be held by designated security personnel. Transmission of documents must be by official courier or diplomatic bag. Copies of classified information are not to be made without prior authorisation from (2) HQ J2-Chief/Head of Security Office. If authorised, copies of NATO/ (1) CONFIDENTIAL may only be released to appropriately cleared individuals and only on strict observation of the need-to-know principle.

(d) **NATO/(1) RESTRICTED**
NATO/ (1) RESTRICTED information shall be handled, displayed, processed and stored in a manner that deters unauthorised access; for example, in a locked desk, cabinet or room to which access is controlled. Copies of classified information are not to be made without prior authorisation from (2) HQ J2 Chief/Head of Security office, If authorised, copies of NATO/ (1) RESTRICTED may only be released to appropriately cleared individuals and only on strict observation of the need-to-know principle.

DECLASSIFIED/DECLASSIFIÉ - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

7. Destruction and Disposal. Classified information, which is no longer required for official purposes, including surplus or superseded information and waste, shall be destroyed in such a manner as to ensure that it cannot be reconstructed.

8. The destruction of information classified NATO/ (1) SECRET is to be recorded. The record is to be signed by the destruction official and an independent witness, both of whom shall be appropriately cleared and authorised to have access to NATO/ (1)SECRET information. Destruction certificates and control records for information classified NATO/ (1) SECRET are to be retained in the registry or office performing the destruction for a period of not less than 5 years.

Breaches or Compromises of Security

9. Whenever a breach or compromise of security affecting classified documents is discovered, an initial report giving details of the breach/compromise must be sent immediately to (2) HQ Security Officer (SO). An investigation into the circumstances of the breach/compromise must be carried out immediately in conjunction with (2) HQ SO and a full report is to be sent to the NOS. At the conclusion of this investigation, remedial or corrective action, where appropriate, shall be taken and the NOS notified. In all cases, the originator shall be informed by the NATO Office of Security.

10. The initial breach/compromise report is to contain the following information:

(a) A description of the information involved, including its classification, marking reference, copy number, date, originator, subject and scope.

(b) A brief description of the circumstances of the compromise, including the date, the period during which the information was exposed to compromise.

(c) If known, the number and/or category of unauthorised individuals who have or could have had access to the document.

(d) Whether the originator has been informed.

Security Surveys

11. The Government/Organisation ..... will facilitate periodic Surveys by NOS (or Delegated Authorities) to ensure that the security arrangements for the protection of released information meet the minimum established standards.

NOTE:

(1) Name of the NAC-approved Activity

(2) Applicable Nation, Organisation or Command

DECLASSIFIED/DECLASSIFIÉ - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

ATTESTATION OF PERSONNEL SECURITY CLEARANCE

1. Certification is hereby given that.

Full Name (LAST NAME, Middle Name(s), First Name):

…….

Title/Rank:

…….

Date and Place of Birth (DD/MM/YYYY, City, Country):

…….

has been authorised to have security clearance by:

…….
(the Government of/name of Organisation)

in accordance with national laws and regulations in compliance with the provisions of the Security Assurance (2) signed by
…….

(the Government of/name of Organisation)

is deemed suitable to be entrusted with information classified up to and including (see Note below):
…….
…….
…….

Note. Insert, as appropriate, one of the following:

(a) NATO/(1) SECRET

(b) NATO/(1) CONFIDENTIAL

2. The validity of this certificate will not expire later than:
……

Signed: ……. (Official stamp)

Title: …….

Date: …….

DECLASSIFIED/DECLASSIFIÉ - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

PERSONNEL SECURITY CLEARANCE CERTIFICATE
(for non-NATO national)

1. Certification is hereby given that:

Full Name (Last Name, First Name):
.....

Date and Place of Birth:
.....

has been granted a Personnel Security Clearance by the Government of:
.....

in accordance with the provisions of the Security Agreement between NATO and **[nation]**, in accordance with security requirements no less stringent than those of NATO, has been briefed on the security regulations for the protection of NATO information and the legal and disciplinary consequences of infraction / breaches of those regulations, and is, therefore, declared suitable to be entrusted with information classified up to and including:

NATO SECRET(*) NATO CONFIDENTIAL(*)

2. The validity of this certificate will expire not later than:
.....

3. Issued by:

Name and address of the issuing authority:
……
……

Contact details of the issuing authority (Phone, e-mail, fax):
……

Full name (Last Name, First Name):

Title:

Signature: Official government stamp

Date:

(*) Delete as appropriate
(**) The marking is not part of the template.

DECLASSIFIED/DECLASSIFIÉ - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

ATTESTATION OF PERSONNEL SECURITY CLEARANCE
(for non-NATO national)

1. Attestation is hereby given that:

Full Name (Last Name, First Name):
……

Date and Place of Birth:
……

Where employed:
……

Purpose and Duration:
……
……
Holder of Passport/Identity Card No: ……...
Issued at: …….....
Dated: .....……

has been granted a Personnel Security Clearance for NATO classified information in accordance with security requirements no less stringent than those of NATO, has been briefed on the security regulations for the protection of NATO information and the legal and disciplinary consequences of infraction / breaches of those regulations, and is, therefore, declared suitable to be entrusted with information classified up to and including:

NATO SECRET(*) NATO CONFIDENTIAL(*)

2. The validity of the attestation will expire no later than:
…….....

3. Issued by:

Name and address of the issuing authority:
……...
……
Contact details of the issuing authority (Phone, e-mail, fax):
……..

Full name (Last Name, First Name):

Title:

Signature: Official stamp

Date:

(*) Delete as appropriate
(**) The marking is not part of the template.

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

NATO OTAN
NORTH ATLANTIC COUNCIL
CONSEIL DE L'ATLANTIQUE NORD

NATO UNCLASSIFIED

13 May 2015

DOCUMENT
AC/35-D/2003-REV5

SECURITY COMMITTEE

DIRECTIVE ON CLASSIFIED PROJECT AND INDUSTRIAL SECURITY

Note by the Acting Chairman

1. At Annex is the fifth revision of the Directive on Classified Project and Industrial Security which is published in support of the NATO Security Policy, C-M(2002)49. It is binding and mandatory in nature upon NATO member nations, commands and agencies.

2. While this revision reflects approved changes and amendments to all sections, the most significant ones are in the Section "Tendering, Negotiation and Letting of Contracts/Sub-Contracts involving classified Information" with focus on pre-contractual security requirements.

3. In addition, two new Sections have been introduced: "Facility Security Officer" and "Handling of NATO Classified Information in Communication and Information Systems (CIS)". Specific attention should also be paid to activities/scenarios involving NATO RESTRICTED Information.

4. This document has been approved by the Security Committee (SC) in Security Policy Format (SP) under the silence procedure (AC/35-WP(2011)0010-REV11 (SP) refers) and will be subject to periodic review.

5. This document replaces AC/35-D/2003-REV4 which should be destroyed.

(Signed) Marco Criscuolo

Annex: 1
15 appendices

Action officer: Rolf Ultes, NOS/POB, ext. 4680
Original: English

NHQD5223

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

DIRECTIVE ON CLASSIFIED PROJECT AND INDUSTRIAL SECURITY

TABLE OF CONTENTS

INTRODUCTION 1-5

Scope 1-5

Authority 1-5

TENDERING, NEGOTIATION AND LETTING OF CONTRACTS/SUB-CONTRACTS INVOLVING CLASSIFIED INFORMATION 1-6

Contracts/Sub-contracts in NATO Nations 1-6

General 1-6

Tendering Process 1-6

Access to Information Classified NATO CONFIDENTIAL or above during the Tendering Process 1-6

Access to Information classified NATO RESTRICTED during the Tender Process 1-7

Unsuccessful Bidders 1-7

Negotiations 1-7

Letting 1-8

Contracts involving NATO RESTRICTED Information 1-8

Contracts involving Information classified NATO CONFIDENTIAL or above 1-8

Programme/Project Security Instruction and Security Aspects Letter 1-8

Notification of Contracts 1-9

30. ..... Contractors/Sub-contractors under the jurisdiction of a NATO Nation requiring by their national laws and regulations notification of contracts involving NR as detailed in Appendix 3 shall notify their NSA/DSA about any such contracts they have been awarded. 1-9

Contracts/Sub-contracts with Contractors in Non-NATO Nations 1-9

Termination of Contracts involving Classified Information 1-10

INDUSTRIAL SECURITY CLEARANCES 1-10

Facility Security Clearances 1-10

Contractor's Personnel performing work on NATO Premises or on other Contractor's Facilities 1-11

Changes to or Revocation of FSC 1-11

FACILITY SECURITY OFFICER 1-11

PERSONNEL SECURITY CLEARANCES 1-13

General Provisions 1-13

Contractual Conditions 1-13

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

Initiating Personnel Security Clearance Procedures 1-13

Revalidation 1-13

Procedures to be followed when a PSC is suspended or revoked 1-13

Procedures to be followed when a PSC is denied 1-14

PSC of an Employee holding the Nationality/Citizenship of another Nation 1-14

Multiple Nationalities 1-15

Provisional PSC 1-15

Verification 1-15

Security Awareness and Briefings of Individuals 1-15

PROGRAMME/PROJECT SECURITY 1-16

Introduction 1-16

Principles 1-16

Programme/Project Security Instruction 1-16

RELEASE OF NATO CLASSIFIED INFORMATION BY PROGRAMME/PROJECT PARTICIPANTS AND CONTRACTORS/SUB-CONTRACTORS 1-18

Security Arrangements for the Release of NATO Classified Information to non-NATO Nations and International Organizations 1-18

Procedures to be followed for the Release of NATO Classified Programme/Project Information to non-Programme/Project Participants from NATO Nations 1-18

HANDLING OF NATO CLASSIFIED INFORMATION IN COMMUNICATION AND INFORMATION SYSTEMS (CIS) 1-18

General 1-18

INTERNATIONAL VISIT CONTROL PROCEDURES (IVCPs) 1-19

Requirements and Procedures for Visits 1-19

INTERNATIONAL TRANSMISSION AND TRANSPORTATION OF NATO CLASSIFIED MATERIAL 1-20

General 1-20

International Hand Carriage of NATO Classified Material at NC or NS level 1-20

General 1-20

Security Arrangements 1-20

Procedure 1-20

Carriage of Material at the level NC by Commercial Courier Companies 1-21

Transportation of NATO Classified Material NC or NS as Freight 1-22

Transportation of NATO Classified Material NC or NS as Freight by Road 1-22

Transportation of NATO Classified Material NC or NS as Freight by Rail 1-23

Transportation of NATO Classified Material NC or NS as Freight by Sea 1-23

Transportation of NATO Classified Material NC or NS as Freight by Aircraft 1-24

Security Principles applicable to all Forms of Transportation 1-25

Countries presenting special Security Risks 1-25

Customs 1-25

Acknowledgement 1-25

Packaging 1-25

Security Guards and Escorts 1-25

Transportation of Explosives, Propellants or Other Dangerous Substances 1-26

GLOSSARY AND ACRONYMS 1-27

20. ..... Contractors/Sub-contractors under the jurisdiction of a NATO Nation requiring by their national laws and regulations notification of contracts involving NR shall notify their NSA/DSA about any such contracts they have been awarded. 1-43

E-mail: ivcp@uvns.hr 1-73

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

The following Appendices to this Directive address the specific procedures, arrangements, and sample documents:

(a)	APPENDIX 1 -	General Responsibilities;
(b)	APPENDIX 2 -	Facility Security Clearance Information Sheet (FSCIS);
(c)	APPENDIX 3 -	Facility and Personnel Security Clearance for Contracts involving NATO RESTRICTED Information - National requirements;
(d)	APPENDIX 4 -	Contract Security Clause for Inclusion in Tenders and Contracts involving NATO RESTRICTED Information;
(e)	APPENDIX 5 -	Security Aspects Letter (SAL);
(f)	APPENDIX 6 -	Project Security Instructions (PSIs) - Structure and Content;
(g)	APPENDIX 7 -	Facilities/Organisations List;
(h)	APPENDIX 8 -	International Visits Control Procedures (IVCPs);
(i)	APPENDIX 9 -	International Visits Processing Times/Lead Times and NU or NR notification requirements;
(j)	APPENDIX 10 -	Security Acknowledgement (in case of Hand Carriage) - Declaration;
(k)	APPENDIX 11 -	Courier Certificate for the International Hand Carriage of classified Documents, Equipment and/or Components;
(l)	APPENDIX 12 -	International Transportation Plan - Transportation Plan for the Movement of Classified Consignments;
(m)	APPENDIX 13 -	Authorisation for Security Guards;
(n)	APPENDIX 14 -	NATO Personnel Security Clearance Certificate (PSCC);
(o)	APPENDIX 15 -	Attestation of a NATO Personnel Security Clearance (APSC).

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

DIRECTIVE ON CLASSIFIED PROJECT AND INDUSTRIAL SECURITY

INTRODUCTION

1. Industrial security is the application of protective measures and procedures to prevent, detect and recover from loss or compromise of classified information handled by industry in contracts. NATO classified information disseminated to industry, generated as a result of a contract with industry, and contracts involving classified information with industry shall be protected to a standard no less stringent than NATO Security Policy (C-M(2002)49) and supporting Directives.

2. This Directive is published by the Security Committee (SC) pursuant to paragraph 5.7 of Enclosure “B” and in support of Enclosure “G“ to the NATO Security Policy (C-M(2002)49).

3. This Directive contains mandatory minimum standards, common procedures and processes in connection with the implementation of industrial security.

Scope

4. This Directive applies to the protection of NATO classified information released or created during all phases of the contracting processes, including licensing, bidding, negotiation, award, performance, and termination. The protection of NATO UNCLASSIFIED information is governed by C-M(2002)60, The Management of Non-Classified Information, and is addressed in this Directive only if required for consistency.

5. The provisions outlined in this Directive are applicable to NATO, NATO Programme/Project Agency/Offices (NPA/NPOs), National Security Authorities (NSA), Designated Security Authorities (DSA), National Security Accreditation Authorities (SAAs) and any other competent national authorities that let contracts involving NATO classified information to Contractors. The following definitions apply:

Contracting Authority:
An organization in NATO or NATO nations including Contractors authorised to tender for, or place a contract with a Contractor or Consultant.

Contractor:
An industrial, commercial or other entity that seeks or agrees to provide goods or services.

Consultant:
An individual who serves either independently or through a Contractor in an advisory capacity. A Consultant expresses views, gives opinions on problems, answers questions as requested or provides advice. The work performed under contract is the provision of advice. Therefore, for the purpose of this Directive, a Consultant is considered the same as a Contractor. Hereafter, referred to as Contractor.

Authority

6. The NSAs/DSAs/SAAs are responsible for the implementation and oversight of security for NATO classified information entrusted to their Contractors. The NSAs/DSAs/SAAs shall ensure that they have the means to make their security requirements binding upon Contractors and that they have the right to inspect and approve the measures taken by Contractors in compliance with this Directive for the protection of NATO classified information.

7. Detailed responsibilities of the NSAs/DSAs, the SC, the NATO Office of Security (NOS), and NPA/NPOs are laid down in Appendix 1. Principle organisations with responsibility for CIS security, e.g. SAAs are addressed in Enclosure “F”.

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

TENDERING, NEGOTIATION AND LETTING OF CONTRACTS/SUB-CONTRACTS INVOLVING CLASSIFIED INFORMATION

Contracts/Sub-contracts in NATO Nations

General

8. All Contractors/Sub-contractors undertaking a NATO contract involving classified information requiring access to, or generation of information classified NATO CONFIDENTIAL (NC) or above shall hold or, in respect of paragraph 11 (b) and (c) below, be able to obtain a Facility Security Clearance (FSC) at the appropriate level issued by the responsible NSA/DSA of the country that has jurisdiction[1] over the Contractor/Sub-contractor's facility. It is the responsibility of the Contracting Authority to verify with the relevant NSA/DSA of a Contractor/Sub-contractor whether it has been granted an appropriate FSC before any NC or above information is released to it. Where no FSC at the required level exist it is the responsibility of the Contracting Authority to initiate an FSC or upgrade action.

9. A FSC is not required by Enclosure G to C-M(2002)49 for access to, or generation of classified information at level of NATO RESTRICTED (NR). However some NATO nations, as identified in Appendix 3, and as mandated by their national laws and regulations, do require a FSC for Contractor/Sub-contractor under their jurisdiction, for access to classified information at the level of NR.

Tendering Process

Access to Information Classified NATO CONFIDENTIAL or above during the Tendering Process

10. A bidder, not holding an appropriate FSC as required by the potential contract/sub-contract shall not be automatically excluded from the competition during the tendering process, as detailed in the scenarios below.

11. The following identifies the three scenarios that may arise during the tendering process for a contract/sub-contract involving classified information NC or above and details the security requirements:

(a) access to classified information NC or above at the bidder's facility during the tendering process:

- when the contract notice, invitation to tender or request for proposals require bidders to hold or generate at their facility information classified NC or above, the bidder's facility shall hold an FSC at the appropriate level. In such circumstances the Contracting Authority shall obtain an assurance from the relevant NSA/DSA that the bidder has been granted an appropriate FSC;
- the Contracting Authority shall obtain the respective assurance from the responsible NSA/DSA by using the Facility Security Clearance Information Sheet (FSCIS) at Appendix 2.

(b) no access to information classified NC or above during the tendering process:

- when the contract/sub-contract notice, invitation to tender or request for proposal concerns a contract/sub-contract that will involve classified information NC or above but does not require the bidder to hold or originate such information at the tender stage, a bidder not holding an appropriate FSC shall not be excluded from the bidding process, but should be advised in the tender document that an FSC shall be required prior to it being awarded the contract/sub-contract;

[1] Power to exercise authority over a subject matter or a territory/geographic area

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

- should a bidder without an appropriate FSC be selected to undertake the contract/sub-contract, the Contracting Authority shall initiate action to grant the bidder an FSC at the required level;
- the contract/sub-contract shall not be awarded until the NSA/DSA has provided an assurance that the selected bidder's facility has been granted an FSC at the required level. The Contracting Authority shall initiate the FSC action by using the FSCIS at Appendix 2.

(c) access to information classified NC or above at the premises of the contracting authorities during the tendering process:

- shall only be granted to individuals who are in the possession of an appropriate Personnel Security Clearance (PSC). An assurance of the PSC of individuals requiring access on the premises of the Contracting Authority shall be provided in the form of a PSC Certificate or a Request for Visit by the appropriate NSA/DSA;
- should a bidder without an appropriate FSC be selected to undertake the contract/sub-contract, the Contracting Authority shall request the relevant NSA/DSA to initiate action to grant the bidder an FSC at the required level;
- the contract/sub-contract shall not be awarded until the NSA/DSA has provided an assurance that the selected bidder's facility has been granted an FSC at the required level. The Contracting Authority shall request the responsible NSA/DSA to initiate the FSC action by using the FSCIS at Appendix 2.

12. Should the NSA/DSA determine that a bidder is ineligible for the required level of FSC the Contracting Authority shall not award the contract.

Access to Information classified NATO RESTRICTED during the Tender Process

13. When the contract notice, invitation to tender or request for proposals require bidders to hold or generate NR information, the contract notice, the invitation to tender or request for proposal shall include a copy of the "Contract Security Clause for Inclusion in Tenders and Contracts Involving NR Information" at Appendix 4. This will inform the bidder on the minimum measures required for the protection of NR classified information.

Unsuccessful Bidders

14. Unsuccessful bidders having been provided NATO classified information in connection with a tender shall be required to return the classified information to the Contracting Authority within 15 working days of receipt of notification of their unsuccessful tender. All individuals having accessed NATO classified information shall be reminded of their responsibility for its protection and of not disclosing such information further.

Negotiations

15. Following the tendering process and at the start of the negotiations for contracts involving NC or above with preferred bidders, if not already confirmed, an assurance shall be obtained that the potential Contractor(s) hold(s) an FSC at the required level. If the Contracting Authority is a NATO civil and military body the request shall be forwarded to the NSA/DSA of the nation with jurisdiction over the potential Contractor(s). If the Contracting Authority is in a NATO nation, the request shall be forwarded to its responsible NSA/DSA. The Contracting Authority shall ensure that all Contractors are required to follow the same approval process when negotiating a sub-contract.

16. In case the potential Contractor does not hold the required FSC, the responsible NSA/DSA shall be requested to initiate the clearance procedure accordingly. For such purposes the FSCIS at Appendix 2 shall be used.

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

17. The Contracting Authority shall also provide information regarding the classification level to the responsible NSA/DSA and the nature of services or supplies requiring access or potential access to NATO classified information in order to allow the responsible NSA/DSA to ensure the necessary security arrangements have been implemented.

Letting

18. Contracting authorities will not normally award a contract involving classified information NC or above before having obtained assurance that the Contractor's facility holds an FSC at the required level. Exceptionally and after consulting with the relevant NSA/DSA, the Contracting Authority may allow the Contractor to commence work on the NR parts of the contract provided the contractual arrangement includes a clause stating that the contract shall be terminated in case the Contractor cannot be granted the required FSC.

Contracts involving NATO RESTRICTED Information

19. Contracts involving classified information at the level of NR shall include a "Contract Security Clause for Tenders and Contracts Involving NR Information" detailing, as a minimum, the provisions specified in Appendix 4. Such contracts shall also include a Security Aspects Letter (SAL) (see Appendix 5) identifying the specific NR aspects of the contract requiring protection.

20. The requirements in contracts for the protection of NR information may be more stringent than that detailed in Appendix 4 and, if required by national laws and regulations, NSAs/DSAs will be responsible for ensuring compliance of Contractors/Sub-contractors being under their jurisdiction with applicable security provisions for the protection of NR information and should conduct verification visits on Contractor's facilities located in their nation. In all other cases it is the responsibility of the Contracting Authority to ensure that the required security provisions of Appendix 4 and the SAL, as applicable, are implemented. Any incident, which has or may lead to NR information being lost or compromised, shall immediately be reported by the SO to the Contracting Authority, which shall inform the competent NATO body or the Contractor's NSA/DSA, as applicable.

Contracts involving Information classified NATO CONFIDENTIAL or above

21. Contracts/sub-contracts involving access to information classified NC or above shall include an article/paragraph, which requires the Contractor/Sub-contractor to protect any such classified information no less stringently than applicable NATO security regulations as implemented by its competent NSA/DSA, and comply with any relevant national security laws and regulations and any additional instructions given by the responsible NSA/DSA. Contract specific NATO security requirements shall be given either in a Programme Security Instruction (PSI) (see Appendix 6) or in a SAL, as appropriate.

Performance of Contracts within Class II Security Areas

22. In accordance with AC/35-D/2001, Directive on Physical Security, unescorted access to Class II Security Areas shall only be granted to individuals who are security cleared. For all other individuals, provisions shall be made for escorts or equivalent controls to prevent unauthorised access to NATO classified information. If escort arrangements or equivalent controls are not feasible, the requirement for individuals to hold an appropriate PSC when the execution of the contract starts shall be clearly stated in the invitation to bid.

Programme/Project Security Instruction and Security Aspects Letter

23. For all programmes involving classified information NC or above managed by an NPA/NPO, the programme security office shall produce a PSI (see Appendix 6) in collaboration with and subject to approval by the NSA/DSA of the NATO nation(s) participating in the programme. PSIs may be produced for other activities if considered necessary by the appropriate security authorities. Security classifications shall be addressed in the Security

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

Classification Guide (SCG). If considered appropriate by the NPA/NPO and programme participants a PSI may also be produced for programmes involving only classified information at the NR level.

24. Contracts which do not require a PSI shall include as a minimum an SAL. In that case security classifications shall be addressed in a Security Classification Checklist.

25. The PSI and/or SAL shall be made binding for all participants.

Notification of Contracts

26. NATO contracting authorities shall notify, via their respective security officers, the NSA/DSA of the nation with jurisdiction over the Contractor about any contracts involving classified information at the level of NC or above, to include details on the nature of services or supplies or work to be performed by the Contractor, the security classification, the nature and volume of classified information to be furnished to or to be generated by the Contractor as well as any other relevant security aspects.

27. Each NPA/NPO shall develop and maintain an up-to-date list of facilities and involved organisations. The list shall be in the format at Appendix 7 and be available to all NSAs/DSAs and NATO civil and military bodies upon request. The list consists of:

(a) the prime Contractors that hold contracts involving classified information NC or above connected with the NATO project/programme;

(b) all government departments or agencies known to be involved in the project/programme; and

(c) any civil or military body involved, when applicable.

28. Each NPA/NPO shall also be responsible for requiring that each prime Contractor maintains a similar list for any Sub-contractors, by project, with access to information classified NC or above.

29. Other contracting authorities awarding a NATO classified prime contract involving classified information at the level of NC or above, shall provide their NSA/DSA with a copy of the security provisions of the contract and the PSI/SAL. That NSA/DSA shall provide copies of the security provisions and PSI/SAL to the NSA/DSA of the country with jurisdiction over the Contractor so that security oversight of the classified information can be maintained.

30. Contractors/Sub-contractors under the jurisdiction of a NATO Nation requiring by their national laws and regulations notification of contracts involving NR as detailed in Appendix 3 shall notify their NSA/DSA about any such contracts they have been awarded.

Contracts/Sub-contracts with Contractors in Non-NATO Nations

31. The letting of the contract involving NATO classified information to Contractors in non-NATO nations constitutes a release of information and has to be in accordance with the established procedures as referenced in paragraph 91.

32. Contracts/sub-contracts with Contractors/Sub-contractors in non-NATO nations which involve NATO classified information require the existence of a bilateral Security Agreement/Arrangement between NATO and the non-NATO nation whose NSA/DSA has jurisdiction over the Contractors/Sub-contractors. It is the responsibility of that NSA/DSA to ensure their Contractors/Sub-contractors provide the required level of protection for the contract involving NATO classified information.

33. If there is no bilateral Security Agreement/Arrangement between NATO and the non-NATO nation, a bilateral Security Agreement/Arrangement between

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

a contracting/sponsoring NATO Nation and the non-NATO Nation is required. The NATO Nation shall provide a written Security Assurance signed by a representative duly mandated by the Non-NATO recipient, to NATO. The Security Assurance shall oblige the non-NATO recipient to protect NATO classified information to a degree no less stringent than the provisions contained in the bilateral Security Agreement/Arrangement for the protection of the NATO nation's classified information of an equivalent classification.

34. If the NATO Nation which has concluded the Security Agreement/Arrangement with the Non-NATO Nation does not have the jurisdiction over the Contracting Authority, the NSA/DSA of the NATO Nation with jurisdiction over the Contracting Authority must be provided with the Security Assurance as detailed in paragraph 33 above and a copy of the Security Agreement/Arrangement. The written consent of the NATO Nation with jurisdiction over the Contracting Authority is required otherwise the contract shall not be placed.

35. Placing contracts/sub-contracts involving classified NATO information shall follow the procedures as established in paragraphs 8 to 30 above.

Termination of Contracts involving Classified Information

36. Upon termination of a contract/sub-contract involving classified information, and where classified information has been provided to or generated by the Contractor/Sub-contractor during the performance of the contract, the classified information shall be returned to the Contracting Authority unless the Contracting Authority has agreed in writing that the classified information can be destroyed in accordance with the national laws and regulations or retained by the Contractor/Sub-contractor, e.g. for purposes of follow-on services or supplies. Disposition instructions shall be included in any contracts involving access to NC and higher.

INDUSTRIAL SECURITY CLEARANCES

Facility Security Clearances

37. The NSA/DSA of each NATO nation is responsible for granting an appropriate FSC for Contractor's facilities under their jurisdiction and which are involved in NATO contracts involving classified information at NC or above level, in accordance with national laws and regulations. Prior to granting an FSC, an assessment shall be made on the following mandatory minimum requirements:

(a) of the integrity and probity of the company which is to be entrusted with NATO classified information at the level of NC or above;

(b) of the personnel security status of owners, directors, principal officials, executive personnel, and employees of the facility, and of such other individuals as per national laws and regulations who may, by virtue of their association, position or employment, be required to have access to NATO classified information or supervise a NATO contract involving classified information, to ensure that they have the requisite level of PSC;

(c) of the foreign ownership, control and influence aspects (such as corporate structure) to ensure that these aspects are adequately addressed and where necessary mitigated; and

(d) of the security arrangements provided for the protection of NATO classified information to ensure that they comply with the requirements of NATO Security Policy and its supporting directives.

38. An FSC is an administrative determination by which an NSA/DSA formally recognizes the capacity or reliability of Contractor's facilities to manage, generate or have access to classified information up to a certain level. Depending on the contract requirements and, subject to national laws and regulations, there may be different types of FSCs, as determined by the NSA/DSA and are conveyed in the NATO FSCIS.

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

39. The following minimum criteria shall be applied by the NSA/DSA in issuing all categories of FSCs:

(a) that the company must establish security processes which covers all appropriate security requirements for the protection of information classified at NC or above in accordance with NATO security regulations;

(b) that the personnel security status of personnel (both management and employees) who are required to have access to information classified at NC or above is confirmed in accordance with NATO personnel security clearance requirements;

(c) that the NSA/DSA has the means to ensure that the industrial security requirements are binding upon industry and that it has the right to inspect and approve the measures taken in industry for the protection of information classified at NC and above; and

(d) that the company shall appoint a Facility Security Officer (FSO) responsible for security who is in a position to report to the NSA/DSA.

40. In granting an FSC, NSAs/DSAs shall ensure that they have the means to be advised of any circumstances that could have a bearing upon the viability of the clearance granted (e.g. a transfer of the controlling interests in the company or facility, a realignment of the business associations, the replacement of any of its principal officers or directors, a change in the facility's physical location, an alteration to the premises it occupies, or a variation in its security procedures).

41. The NSAs/DSAs shall evaluate the extent to which the circumstances described above represent a threat to the security of NATO classified information that may be entrusted to that company or facility. If it is determined that there is a threat, the NSAs/DSAs will take appropriate steps to negate or mitigate the threat prior to issuing or maintaining the FSC.

42. The responsible NSA/DSA shall confirm the level of the FSC granted to, or initiate facility clearance action for a company, when requested, in the FSCIS format (Appendix 2).

43. The NSA/DSA may specify additional security measures to be taken for the protection of NATO classified information in each company/facility in its nation in order to qualify for an FSC.

Contractor's Personnel performing work on NATO Premises or on other Contractor's Facilities

44. Contractor/Sub-contractor's personnel, including freelance consultants and interpreters, or any other type of freelance personnel or self-employed service providers who carry out works on NATO premises or Contractor's facilities in connection with a classified NATO programme/project or any other type of NATO contract requiring access to information classified NC or above shall hold a PSC at the requisite level and, if required by national laws and regulations, an appropriate FSC.

Changes to or Revocation of FSC

45. Should an NSA/DSA change or withdraw an FSC that it has issued, the NSA/DSA shall at once notify any other NSA/DSA and/or NPA/NPO to which it has provided a clearance notification. The contractual arrangement shall include a clause allowing for the termination of the contract in case of the revocation of the required FSC.

FACILITY SECURITY OFFICER

46. A FSO shall be in place for a Contractor/Sub-contractor to be granted an FSC. The FSO will be responsible for the overall protection of NATO classified information and obliged to ensure the effective implementation of security requirements and procedures within the facility involved in any contract/sub-contract requiring access to NATO classified information.

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

47. The FSO shall, in accordance with national laws and regulations, serve as the main point of contact between the Contractor/Sub-contractor and the Contracting Authority or relevant NSA/DSA for all security related aspects. When appointing the FSO, the following requirements apply:

(a) the FSO shall be:
- a citizen of the nation where the facility is located, or a citizen of a NATO nation *(for contracts involving classified information NC and above);*
- an employee of the Contractor/Sub-contractor;
- granted a PSC at the appropriate level;
- a part of the facility's management, or reporting directly to one of the members of the management in order to exercise security authority;

(b) the FSO shall undertake appropriate briefing and/or training regarding protective security and threat awareness;

(c) the responsible NSA/DSA should endeavour to create and maintain a close cooperation with the FSO.

48. The FSO is responsible for the following tasks:

(a) establishing and maintaining a system of procedures and measures for the protection of NATO classified information. These measures must ensure that all security requirements specified for personnel security, physical security, security of information and CIS security (CISS) are adhered to and are in place throughout the lifetime of the classified project/contract;

(b) reporting to the responsible NSA/DSA any circumstances that may have an impact on the status of the FSC (e.g. changes in the ownership or key management personnel, changes in personnel who are involved in the classified project, changes to physical security, security of information and CISS, etc.), or PSCs (e.g. changes to or other circumstances which necessitate revalidation or which may adversely affect the individual's loyalty, reliability and trustworthiness, etc);

(c) reporting to the responsible NSA/DSA any suspected espionage, sabotage or subversive activities at the facility, including any indication of loss, compromise or suspected compromise of NATO classified information and any other security risks concerning NATO classified information;

(d) providing initial security briefings to new employees, and to all cleared persons before they are given access to NATO classified information. Providing periodic security training and security awareness programs for all personnel as required and conduct debriefings with individuals who are terminating employment on their continuing responsibilities concerning the safeguarding of NATO classified information they have accessed;

(e) conducting periodic security spot-checks or inventories as required of their facility;

(f) initiating a preliminary enquiry to ascertain the circumstances of any security violation, submit an initial investigation report of the security incident and final report including the corrective actions taken to the responsible NSA/DSA;

(g) cooperating in security inspections and investigations undertaken by the responsible NSA/DSA for assessing the protection of NATO classified information and assist in personnel security investigations of current or former employees; complying with any procedure that is, or may be, established by the NSA/DSA regarding the safeguarding and release of NATO classified information related to the contract/sub-contract.

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

PERSONNEL SECURITY CLEARANCES

General Provisions

49. All individuals (e.g. Contractors/Sub-contractor's personnel, including freelance consultants, interpreters, or any other type of freelance personnel or self-employed service providers) who require access to, or whose duties or functions may afford access to information classified NC or above, shall be appropriately cleared and briefed before such access is authorised. Individuals shall only have access to NATO classified information for which they have a need-to-know. Typical categories of personnel being subject to the security clearance procedure, in relation to the issuing of an FSC, are:

(a) owners of companies, members of supervisory boards and members of management's boards who may be subject to the personnel security clearance process in accordance with requirements in national laws and regulations;

(b) FSOs, CIS Security staff, registry staff, couriers and subject matter experts of a company may be subject to the personnel security clearance process as required for the fulfilment of the contract involving NATO classified information.

50. A PSC is not required for access to NR information; individuals shall have a need-to-know, shall be briefed about their responsibilities for the protection of NR information and shall acknowledge in writing that they fully understand their responsibilities.

51. Personnel security is addressed further at Enclosure "C" to the NATO Security Policy (C-M(2002)49) and in the supporting Directive on Personnel Security (AC/35-D/2000).

Contractual Conditions

52. Before letting a sub-contract involving information classified NC or above the Contractor shall contact its responsible NSA/DSA to ensure that Sub-contractor's facility and personnel requiring access to NATO information classified NC or above fulfil the requirements of this Directive.

Initiating Personnel Security Clearance Procedures

53. The FSO shall request each individual requiring access to NATO classified information NC and above to complete the respective national PSC questionnaire and forward the completed form to his/her responsible NSA/DSA.

Revalidation

54. The FSO is responsible to ensure the timely processing of a request for revalidation of the employee's PSC with the responsible NSA/DSA.

55. If a NATO PSC is not revalidated within the life of the clearance, a period of a further 12 months may be allowed for the revalidation to be completed, provided that the responsible NSA/DSA has commenced the action necessary to revalidate the clearance.

56. If, at the end of this additional 12-month period, the revalidation has still not been completed, the individual shall not have access to NATO classified information NC and above.

Procedures to be followed when a PSC is suspended or revoked

57. If the NSA/DSA of the nation with jurisdiction over the Contractor/Sub-contractor learns adverse information about an individual who is a national of another NATO nation, it shall immediately inform the NSA/DSA of the individual's country of citizenship in order to determine whether the individual shall continue to hold a PSC.

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

58. In the case where the NSA/DSA of the country of citizenship of an individual who is employed in another NATO nation decides to suspend or revoke the individual's security clearance, it shall immediately inform the NSA/DSA of the nation of origin of the facility that requested the PSC.

59. If an employee's security clearance has been suspended or revoked, the NSA/DSA of the nation with jurisdiction over the Contractor/Sub-contractor shall inform the facility where the individual is employed and vice versa. Other NSAs/DSAs to whom clearance verification has been provided shall be notified of the suspension or revocation.

60. On receiving the information that a PSC has been suspended or revoked, the FSO of the facility/Security Officer of the NATO civil and military body, which employs the individual, shall ensure that the individual is denied access to classified information NC or above and debriefed.

Procedures to be followed when a PSC is denied

61. The NSA/DSA of the nation with jurisdiction over the Contractor/Sub-contractor shall inform the facility where the individual is employed of the denial of a PSC. If other NSAs/DSAs have been involved in the PSC process they shall also be notified of the denial of the issuing of the clearance.

62. Should the NSA/DSA of a parent nation of an individual decide not to grant a PSC it will immediately inform the NSA/DSA of the nation which has jurisdiction over the facility that requested the PSC.

63. Equally, should the NSA/DSA of the nation with jurisdiction over the Contractor/Sub-contractor that requested the PSC decides not to grant it, it will immediately inform the NSA/DSA of the individual's country of citizenship.

64. On receiving the information that a PSC has been denied, the facility/NATO body which employs the individual shall ensure that they are not involved in classified work at the level of NC or above.

PSC of an Employee holding the Nationality/Citizenship of another Nation

65. If a PSC is required for a Contractor's/Sub-contractor's employee whose nationality/citizenship is that of another NATO nation, the NSA/DSA of the nation which has jurisdiction over the Contractor shall obtain a PSC or assurance from the employee's country of nationality/citizenship.

66. As an alternative, having the character of subsidiarity, the NSA/DSA of the nation which has jurisdiction over the Contractor may, where permitted by national laws and regulations, grant a PSC to an employee holding the nationality/citizenship of another NATO nation provided that:

(a) the employee has resided in the Contractor's country for at least 5 consecutive years;

(b) the NSA/DSA of the nation which has jurisdiction over the Contractor have checked their appropriate records to ensure that there is no adverse information;

(c) the material and information concerned with the contract is not at the COSMIC TOP SECRET (CTS) level; and

(d) an assurance is requested from the NSA/DSA of the employee's country of citizenship that there is no adverse information in respect to the individual that would prevent the granting of a NATO PSC by the parent nation.

67. If a facility wishes to employ a citizen of a non-NATO nation in a position that requires access to NATO classified information up to and including NATO SECRET (NS), it is the responsibility of the NSA/DSA of the nation which has jurisdiction over the hiring facility to

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

determine the suitability of the individual for accessing NATO classified information in accordance with the Directive on Personnel Security.

Multiple Nationalities

68. For individuals holding multiple nationalities, where appropriate, the host nation granting the PSC should obtain assurances on the individuals' suitability to be granted a PSC from the other nations, subject to the host nation's security policy.

Provisional PSC

69. The NSA/DSA may issue a provisional PSC in accordance with its national laws and regulations. The period of validity of such a PSC and its level shall be determined and notified by the issuing NSA/DSA.

70. In exceptional cases, where the attainment of major operational objectives would otherwise be seriously impaired, and it is not possible to obtain the clearance in time by prioritising a particular request, access may be permitted following the procedures set out in the Directive on Personnel Security(AC/35-D/2000). However, such access may be permitted only with the prior approval of the originator, be limited only for citizens of NATO nations, and in connection with contracts requiring access to classified information not higher than NS.

Verification

71. The verification that the individual has a valid PSC may either be in the form of request for visit (RFV) (Appendix B to Attachment 1 of Appendix 8), in the form of the NATO Personnel Security Clearance Certificate (PSCC) (Appendix 14) or in the form of an Attestation of NATO Personnel Security Clearance (APSC) (Appendix 15).

Security Awareness and Briefings of Individuals

72. All individuals employed in positions where they have access to NATO classified information, shall be briefed on security procedures and their security obligations. All individuals having access to NATO classified information shall acknowledge that they fully understand their responsibilities and the consequences which the law or administrative or executive order of their nation provides when classified information passes into unauthorised hands either by intent or through negligence. A record of the acknowledgement shall be maintained by the FSO.

73. All individuals who are authorised access to, or required to handle NATO classified information, shall initially be made aware, and periodically reminded of the dangers to security arising from indiscreet conversation with persons having no need-to-know, their relationship with the media, and the threat presented by the activities of intelligence services which target NATO and its member nations. Individuals shall be thoroughly briefed on these dangers and must report immediately to the appropriate security authorities any approach or manoeuvre which they consider suspicious or unusual.

74. All individuals who cease to be employed in duties requiring access to NATO classified information shall be made aware of, and acknowledge, their responsibilities for the continued safeguarding of NATO classified information.

75. Additional guidance can be obtained from Guidelines on Security Education and Awareness AC/35-D/1029.

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

PROGRAMME/PROJECT SECURITY

Introduction

76. Where established, the NPA/NPO is responsible for managing project security for major NATO programmes/projects or procurement activities. The security risks related to the operational, technological, political and commercial sensitivities of the project must be considered, and although these risks are managed on their behalf by the NPA/NPO, individual programme participants (the security stakeholders) must be made aware of the security risks.

77. At the start of a programme/project it is important to define the process required to ensure effective management of security throughout the activity, primarily by identifying and recording the relevant security sensitivities and identifying the appropriate protection in a PSI. All participants are responsible for the implementation of the PSI. It is also important to ensure that the security requirements for the programme/project are kept up to date during the entire life of the programme/project.

78. The allocation of a NATO classification indicates the required level of protective security to be provided to material or information associated with the NATO programme/project and the expected impact or damage as a consequence of loss or compromise associated with programme material and information. However, the classification alone does not prevent the release of information to other trusted nations, subject to an appropriate release process. Although material generated under the programme/project shall receive a NATO classification it should be recognised that the release authority remains with the programme/project participants, even for releases to other NATO nations.

Principles

79. Security measures are established to deter, detect and prevent the compromise of information and protect its confidentiality, integrity and availability. Within project security, it is important to recognise that such security measures are not only required for the technological aspects of the material, but also aspects such as how the material is to be used, where it will be used, details of the acquisition programme (e.g. prices, dates, quantities, etc.), and consideration of the need for associated specific information/data (e.g. mission plans, intelligence data libraries) or material (e.g. specific radios for interoperability). When considering the security risks to the programme/project, attention needs to be given to any operational, technological, commercial and political risks. Programme/project security must be the result of a team effort involving program management, and support personnel from disciplines such as technical, intelligence, security, and foreign disclosure.

80. Following determination of the threats and vulnerabilities associated with the programme/project, security is achieved by:

(a) classification of information. The classification markings applied are appropriate to the state of development of the programme/project. The preparation of a SCG requires collaboration amongst the programme/project technical staff and security professionals. The SCG is one of the most important tools in preparing the other programme/project related security documents;

(b) need-to-know. This principle is to be adhered to by all personnel involved in the programme/project; and

(c) the applicable security protection of a programme/project should be reviewed regularly or at each programme/project approvals milestone to ensure consistency and effectiveness.

Programme/Project Security Instruction

81. For all programmes/projects managed by NPA/NPO involving information classified NC or above, a PSI shall be developed utilising the template at Appendix 6. The purpose of the PSI is to supplement the security policies and requirements detailed in C-M(2002)49, and its supporting

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

Directives. It must establish specific security procedures associated with the NATO programme/project concerned and assign responsibilities for the implementation of security measures concerning classified information generated and exchanged under the development, production and follow-on support of the NATO programme/project. If considered appropriate by the NPA/NPO and programme participants a PSI may also be produced for programmes involving only classified information at the NR level.

82. The PSI also may include marking and handling instructions for unclassified information.

83. The PSI shall be developed by the NPA/NPO in conjunction with the NSAs/DSAs and technical staff of the programme participating NATO nations. It shall include an SCG which must identify the security sensitivities and security classification of the aspects related to the programme.

84. The PSI shall apply to all military and civilian establishments and as described below to Contractors/Sub-contractors and their personnel involved in the programme/project. Prime Contractors participating in the programme/project shall be provided with the complete PSI, which shall be made binding through appropriate contractual language. For Sub-contractors the complete PSI shall be provided if appropriate or alternatively only the relevant provisions of the PSI shall be provided and made binding through appropriate contractual language.

85. The following general principles shall be observed in connection with the security classification requirements of NATO contracts involving classified information (prime and sub):

(a) the assignment of security classifications to background information shall be the responsibility of the originator of the classified information; the classification of foreground information is a mutual responsibility of the participants in the programme/project;

(b) security classifications shall be applied only to those aspects of a programme/project that must be protected, and the level of such classifications must be strictly related to the degree of protection required;

(c) the classification of a compilation of information from more than one source shall be co-ordinated among the sources to determine the appropriate NATO security classification;

(d) information shall be declassified or downgraded as soon as appropriate; and

(e) the originator will approve any change of the classification level of background information. Changes to the classification of foreground information shall be co-ordinated among the participants.

86. The responsibility for applying a security classification to elements of a programme/project dealing with a product wherein all elements are clearly defined and their classification pre-determined, rests with the NPA/NPO of the contract, acting in collaboration with the NSAs/DSAs of the participating NATO nations.

87. The programme/project SCG should be developed in close co-operation with industry participating in the programme/project. A “Security Classification Board” may be established to assist in the preparation of classification guidance. Such Boards should be comprised of appropriate representatives of the NSAs/DSAs of the participating nations and the NPA/NPO, and advised by the participating prime Contractor(s).

88. The initial assessment that information should be classified, which was not previously identified for classification in a programme/project, may be made by the Contractor having system design responsibility. In such case, the Contractor shall recommend that the NPA/NPO take appropriate classification action. However, the decision to classify information ultimately is

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

the responsibility of the participating NSAs/DSAs or other designated classification authority. These decisions will be codified in the programme/project SCG.

89. In the absence of clearly defined classification guidance, any participant in the programme/project may forward a classification proposal to the responsible NPA/NPO regarding interim classification. The NPA/NPO shall review the proposed classification guidance, consult with the NSAs/DSAs, and, if agreed, update the programme/project SCG.

90. The PSI and SCG are to be approved by the responsible NSA/DSA and issued and maintained by the NPA/NPO. The PSI and SCG are to be reviewed regularly and amended as necessary in consultation with the programme/project NSAs/DSAs so that any sensitivities relating to the programme are identified and managed to ensure that the most appropriate degree of programme/equipment security is afforded throughout the programme, including during disposal.

RELEASE OF NATO CLASSIFIED INFORMATION BY PROGRAMME/PROJECT PARTICIPANTS AND CONTRACTORS/SUB-CONTRACTORS

Security Arrangements for the Release of NATO Classified Information to non-NATO Nations and International Organizations

91. Enclosure "E" to C-M(2002)49 NATO Security Policy sets out the principles for authorizing the release of NATO classified information to non-NATO nations and international organizations, and the release authority conditions. AC/35-D/2002 “Directive on Security of Information” addresses the specific procedures and arrangements.

Procedures to be followed for the Release of NATO Classified Programme/Project Information to non-Programme/Project Participants from NATO Nations

92. The release of NATO classified information to non-programme/project participants from NATO nations during the course of a programme/project shall be coordinated by the NPA/NPO and permitted only with the approval of the programme/project participants. These release procedures shall be fully detailed in the PSI.

HANDLING OF NATO CLASSIFIED INFORMATION IN COMMUNICATION AND INFORMATION SYSTEMS (CIS)

General

93. Only appropriately security accredited CIS (including stand-alone work stations) shall be used for the storing, processing or transmitting (called hereafter “handling") of NATO classified information.

94. CIS used within national industrial facilities to handle NATO classified information shall be accredited by the respective national Security Accreditation Authorities or their delegated SAAs ensuring that the NATO’s minimum security standards, as described in the policy on Security Within the NATO and its supporting Directives on CIS Security, are met for the handling of NATO classified information.

95. For security accreditation of CIS handling NATO’s classified information, whose components are under different jurisdictional domains (e.g. different SAAs), all SAAs having a legitimate interest in the security of the CIS shall take part in the security accreditation process.

96. The security accreditation of CIS handling NR information may be delegated to Contractors according to national laws and regulations. Where this delegation is exercised, the relevant NSAs/DSAs/SAAs shall retain the responsibility for the protection of NR information handled by the Contractor and the right to inspect the security measures taken by the Contractors. In addition, the Contractor shall provide the Contracting Authority and, where appropriate,

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

the security authority as established in Appendix III of this Directive, with a statement of compliance certifying that the CIS handling NR information has been accredited in compliance with the policy on Security within the NATO and its supporting Directives on CIS Security.

97. Interconnection of industrial facilities' classified CIS to NATO CIS shall be jointly accredited by the respective national and NATO SAAs. The appropriate security arrangements shall be in place to ensure that the SAAs and the different CIS Providers of the interconnected CIS are bound by the requirement to protect NATO information.

98. Where required, the capability for handling NATO classified information in CIS shall be reflected in the Facility Security Clearance Information Sheet (FSCIS – Appendix 2).

99. Enclosure "F" to C-M(2002)49, the "Primary Directive on CIS Security" (AC/35-D/2004), the "INFOSEC Management Directive for CIS" (AC/35-D/2005) and all relevant Technical and Implementation Directives on CIS Security (AC/322 documents) provide further policy and directions for the conformant implementation of CIS handling NATO classified information.

100. For further guidance the national Security Accreditation Authority (SAA) shall be consulted.

Security Accreditation Process

101. The security accreditation process shall determine the extent to which CIS Security measures are to be relied upon for the protection of NATO classified information and system assets, during the process of establishing the security requirements. The security accreditation process, shall determine that an adequate level of protection has been achieved, and is being maintained. The security accreditation process shall be carried out in accordance with the requirements of the INFOSEC Management Directive for CIS.

Security-related Documentation

102. Security-related documentation shall be established in accordance with the requirements of the INFOSEC Management Directive for CIS and the SAA requirements for a specific CIS. Security-related documentation shall be required throughout the system life cycle, from the planning stage until the disposal stage. The security-related documentation (for example, System-specific Security Requirement Statements (SSRS) and Security Operating Procedures (SecOPs)) shall be developed in an iterative process throughout the system life cycle.

Interconnection of CIS

103. The policy on Security within the North Atlantic Treaty Organisation and its supporting directives on CIS Security require security measures to control the interconnection of CIS handling NATO classified information. The supporting INFOSEC Management Directive for CIS sets out the security accreditation requirements and the supporting CIS Security Technical and Implementation Directives (AC/322 documents) set out the measures to be implemented.

INTERNATIONAL VISIT CONTROL PROCEDURES (IVCPs)

Requirements and Procedures for Visits

104. Procedures for visit requests are formalised in the standard Request for Visit (RFV) procedure as established at Appendix 8. Lead times for the handling of the requests are laid down in Appendix 9.

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

INTERNATIONAL TRANSMISSION AND TRANSPORTATION OF NATO CLASSIFIED MATERIAL

General

105. The international transmission of NATO classified information up to and including NS shall be as set out in the Directive on Security of Information (AC/35-D/2002). Electronic transmission of NATO classified information shall be in accordance with the requirements of Enclosure "F" of NATO Security Policy and its supporting Directives. Information classified at the COSMIC TOP SECRET (CTS) level shall be transmitted by diplomatic pouch or military courier. International hand carriage of CTS is prohibited.

106. Information classified up to and including NS that cannot be transmitted by one of the foregoing methods and relates to contracts, may be transmitted by other means in accordance with the relevant provisions below.

International Hand Carriage of NATO Classified Material at NC or NS level

General

107. When transmission through the channels specified in the Directive on the Security of Information will result in an unacceptable delay that will adversely affect performance of the programme, project, or contract, and when it has been verified that the information is not available at the intended destination, the procedure of personal hand carriage may be permitted, provided the following provisions are complied with:

(a) the courier shall hold a PSC at appropriate level. Commercial courier companies shall not be used except as permitted at paragraph 115 below;

(b) in exceptional circumstances, the NSA/DSA of the dispatching facility may, with the previous agreement of the NSA/DSA of the receiving facility, consider issuing a Courier Certificate to an employee with the appropriate PSC who is assigned to the receiving facility, and to whose NATO nation the release of the classified material relating to the programme/contract has been authorised.

Security Arrangements

108. The hand carriage of NATO classified material will comply with the provisions of Enclosure "E" of NATO Security Policy and the supporting Directive on the Security of Information. In addition, the material must have been authorised by the originating government for release in conjunction with the project, programme or contract.

109. The courier shall be briefed by the FSO before departure on all the security measures to be implemented and shall sign the Security Acknowledgment at Appendix 10.

110. The courier shall be responsible for the safe custody of the NATO classified material until such time that it has been handed over to the consignee's FSO. In the event of a breach of security or loss of classified information, the consignor's NSA/DSA may request the authorities in the country (i.e. a NATO nation or non-NATO nation with a Security Agreement/Arrangement with NATO or a NATO nation) in which the breach or loss occurred to carry out an investigation, report their findings and take legal or other action as appropriate.

Procedure

111. When hand carriage of NATO classified material is permitted, the following minimum procedure shall apply:

(a) the courier shall carry a Courier Certificate based on Appendix 11, authorising him to carry the package as identified. The Courier Certificate shall be stamped and signed by the consignor's NSA/DSA and by the consignor's FSO;

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

(b) a copy of the "Instructions for the Courier" (Attachment 1 to Appendix 11) shall be attached to the certificate; and

(c) the Courier Certificate shall be returned to the issuing NSA/DSA through the consignor's FSO immediately after completion of the journey(s) or be kept available at the company for monitoring purposes if permitted by the issuing NSA/DSA national laws and regulations. Any circumstances that occurred during the trip which raise security concerns shall be reported by the courier on the certificate.

112. If the courier is making multiple hand carriages of NATO information classified NC and above, then the "Multi-Travels Courier Certificate" (Attachment 2 to Appendix 11) shall include:

(a) the courier's name and the destination countries. It will be stamped and signed by the NSA/DSA and the consignor's FSO. The certificate cannot be valid for more than one year;

(b) for each journey, a "Description of Consignment" must be signed by the consignor's FSO. This description will be returned to the issuing NSA/DSA, through the consignor's FSO in order to assure accountability or be kept available at the company for monitoring purposes if permitted by the issuing NSA/DSA national laws and regulations ; and

(c) at the end of each journey, the courier will sign the Note at the bottom of the "Multi-Travels Courier Certificate" certifying that no situation occurred that might have compromised the security of the consignment during the journey. The declaration will be witnessed by the consignor's FSO.

113. The consignor's FSO is responsible for instructing the courier in all of his/her duties and of the provisions of the "Instructions for the Courier" (Attachment 1 to Appendix 11) and a Security Acknowledgement (Appendix 10) has to be signed.

114. If customs authorities (of the NATO nation or of a non-NATO nation with a Security Agreement with NATO) request to examine the consignment and inspection is unavoidable, the procedures detailed in the customs section below shall be followed. Customs authorities will be permitted to observe sufficient parts of the consignment to determine that it does not contain material other than that which is declared.

Carriage of Material at the level NC by Commercial Courier Companies

115. The following criteria shall be applied when consignments of NATO classified material at the level NC is carried by non-security cleared commercial courier companies;

(a) the use of transmission channels as described above is not feasible due to a case of urgency or cannot meet the needs of industry;

(b) the commercial courier company provides courier services, and if required by national laws and regulations has concluded a framework arrangement with the NSA/DSA of the consignor which describes the specific obligations of the commercial courier company, include reporting obligations in the case of suspected or actual breaches of security, or losses of NATO classified material;

(c) the commercial courier company is located and registered in a NATO nation and has established a protective security programme for handling valuable items with a signature service, including a record of continuous accountability on custody through either a signature and tally record, or an electronic tracking/tracing system;

(d) the commercial courier company must obtain and provide to the consignor proof of delivery on the signature and tally record, or the courier must obtain receipts against package numbers;

(e) the commercial courier company must guarantee the consignment will be delivered to the consignee prior to a specific time and date within a 48-hour-period;

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

(f) the commercial courier company may charge a commissioner or Sub-contractor, which is located and registered in a NATO nation and also meets the above requirements. However, the responsibility for fulfilling the above requirements must remain with the commercial courier company.

Transportation of NATO Classified Material NC or NS as Freight

116. The consignor and the consignee of a consignment of NATO classified material to be transported as freight internationally shall jointly organise the transport arrangements. The consignor shall submit a written transportation plan to its NSA/DSA who, after consultation with the NSA/DSA of the consignee, will advise the consignor whether the transportation plan is acceptable and/or of any changes that are required.

117. The NSA/DSA of the consignor shall notify, as appropriate, the NSA/DSA of any transited nation of the appropriate details of the transportation, including any cancellation thereof, with sufficient advance notice to enable them to provide the necessary security assistance.

118. When, in the opinion of the NSA/DSA concerned, a consignment at the level NC or NS is of such size and weight, or other circumstances render the standards defined in the Directive of Security of Information or hand carriage impractical or unavailable, commercial carriers may be used. The following procedures shall be applied:

(a) the commercial carrier shall hold an FSC if required by national laws and regulations or if it is to store NC or above at its premises;

(b) the commercial carrier shall deploy personnel that have been granted a PSC at a minimum level to the material being transported;

(c) prior to any international transmission by commercial carrier, the NSAs/DSAs of the consignor and of the consignee must agree on an International Transportation Plan as described in Appendix 12; and

(d) when a International Transportation Plan is developed that will involve more than one international shipment of classified material, a Notice of Classified Consignment (Attachment 1 to Appendix 12) shall be used to identify each shipment and provide details to the recipient, transportation personnel and any other personnel who will be involved in ensuring the security of the shipment.

Transportation of NATO Classified Material NC or NS as Freight by Road

119. The following minimum criteria shall be applied when consignments of NATO classified material NC or NS are transported by road:

(a) when storage of classified consignments is required at the carrier's facility, the carrier shall hold an FSC at the appropriate level issued by the respective NSA/DSA;

(b) classified material shall be secured in vehicles or containers by a lock or padlock of a type currently approved by the NSA/DSA concerned. Closed vans and cars that may be sealed should be used since they offer maximum security. If this is not physically possible, the consignment should be encased to protect the classified aspects and prevent unauthorised persons from gaining access;

(c) the transport shall be accompanied by at least two individuals who could be the driver, co-driver or additionally deployed security escorts or guards, and who both shall hold a PSC at the level commensurate with the classification level of the material. At least one individual shall carry a "Courier Certificate" based on Appendix 11 and assume responsibilities of a "Courier" as described above.

(d) in cases where stops must be made, arrangements shall be made in advance to use storage provided by government establishments or facilities having an appropriate FSC and the necessary cleared personnel and capabilities to ensure security of consignment. In

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

the event such arrangements cannot be made or an emergency situation arises due to accident or breakdown of the vehicle, at least one of the security cleared individuals accompanying the material shall be responsible for keeping the consignment under constant control, and

(e) communication checks along the road shall be pre-arranged to ensure security of the consignment.

Transportation of NATO Classified Material NC or NS as Freight by Rail

120. The following minimum criteria shall apply when consignments of NC and NS material are transported by rail :

(a) passenger accommodation shall be made available for appropriately cleared security guards or escorts who shall carry a Courier Certificate based on Appendix 11 and assume responsibilities of a “Courier” as described above.; and

(b) during stops, the security guards/escorts shall remain with the consignment.

121. Depending on the volume of the consignment, priority shall be given to rail cars or containers that can be closed and sealed, giving maximum security.

Transportation of NATO Classified Material NC or NS as Freight by Sea

122. The following minimum standards shall be applied when consignments of NATO material classified NC or NS are sent by sea:

(a) where possible consignments should be carried in ships sailing under the flag of a NATO nation. Ships sailing under the flag of a non-NATO nation, which represents a special security risk (as defined in the Directive on the Security of Information, "International Transmission") shall not be used. Where practicable, a guard or escort holding an appropriate PSC shall accompany the consignment;

(b) material shall be secured in locked containers approved by the NSA/DSA of the consignor. However, when this is not possible, blocked-off stowage may be approved by the NSA/DSA of the consignor. Use of security tapes or seals on the openings shall be considered. Blocked-off stowage is stowage in the hold of a ship where the material is covered and surrounded by other cargo consigned to the same destination in such a way that access to the material is physically impracticable. Where it is not possible or impracticable to carry a consignment in the hold, it may be carried as deck cargo, provided it is secured in a locked container and packaged so it is not evident that it contains classified material;

(c) stops at or entering the territorial waters of countries presenting special security risks shall normally be avoided but if unavoidable the security risk shall be assessed by the NSAs/DSAs concerned in the light of the political environment, when they receive the transportation plan drawn up by the consignor and the consignee. Unless the ship is in an emergency situation, it shall not enter the territorial waters of any of these countries;

(d) stops at any other country shall not be permitted unless the prior approval of the consignor's NSA/DSA has been obtained;

(e) in all cases, loading and unloading shall be under security control; and

(f) deliveries to the port of embarkation and collection from the port of disembarkation must be so timed to prevent, as far as possible, a consignment being held in port warehouses unless the warehouse has been granted an FSC by the *consignor’s* or consignees NSA/DSA, *as applicable*. Where this is not possible, sufficient security guards must be provided to keep the consignment under adequate and permanent supervision until collection is achieved.

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

Transportation of NATO Classified Material NC or NS as Freight by Aircraft

123. Preference shall be given to the use of military aircraft of a NATO nation to transport NC or NS material. If utilisation of a military aircraft of a NATO nation is not feasible, an NSA/DSA approved commercial air carrier may be used, provided it is registered in or chartered by a NATO nation. Exceptionally, airlines from non-NATO nations may also be used provided the security of the consignment can be assured by the appropriate measures taken by NSA/DSA. Scandinavian Airlines System aircraft also may be used.

124. The following minimum standards shall be observed:

(a) every effort shall be made to deliver the consignment straight to the aircraft rather than permitting it to be stored in warehouses, etc., at airports and airfields. When a consignment cannot be loaded straight away, it shall either be stored in a NSA/DSA cleared storage facility, or kept under guard. A sufficient number of security guards must be provided to keep the consignment under adequate and continuous supervision;

(b) every effort shall be made for the aircraft to be met on landing and the consignment to be removed at its final destination. When this is not feasible, the consignment shall be kept at the airport and a sufficient number of security guards must be provided to keep the consignment under adequate and continuous supervision;

(c) direct flights shall be used wherever possible;

(d) intermediate routine stops of short duration may be permitted, provided the consignment shall remain in the aircraft. However, if the cargo compartment is to be opened, every effort shall be made to ensure that the courier or other personnel holding an appropriate PSC are available to ensure the protection of the classified material;

(e) in the event the aircraft is delayed at an intermediate stop or has to make an emergency landing, the security guard, or the person fulfilling the duties of the security guard, shall take all measures considered necessary for the protection of the consignment and if necessary seeking the assistance of his Diplomatic mission in the country concerned;

(f) transportation over countries presenting special security risks, as defined in the “Directive on the Security of Information, International Transmission” should be avoided; and

(g) stops in a non-NATO nation having a valid security agreement with NATO, may be allowed by the NSA/DSA of the consignor. Stops at airfields in non-NATO nations not having a Security Agreement with NATO, except in an emergency, shall not be permitted;

125. When the conditions outlined below are met and if permitted by national laws and regulations, the requirements for a commercial air carrier to hold an FSC do not apply:

(a) the commercial air carrier agrees to be responsible for the consignment while it is in the hold of the air plane, and will be cognisant of, and agrees to comply with the security requirements, particularly the emergency procedures specified by the NSA/DSA;

(b) consignments shall be transmitted point-to-point, the service provided by the commercial air carrier cannot be sub-contracted, and the intermediate stops are not permitted;

(c) a written transportation plan approved by the participating NSA/DSA shall be in place before the consignment is released to the cargo handling service or to the commercial air carrier;

(d) sufficient physical protection shall be provided to the consignment as agreed by the NSA/DSA.

126. Companies that provide cargo handling services (such as freight forwarders) for NC and NS consignments shall have an FSC and approved protection capability if the consignment is to be stored at the facility.

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

Security Principles applicable to all Forms of Transportation

Countries presenting special Security Risks

127. Countries presenting special security risks shall be assessed by the NSAs/DSAs concerned in the light of the political environment, when they receive the transportation arrangements. Arrangements for consignments of classified material shall be stipulated for each programme/project. However, such arrangements shall ensure that there is no likelihood of unauthorised access to classified material.

Customs

128. As a general rule, customs authorities shall be advised by the appropriate national authorities of impending consignments and should be urged to honour the official authority of the shipping documents and of the authorisation documents carried by the security guard or courier. Consignments should not be opened unless there is a pertinent reason for so doing. If a consignment is opened, this should be done out of sight of persons who do not have a need-to-know and in the presence of the courier. When access is no longer necessary it shall be repacked securely, and the customs authorities shall be requested to reseal it and endorse the shipping documents, confirming that it was opened by such authorities. To facilitate customs clearance, advantage should be taken of the Transport International Routier (TIR) for road shipments, Transport International Ferroviaire (TIF) for rail shipments, or other similar shipping arrangements.

129. Nothing in the previous paragraph or elsewhere in this section should be construed to abrogate any nation's rights of examination of any consignment.

Acknowledgement

130. The consignee shall acknowledge receipt of the consignment to the sender.

Packaging

131. Packaging of consignments shall be in compliance with the Directive on the Security of Information. The FSO of the consigning facility is responsible for appropriate packaging. In no circumstances shall the packaging reveal the fact that the material is classified.

Security Guards and Escorts

132. Individuals fulfilling the duties of security guards may be civilian or military personnel and may be armed or unarmed depending on national practices and arrangements made between the NSAs/DSAs of the nations affected by the transportation. Similarly, the nationality of such guards in any particular nation shall be subject to mutual agreement of the NSAs/DSAs and in accordance with NATO security policy addressed further at Enclosure "C" to the NATO Security Policy (C-M(2002)49) and in the supporting Directive on Personnel Security (AC/35-D/2000).

133. In addition to the security guards, security escorts may be provided if the NSAs/DSAs concerned consider this desirable or as required under their national laws and regulations. These escorts need not be security cleared unless otherwise required by national laws and regulations.

134. The security guard/escort shall be composed of an adequate number of personnel as to ensure regular tours of duty and rest. The number of guards/escorts on a consignment shall depend on the classification level of the material, the method of transportation to be used, the estimated time in transit, and the quantity of material will also be considered. A reserve of personnel shall be provided to cater for emergencies.

135. It is the responsibility of the consignor (and, where applicable, the consignee) to instruct security guards in their duties. In particular, the route and the security plan must be explained, and

details given, where appropriate, of the authorities that security guards shall contact and other measures to be taken in the event of an emergency. Security guards shall also be given a copy of "Notes for the Courier", and be required to sign the Security Acknowledgement.

136. The consignor's NSA/DSA may issue to the consignor sufficient authorisation documents so that they may be completed and issued to the security guards (Appendix 13).

137. Both the authorisation documents and "Instructions for the Courier" (Attachment 1 to Appendix 11) shall be written in English and French; a copy in other languages may, in addition, be issued if this is deemed necessary or recommended by the NSA/DSA concerned.

Transportation of Explosives, Propellants or Other Dangerous Substances

138. If the classified material contains explosives, propellants or other dangerous substances, the transmission across international borders is subject not only to the security and customs requirements, but also to mandatory international and national safety regulations. The consignor is responsible for compliance with these regulations.

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

GLOSSARY AND ACRONYMS

GLOSSARY

Attestation of Personnel Security Clearance (APSC)	An approved format to confirm the security clearance level of an individual in the context of a contract involving NATO classified information.
Background Information	Knowledge that has been generated by one of the participants outside of the collaborative programme but which has been provided to the programme. Only the originating participant needs to be consulted for authorising the release of that information to parties outside the programme.
Breach of Security	An act or omission, deliberate or accidental, contrary to NATO Security Policy and supporting directives, that results in the actual or possible compromise of NATO classified information or supporting services and resources (including, for example, classified information lost while being transported; classified information left in an unsecured area, where persons without an appropriate PSC have unescorted access; an accountable document cannot be found; classified information has been subjected to unauthorised modification; destroyed in an unauthorised manner or, for CIS, there is a denial of service).
Classified Information	Any information (namely, knowledge that can be communicated in any form) or material determined to require protection against unauthorised disclosure and which has been so designated by a security classification.
Commercial Courier Company	Commercial company that offers a service where a consignment is moved under a trace and tracking scheme.
Compromise	Compromise denotes a situation when - due to a breach of security or adverse activity (such as espionage, acts of terrorism, sabotage or theft) - NATO classified information has lost its confidentiality, integrity or availability, or supporting services and resources have lost their integrity or availability. This includes loss, disclosure to unauthorised individuals (e.g. through espionage or to the media) unauthorised modification, destruction in an unauthorised manner, or denial of service.
Confidentiality	The property that information is not made available or disclosed to unauthorised individuals or entities.
Consignee	The Contractor, facility or other organisation receiving material from the consignor.
Consignor	The Contractor, facility or other organisation responsible for organising and dispatching material.
Contract	A legally enforceable agreement to provide goods or services.

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

Contract involving NATO Classified Information	Any contract issued by a NATO civil or military body or a NATO nation in support of a NATO funded or administered programme/project that will require access to or generation of NATO classified information.
Contractor	An industrial, commercial or other entity that seeks or agrees to provide goods or services.
Courier	A person officially assigned to hand-carry material.
Designated Security Authority (DSA)	An authority responsible to the National Security Authority (NSA) of a NATO nation which is responsible for communicating to industry the national policy in all matters of NATO industrial security policy and for providing direction and assistance in its implementation. In some NATO nations, the function of a DSA may be carried out by the NSA or a DSA may delegate functions to other competent security authorities.
Document	Any recorded information regardless of its physical form or characteristics, including, without limitation, written or printed matter, data processing cards and tapes, maps, charts, photographs, paintings, drawings, engravings, sketches, working notes and papers, carbon copies or ink ribbons, or reproductions by any means or process, and sound, voice, magnetic or electronic or optical or video recordings in any form, and portable IT equipment with resident computer storage media, and removable computer storage media.
Escorts	Armed or unarmed national police, military personnel, government personnel or other government designated personnel that facilitate the secure movement of information and materiel.
Facility	An installation, plant, factory, laboratory, office, university or other educational Institution, or commercial undertaking, including any associated warehouses, storage areas, utilities and components which, when related by function and location, form an operating entity.
Facility Security Clearance (FSC)	An FSC is an administrative determination by which an NSA/DSA formally recognizes the capacity and reliability of Contractor's facilities to manage generate and have access to NATO classified information up to a certain level.
Foreground Information	Foreground information is knowledge that has been generated in pursuance of a collaborative/cooperative programme. It is owned by all participants. To determine the releasability of foreground information approval of all owners is required.
Freight	Material carried by a vessel or vehicle, especially by a commercial carrier; cargo. Also – the commercial transportation of material.
Guards	Civilian (Government or participating Contractor employees) or military personnel who may be armed or unarmed. They may be assigned for security guard duties only or may combine security guard duties with other duties.

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

Industry	Organized economic activity concerned with manufacture, extraction and processing of raw materials, construction or output of a specific service.
CIS Security	The application of security measures for the protection of communication, information and other electronic systems, and the information that is stored, processed or transmitted in these systems with respect to confidentiality, integrity, availability, authentication and non-repudiation.
Infraction	A security infraction is an act or omission, deliberate or accidental; contrary to NATO Security Policy and supporting directives that does not result in the actual or possible compromise of NATO classified information. (E.g. classified information left unsecured inside a secure facility where all persons are appropriately cleared, failure to double wrap classified information, etc.).
Integrity	The property that information (including data, such as cipher text) has not been altered or destroyed in an unauthorised manner.
International Visits	Visits made by individuals subject to one NSA/DSA or belonging to a NATO body, to facilities or bodies subject to another NSA/DSA or to NATO, which will require, or may give rise to access to NATO classified information or where, regardless of the level of classification involved, national legislation governing the establishment or body to be visited in support of NATO approved related activities requires that such visits shall be approved by the relevant NSA/DSA. All NATO civil and military bodies fall within the security jurisdiction of NATO.
Major Programme/Project	A programme or project of major significance, normally involving more than two nations and security measures that extend beyond the normal basic requirements described in NATO Security Policy.
Material	Material includes documents and also any items of machinery, equipment/components, weapons or tools, either manufactured or in the process of manufacture.
Nationals	Nationals includes “nationals of a Kingdom”, “citizens of a State”, and ”Permanent Residents in Canada”. “Permanent Residents in Canada” are individuals who have gone through a national screening process including residency checks, criminal records and security checks, and who are going to obtain lawful permission to establish permanent residence in the nation.
National Security Authority (NSA)	An authority of **a** NATO nation which is responsible for the maintenance of security of NATO classified information in national agencies and elements, military or civil, at home or abroad.

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

NATO	"NATO" denotes the North Atlantic Treaty Organisation and the bodies governed either by the Agreement on the status of the North Atlantic Treaty Organisation, National Representatives and International Staff, signed in Ottawa on 20th September, 1951 or by the Protocol on the status of International Military Headquarters set up pursuant to the North Atlantic Treaty, signed in Paris on 28th August, 1952.
NATO Classified Information	Means information or material determined by or on behalf of NATO to require protection against unauthorised disclosure which has been so designated by a security classification NR or above.
NATO Programme/Project	A Council approved programme/project that is administered by a NATO agency/office under NATO regulations.
NATO Programme/Project Agency/Office (NPA/NPO)	The executive body for the administration of a NATO programme/project.
Need-to-Know	The principle according to which a positive determination is made that a prospective recipient has a requirement for access to, knowledge of, or possession of information in order to perform official tasks or services .
Negotiations	The term encompasses all aspects of awarding a contract or sub-contract from the initial "notification of intention to call for bids" to the final decision to let a contract or sub-contract.
Originator	The nation or international organisation under whose authority information has been produced or introduced into NATO.
Personnel Security Clearance (PSC)	A determination that an individual is eligible to have access to classified information.
Personnel Security Clearance Certificate (PSCC)	An approved format used by NSAs/DSAs to confirm the level and validity of a PSC.
Prime Contract	The initial contract led by a NATO Project Management/Agency/ Office for a Programme/project.
Prime Contractor	An industrial, commercial or other entity of a NATO nation which has contracted with a NATO Project Management Agency/Office to perform a service, or manufacture a product, in the framework of a NATO project, and which, in turn, may subcontract with potential Sub-contractors as approved.
Programme/Project Security Classification Guide	Part of the program (project) security instructions (PSI) which identifies the elements of the program that are classified, specifying the security classification levels. The security classification guide may be expanded throughout the program life cycle, and the elements of information may be re-classified or downgraded.

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

Programme/Project Security Instruction (PSI)	A compilation of security regulations/procedures, based upon NATO Security Policy and supporting directives, which are applied to a specific project/programme in order to standardise security procedures. The PSI may constitute an Annex to the prime contract, and may be revised throughout the programme lifecycle. For sub-contracts let within the programme, the PSI constitutes the basis for the SAL.
Risk	The likelihood of a vulnerability being successfully exploited by a threat, leading to a compromise of confidentiality, integrity and/or availability and damage being sustained.
Risk management	A systematic approach to determining which security counter-measures are required to protect information and supporting services and resources, based upon an assessment of the threats and vulnerabilities. Risk management involves planning, organising, directing and controlling resources to ensure that the risk remains within acceptable bounds.
Security Aspects Letter (SAL)	A document, issued by the appropriate authority, as part of any NATO classified contract or sub-contract, other than Major Programmes/Projects, identifying the security requirements or those elements thereof requiring security protection.
Security Classification Check List (SCCL)	Part of a security aspect letter (SAL) which describes the elements of a contract that are classified specifying the security classification levels. In case of contracts let within a programme/project, such elements of information derive from the programme (project) security instructions issued for that programme.
Sub-contract	A contract entered into by a prime Contractor with another Contractor (i.e., the Sub-contractor) for a provision of goods or services.
Sub-contractor	A Contractor to whom a prime Contractor lets a sub-contract.
Threat	The potential for compromise, loss or theft of NATO classified information or supporting services and resources. A threat may be defined by its source, motivation or result, it may be deliberate or accidental, violent or surreptitious, external or internal.
Transportation by freight	Transportation of a consignment of such size and weight which makes the application of the respective standards defined in the Directive of Security of Information or hand carriage impractical.
Vulnerability	A weakness, an attribute, or lack of control that would allow or facilitate a threat actuation against NATO classified information or supporting services and resources.

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

GENERAL RESPONSIBILITIES

NATO NATIONS

1. Each NATO nation shall:

(a) designate one or more authorities (DSA) responsible to the NSA, where applicable. The DSA is responsible for communicating national and NATO security policy to industry and for providing direction and assistance in its implementation; in some countries there may be more than one authority designated as a DSA or the function of a DSA may be carried out by the NSA;

(b) certain functions of the NSA/DSA may be carried out by other competent security authorities in accordance with national laws and regulations;

(c) ensure that it has the means to make its industrial security requirements binding upon industry and that it has the right to inspect and approve the measures taken in industry for the protection of NATO classified information;

(d) determine, as appropriate, the aspects of a NATO contract or sub-contract requiring security protection and the security classification to be accorded to each aspect. Prior to the release of NATO classified information to a Contractor, prospective Contractor, or Sub-contractor, the NATO nation shall :

(i) ensure that the Contractor(s), prospective Contractor(s), or Sub-contractor(s) and their facility(ies) have the capability to protect NATO classified information adequately, in accordance with national laws and regulations;

(ii) grant a Facility Security Clearance (FSC) to the facility(ies), if appropriate;

(iii) grant a NATO Personnel Security Clearance (PSC) to all personnel whose duties require access to information classified NC or above; and

(iv) ensure that access to the NATO classified information is limited to those persons who have a need-to-know for purposes of performance on the NATO project/programme;

(e) make arrangements whereby persons considered by the NSA/DSA to be a security risk can be excluded or removed from positions in which they might endanger the security of NATO classified information;

(f) implement, as and when necessary, the NATO procedures for the mutual safeguarding of the secrecy of inventions;

(g) provide, upon request to an NSA/DSA of a NATO nation, or to a NATO civil or military body, an FSCC to enable a facility falling within its security cognisance to negotiate or fulfil a contract/sub-contract involving information classified NC or above;

(h) provide, upon request, to a NSA/DSA of another NATO nation, or a NATO civil or military body, a PSC for the persons for whom it has security responsibilities to enable them to fulfil on a NATO classified contract;

(i) take action with regard to the specific arrangements to be carried out in matters of transportation and international visits in accordance with the requirements of NATO security policy and this directive:

(i) investigate all cases in which it is known, or where there are grounds for suspecting, that NATO classified information has been lost or compromised. Each member nation shall comply with the investigative requirements set out in NATO security policy and its supporting directives and promptly inform

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

the NPA/NPO and the other member nations concerned and if applicable the NOS of the details of any such occurrences; and

(ii) ensure that for any facility in which NATO classified information is to be used, a person or persons shall be appointed, where appropriate, in accordance with national laws and regulations, to effectively exercise the responsibilities for safeguarding the NATO classified information. These officials shall be responsible for limiting access to the NATO classified information involved in a contract to those persons who have been cleared and authorised for access and have a need-to-know.

SECURITY COMMITTEE (SC)

2. The SC shall:

(a) formulate NATO industrial security policy and supporting directive(s) and make appropriate recommendations to the North Atlantic Council (c) for the security protection of NATO classified information entrusted to industry; and

(b) consider matters of industrial security referred to it by the NAC, a member nation, the Secretary General, the NATO Military Committee (NAMILCOM), Strategic Commands and heads of NATO civil and military bodies.

NATO OFFICE of SECURITY (NOS)

3. The NOS shall:

(a) assist and give guidance in industrial security matters to NPA/NPOs and such other NATO industrial projects as may be designated by the NAC and supervise the implementation of NATO security policies and directives in those organisations and projects;

(b) in agreement with the NSAs/DSAs of member nations concerned, assist and give guidance to other NSAs/DSAs in the implementation of NATO security policies and directives in connection with the activities of NPA/NPOs;

(c) in agreement with the NSAs/DSAs of member nations concerned, assist and give guidance on NATO security policies and directives to facilities participating in the activities of NPA/NPOs;

(d) make periodic inspections of the security arrangements for the protection of NATO classified information in NPA/NPOs;

(e) with the agreement of the appropriate NSA/DSA, make periodic examinations of the security arrangements for the protection of NATO classified information in the member nations; and

(f) give guidance and advice, when requested by NSAs/DSAs, on matters of industrial security arising in all NATO-related projects.

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

NATO PROGRAMME/PROJECT AGENCIES / OFFICES

4. Each of the NPA/NPOs and other NATO agencies with project management responsibilities as may be designated by the NAC will be bound by the general security regulations laid down in NATO security policy and supporting directives, and any other security regulations approved by the NAC as may apply. Each of the NATO Management Agencies/ Offices shall:

(a) draw up the implementing security regulations for the agency/office in compliance with the provisions of NATO security policy and supporting directives and supervise their enforcement;

(b) in conjunction with the NSAs/DSAs concerned and the NOS, co-ordinate the implementation of NATO security policies and directives, both by potential Contractors and by Contractors, and deal with any security problems arising in any NATO project in which the agency/office is engaged;

(c) obtain the appropriate Facility Security Clearance(s) as required in conjunction with contracts involving classified NATO information;

(d) take action as required, and in accordance with the provisions of NATO security policy and this directive, in respect of the special arrangements for International Visits;

(e) be responsible for preparing Project Security Instructions (PSI) for the programmes they manage for approval by participating NSAs/DSAs; and

(f) may be responsible for raising a Transportation Plan as identified in the PSI.

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

FACILITY SECURITY CLEARANCE INFORMATION SHEET (FSCIS)

1. INTRODUCTION

1.1 Attached is a sample format of a Facility Security Clearance Information Sheet (FSCIS) for the quick exchange of information between National Security Authority or Designated Security Authority or other competent national security authorities (hereinafter referred to as “NSA/DSA”) and NATO contracting authorities (NATO Programme/Project Offices/NATO Programme/Project Agencies) with regards to the Facility Security Clearance (FSC) of a facility involved in classified tenders, contracts or sub-contracts.

1.2 The FSCIS is not for use by Contractors.

1.3 The FSCIS is divided into a request and reply section and can be used for the purposes identified above or for any other purposes for which the FSC status of a particular facility is required. The reason for the enquiry must be identified by the requesting NSA/DSA/NPO/NPA in form field 7 of the request section.

1.4 The details contained in the FSCIS shall normally not be classified and therefore the preferable way for the exchange of the FSCIS will be electronically between the respective NSAs/DSAs/NPOs/NPAs.

1.5 NSAs/DSAs should make every effort to respond to a FSCIS request within 5 working days. In urgent cases, NSA/DSA will send the response within 3 working days.

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

Procedures and Instructions for the Use of the Facility Security Clearance Information Sheet (FSCIS).

These detailed instructions are for the NSA/DSA that completes the FSCIS.

The request should preferably be typed in capital letters

HEADER	The requesting NSA/DSA/NPA/NPO inserts full country or international organization name.
1. REQUEST TYPE	The requesting NSA/DSA/NPA/NPO selects the appropriate checkbox for the type of FSCIS request. Include the level of security clearance requested. The following abbreviations should be used: TS = National TOP SECRET CTS = COSMIC TOP SECRET S = National SECRET NS = NATO SECRET C = National CONFIDENTIAL NC = NATO CONFIDENTIAL CIS = Communication and information systems for processing classified information A FSC is not required by Enclosure G to C-M(2002)49 for access to, or generation of classified information at level of NATO RESTRICTED (NR). However some NATO Nations, as identified in Appendix 3, and as mandated by their national laws and regulations, do require a FSC for Contractors/Sub-contractors under their jurisdiction, for access to classified information at the level of NR.
2. SUBJECT DETAILS	The Form Fields 1 through 6 are self-evident. Form Field number 5 is optional.
3. REASON FOR REQUEST	Give the specific reason for the request, provide project indicators, number of contract, letter of intent or invitation. Please specify the need for storage capability, CIS classification level, etc. Any deadline/expiry/award dates, which may have a bearing on the completion of a FSC, should be included.

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

4. REQUESTING NSA/DSA/NPA/NPO	State the name of the actual requestor (on behalf of the NSA/DSA) and the date of the request by using the "day/month/year" (dd/mm/yyyy) format.
5. REPLY SECTION	Form Field 1-6: Select appropriate fields. Form Field 2: In case an FSC is in progress it is essential to give the requestor an indication of the required processing-time (if known). Form Field 6: (a) The validation date inputted will be either when the FSC for the Contractor's facility expires, and/or when this FSCIS expires (if different). Any date inputted must be in the "day/month/year" format. It should be noted that some NATO Nations do not have an expiry date for FSCs or the FSCIS, so will be marked "n/a". (b) Should an FSC and/or FSCIS expire prior to the award of a NATO Classified Contract the requesting NSA/DSA/NPA/NPO is responsible for submitting a new FSCIS request to the NSA/DSA of the Contractor to re-validate the FSC of the facility.
6. REMARKS	May be used for additional information with regard to the FSC, the facility or the foregoing Items.
7. ISSUING NSA/DSA	State the name of the providing authority (on behalf of the NSA/DSA) and the date of the reply by using the "day/month/year" (dd/mm/yyyy) format.

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

FACILITY SECURITY CLEARANCE INFORMATION SHEET (FSCIS)

All fields must be completed and the form communicated via Government-to-Government or Government to International Organization channels

REQUEST FOR A FACILITY SECURITY CLEARANCE ASSURANCE
TO : _____
(NSA/DSA Country name)

Please complete the reply boxes, where applicable:

[ ] Provide an FSC assurance at the level of: [ ] TS [ ] CTS [ ] S [ ] NS [ ] C [ ] NC
for the facility listed below
[ ] Including protecting of classified material/information
[ ] Including Communication and Information Systems (CIS) for processing classified information

[ ] Initiate an FSC up to and including the level of ..... with …….level of protection and ……level of CIS, if the facility does not currently hold these levels of capabilities.

Confirm accuracy of the details of the facility listed below and provide corrections/additions as required.

	Corrections / additions:
1. Full facility name: ……	……..
2. Full facility address: ……	……..
3. Mailing address (if different from 2.) ……	……..
4. Zip/postal code / city / country ……	……..
5. Name of the Security Officer ……	……..
6. Telephone/Fax/E-mail of the Security Officer ……	……..

7. This request is made for the following reason(s): (indicate particulars of the pre-contractual stage, contract, sub-contract, programme/project):
……
……

Requesting NSA/DSA/NPA/NPO: Name: …… Date: (*dd/mm/yyyy*) ……

REPLY (within 5 working days)

This is to certify that the above mentioned facility:

1. [ ] holds an FSC up to and including the level of:
   [ ] TS [ ] CTS [ ] S [ ] NS [ ] C [ ] NC
   [ ] Other: ……..
2. [ ] on the above mentioned request, the FSC process has been initiated. You will be informed when the FSC has been granted or refused.
3. [ ] does not hold an FSC.
4. has the capability to protect classified information/material:
   [ ] yes, level: ……..…….. [ ] no
5. has Accredited CIS:
   [ ] yes, level: ……..…….. [ ] no
6. This FSC assurance expires on …….. (*dd/mm/yyyy*), or as advised otherwise by the NSA/DSA.
   In case of an earlier invalidation or in case of any changes of the information listed above you will be informed.
7. Remarks:
   ……
   ……

Issuing NSA/DSA:
Name: …… Date: (*dd/mm/yyyy*)....……

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

FACILITY AND PERSONNEL SECURITY CLEARANCE FOR CONTRACTS INVOLVING NATO RESTRICTED INFORMATION - NATIONAL REQUIREMENTS -

"These national requirements for FSC/PSC and notifications for contract involving NR shall not put additional obligations on other NATO nations or Contractors under their jurisdiction".

MEMBER NATION	FSC		Notification of contract/subcontract involving NR information to NSA/DSA		PSC	
	YES	NO	YES	NO	YES	NO
Albania		X	X			X
Belgium		X		X		X
Bulgaria		X		X		X
Canada	X		X		X	
Croatia		X	X			X
Czech Republic		X		X		X
Denmark	X		X		X	
Estonia	X		X			X
France		X		X		X
Germany		X		X		X
Greece		X		X		X
Hungary		X		X		X
Iceland		X		X		X
Italy		X		X		X
Latvia		X		X		X
Lithuania		X		X[2]		X
Luxembourg	X			X	X	
Netherlands	X[3]		X[2]			X
Norway		X	X			X
Poland		X		X		X
Portugal		X		X		X
Romania		X	X			X
Slovakia	X		X			X
Slovenia	X		X			X
Spain		X	X			X
Turkey	X				X	
United Kingdom		X		X		X
United States	X			X		X

[2] NSA/DSA however requests notification by NATO contracting authorities
[3] For military-related contract only

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

CONTRACT SECURITY CLAUSE

FOR INCLUSION IN

TENDERS AND CONTRACTS

INVOLVING

NATO RESTRICTED INFORMATION

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

INTRODUCTION

1. This contract security clause is published by the Security Committee (AC/35) in support of NATO Security Policy, C-M (2002)49, and its supporting directives.

BACKGROUND

2. This contract security clause contains rules and regulations that shall be applied by the Contractor addressing the minimum security requirements for the protection of NATO RESTRICTED (NR) information received or produced by it as a result of the contract. This security clause addresses all aspects of security (personnel security, physical security, security of information, Communication and Information System (CIS) Security, and industrial security) that the Contractor is required to implement.

3. This contract security clause forms part of the contract and shall provide direction to ensure compliance by Contractors on the protection of NR information.

SECTION I - RESPONSIBILITY

4. Contractors handling and/or storing NR information shall appoint an individual of suitable seniority who shall act as the Security Officer (SO) of the facility with responsibility for ensuring the protection of NR information in compliance with the provision of this security clause and any other additional requirements advised by the Contracting Authority. The SO shall also act as the point of contact with the Contracting Authority or if applicable with the National Security Authority (NSA) or Designated Security Authority (DSA).

SECTION II - PERSONNEL SECURITY

5. A Personnel Security Clearance (PSC) is not required for access to information classified NR. Individuals who require access to NR information shall be briefed on security procedures and their responsibilities by the nominated SO, have a need-to-know and acknowledge in writing that they fully understand their security responsibilities and the consequences if information passes into unauthorised hands either by intent or through negligence. A record of the acknowledgement of responsibilities by Contractor's employees shall be retained by the facility security officer.

SECTION III - PHYSICAL SECURITY

6. NR information shall be stored in a locked container that deters unauthorised access; such as a locked desk or cabinet, or in a room or area to which access is controlled (hereinafter referred to as Administrative Zone[4]).

7. NR information shall be handled in Administrative Zones or held under personal custody.

[4] An Administrative Zone may be established around or leading up to NATO Class I or Class II security areas. Such a zone requires a visibly defined perimeter within which the possibility exists for the control of individuals and vehicles. Only information classified up to and including NR shall be handled and stored in Administrative Zones.

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

SECTION IV - SECURITY of INFORMATION

Control and Handling

8. Unless a NATO Nation has specifically mandated contractors under their jurisdiction to do so, NR information is not required to be individually recorded or processed through a Registry System.

Access

9. Access to NR information shall be granted only to personnel involved in the contract who fulfil the conditions according to Paragraph 5, second sentence.

Reproduction

10. Documents, extracts, and translations of information classified NR may be reproduced by individuals authorised for access to the information and on equipment with controlled access.

Destruction Requirements

11. NR information shall be physically destroyed in such a manner that ensures it cannot be reconstructed in full or in part.

12. Destruction of reproduction equipment utilising electronic storage media shall be in accordance with the applicable requirements in section VI.

Packaging

13. Information classified NR shall, as a minimum, be transmitted in a single opaque envelope or wrapping. The markings on the package shall not reveal that it contains information classified NR.

Carriage/ Movement within a Contractor's Facility

14. NR information carried within the perimeter of the site or establishment shall be covered in order to prevent observation of its contents.

National/International Transmission

15. The carriage of NR material shall as a minimum be in a single opaque envelope or packing (no marking shall be visible on the outer envelope) and may be:

(a) moved by postal or commercial services;

(b) carried by Contractor's personnel; or

(c) transported as freight by commercial services.

Release

16. NR shall not be released to entities not involved in the contract without the prior approval of the contracting authority.

Security Incidents

17. Any Incident, which has or may lead to NR information being lost or compromised shall immediately be reported by the SO to the Contracting Authority.

SECTION V - SUB-CONTRACTING

18. Sub-contracts shall not be let without the prior approval of the Contracting Authority.

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

19. Sub-contractors shall be contractually obliged to comply with the provisions of this document and any other additional security requirements issued by the Contracting Authority.

Notification of Contracts

20. Contractors/Sub-contractors under the jurisdiction of a NATO Nation requiring by their national laws and regulations notification of contracts involving NR shall notify their NSA/DSA about any such contracts they have been awarded.

International Visits

21. Visits involving NR information will be arranged directly between the SO responsible for the visitor and the SO of the facility to be visited without formal requirements. The SO of the facility to be visited should be asked if a request for visit is required to be provided to its NSA/DSA and if so, the SO of the facility to be visited should submit a visit request to its NSA/DSA on behalf of the visitor. However, visitors are not required to hold a PSC.

SECTION VI - HANDLING OF NATO RESTRICTED INFORMATION ON INFORMATION AND COMMUNICATION SYSTEMS (CIS)

Security Accreditation of Communication and Information Systems (CIS)

22. Security accreditation shall be performed for all contractors' CIS that are used to handle (store, process or transmit) NATO RESTRICTED (NR) information.

23. This contract security clause contains the rules and regulations that shall be applied by the contractor's SO or other appropriate officer to address and satisfy the minimum security requirements for the protection of NR information received or produced by the contractor as a result of the contract. This clause includes specific provisions to be satisfied by the contractor under delegation from the Contracting Authority for the accreditation of the contractor's CIS handling NR information. Under this delegated authority the contractor shall provide the Contracting Authority with a written statement of compliance confirming that its CIS has been accredited in compliance with the minimum requirements specified below. This written statement may be included in the contractor's response in acknowledgement of the receipt and requirements of the Security Aspects Letter associated with the contract.

24. It is the responsibility of the contractor to implement these minimum security requirements when handling NR on its CIS.

25. The SO shall assess and verify the compliance of the CIS over its entire life-cycle, in order to ensure that it continues to be consistent with the requirements of this document.

26. The following describes the minimum security requirements for handling NR information on contractors' CIS that shall be met:

26.1 Identification and Authentication

26.1.1. An up-to-date list of authorised users shall be maintained by security management staff.

26.1.2. Credentials shall be established and maintained to identify authorised users.

26.1.3. Users shall themselves authenticate to, and be authenticated by, the system before any access to the CIS will be granted.

26.1.4. Passwords shall be a minimum of 9 characters long and shall include numeric and "special" characters (if permitted by the system) as well as alphabetic characters;

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

26.1.5. Passwords shall be changed at least every 180 days. Passwords shall be changed as soon as possible if they have, or are suspected to have been compromised or disclosed to an unauthorised person.

26.1.6. The re-use of a number of previous passwords shall be denied.

26.1.7. The system shall provide only limited feedback information to the user during the authentication process.

26.1.8. Accounts that are no longer required shall be locked or deleted.

26.1.9. When the authentication of the person is not enforced by physical security measures surrounding the location where the system is installed (e.g. perimeter/building security) or by non-technical security measures surrounding the office areas where components of system are located (e.g. server rooms, user workstation areas), two-factor authentication shall be used.

26.2 Access Control

26.2.1. The identification and authentication data shall be used by the system to determine user privileges, in accordance with the access control requirements set out in the security-related documentation.

26.2.2. From the user account only, it shall be possible for the security management staff to identify the specific user and/or roles.

26.2.3. Mechanisms shall be implemented to restrict access to only that information to support a given project or contract, taking into account the need-to-know principle.

26.2.4. Access to security and system information shall be restricted to only authorised security and system administrators.

26.2.5. Access privileges shall be implemented to restrict the type of access that a user may be permitted (e.g., read, write, modify, and delete).

26.2.6. The system (e.g. Operating System) shall lock an interactive session after a specified period of user inactivity by clearing or overwriting display devices, making the current contents unreadable and by disabling any user’s data access/display devices other than unlocking the activity of the session.

26.2.7. The system shall allow user-initiated locking of the user’s own interactive session by clearing or overwriting display devices, making the current contents unreadable and by disabling any user’s data access/display devices other than unlocking the activity of the session.

26.2.8. Security mechanisms and/or procedures to regulate the introduction or connection of removable computer storage media (for example USB, mass storage devices, CD-RWs) to user workstations/portable computing devices shall be implemented.

26.3 Security Audit

26.3.1. An audit log shall be generated and maintained. System Level, Application Level and User Level events shall be included in the log, as required by the relevant Security Authority as a result of a Risk Assessment. For each of the auditable events, it shall associate individual user identities to those events, and shall include date and time of the event, type of event, user identity, and the outcome (success or failure) of the event. The following events shall always be recorded:

- all log on attempts whether successful or failed;
- log off (including time out where applicable);
- the creation, deletion or alteration of access rights and privileges;
- the creation, deletion or alteration of passwords.

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

26.3.2. The audit trail and associated archive shall be protected from unauthorised deletion and/or modification; it shall be presented in humanreadable format either directly (e.g., storing the audit trail in human-readable format) or indirectly (e.g., using audit reduction tools) or both.

26.3.3. Access to audit information shall be controlled; access permissions shall be established to permit access only by the appropriate security management staffs.

26.3.4. The audit data shall be retained for a period agreed by the Contracting Authority, based, where appropriate, on the requirements established by the NSA or DSA.

26.3.5. A means shall be available to analyse and review system activity and audit data, looking for possible or real security violations (analysis may work in support of intrusion detection/ automatic response to an imminent security violation).

26.4 Protection against Malicious Software

26.4.1. Virus/malicious code detection software shall be installed on all servers, portable computing devices and workstations dependant upon the vulnerability of the underlying operating system environment. It shall be configured to automatically check on the introduction of removable media (e.g., CDs, USB mass storage devices, flash memory).

26.4.2. The virus/malicious code detection software shall be regularly updated.

26.5 Mobile Code

26.5.1. The source of the mobile code shall be appropriately verified.

26.5.2. The integrity of the mobile code shall be appropriately verified.

26.5.3. All mobile code shall be verified as being free from malicious software.

26.5.4. Available technical measures shall be enabled to ensure the use of mobile code is appropriately managed. For example, Microsoft Office applications and Internet Browser applications shall be configured to control import/acceptance of mobile code as well as use and creation of mobile code.

26.6 Availability

26.6.1. Security measures ensuring availability of NR information shall be implemented when required by the Contracting Authority.

26.7 Import/Export of Data

26.7.1. Data transfers between machines, virtual or physical, in different security domains shall be controlled and managed to prevent the introduction of NR data to a system not accredited to handle NR data.

26.7.2. All data imported to or exported from the CIS shall be checked for malware.

26.8 Configuration Management

26.8.1. A detailed hardware and software configuration control system shall be available and regularly maintained.

26.8.2. Configuration baselines shall be established for servers, LAN Components, Portable Computing Devices and workstations.

26.8.3. Configuration checks shall be made by appropriate Security Management staff on hardware and software to ensure that unauthorised hardware and software has not been introduced.

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

26.8.4. An inventory of hardware and software should be maintained, with equipment and cabling labelled as part of the inventory.

26.8.5. The configuration of the security enforcing and security relevant functions of the operating system shall only be subject to change by a limited number of authorised system and security administrators.

26.8.6. The security configuration of the operating system shall be maintained with the implementation of the appropriate security patches and updates. Regression Aspects i.e. any potential adverse affects of the modification on existing security measures, shall be considered and appropriate action taken.

26.8.7. The installation and configuration of application software with security relevant or security-enforcing functions shall be subject to a limited number of authorised system and security administrators.

26.8.8. The configuration of the operating system shall be subject to periodic checks to ensure its security compliance.

26.8.9. Changes to the system or network configuration shall be assessed for their security implications/impacts.

26.8.10. The Basic Input/Output System (BIOS) or similar firmware shall be password protected in order to protect access to the system's password data.

26.9 Security Management

26.9.1. Mechanisms shall be implemented which manage security data and functions; only defined authorised users (or roles) may perform security functions and access security relevant data.

26.9.2. The compromise or suspected compromise of NR information shall be immediately reported for inspection and investigation purposes, through the SO, to the Contracting Authority and, if required by national laws and regulations, to the relevant NSA or DSA.

26.10 Approved products

26.10.1. An approved product is one that has been approved for the protection of NR information either by NATO or by the National CIS Security Authority (NCSA) of a NATO Nation or in accordance with national laws and regulations.

26.10.2. The relevant NSA, NCSA or DSA shall be consulted, through the Contracting Authority, to determine, whether approved products shall be used, unless already defined by the NATO policies or equivalent national laws and regulations.

26.11 Security Testing

26.11.1. The system shall be subject to initial and periodic security testing to verify that security measures work as expected.

26.12 Transmission Security

26.12.1. NR information transmitted over a CIS not accredited to handle NR information (e.g. Internet) shall be encrypted using approved cryptographic products.

26.13 Wireless LAN

26.13.1. The range of Access Points shall be set to minimise exposure to external attacks, special attention shall be given to the selection of antennae, their location, power and signal propagation.

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

26.13.2. NR information transmitted over a wireless connection shall be encrypted using an approved cryptographic product.

26.14 Virtualisation

26.14.1. When existing systems are combined using a virtualisation product, the accreditation of each of the systems shall be reviewed to ensure that any mitigations and assumptions previously made are still appropriate.

26.14.2. A deployed virtualisation product itself shall be treated as at least the highest Protective Marking of any of its virtual machines (i.e. NR).

26.14.3. Virtual Machines shall be appropriately configured and managed. System patching, administration of accounts, and maintenance of anti-virus software, shall all be performed as if the machine were a physical machine. The host-operating machine shall also be correctly configured and maintained.

26.14.4. Network routing provided internally by the virtualisation product to connect virtual machines shall not be considered as a security measure. For example, a firewall shall not be virtualised.

26.14.5. The administrative interface for the hypervisor, shall only be used for administration of the hypervisor, and shall not be used for the normal administration of services provided by the virtual machines.

26.14.6. Access to the hypervisor functions shall be appropriately controlled.

26.14.7. The ability to “cut-and-paste” between virtual machines shall be appropriately configured and controlled.

26.14.8. The ability to create virtual machines shall be appropriately configured and controlled.

26.14.9. Virtual Machines shall be suitably de-commissioned after use.

26.14.10. Software based virtual networks created between virtual machines shall be appropriately configured, controlled and monitored.

26.14.11. Virtual Servers and Virtual Workstations shall not be located on the same physical host.

26.14.12. Virtual machines operating in different areas of the system architecture shall not be located on the same physical host, for example, virtual machines operating in a De-Militarised Zone (DMZ) shall not be located on the same physical host as those operating in the LAN.

26.14.13. The management of the Virtualisation infrastructure shall be appropriately controlled. Only Virtual Management, patch management, anti malware and Active Directory communication mode shall be allowed.

26.14.14. Management of the Virtualisation infrastructure shall be performed via a dedicated Administrative account.

26.14.15. The Storage Area Network (SAN) used for Virtualisation shall be isolated and only accessible by the physical host.

26.14.16. The SAN used to host Virtualisation operating at different security classifications shall be isolated onto separate Logical Unit Numbers.

26.14.17. Modifications to the ‘Master Copy/Version’ of a Virtual Machine shall be appropriately controlled.

26.14.18. Network cards shall not be shared across Virtual Machines that are operating in different Security Domains.

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

26.15 Interconnections to a CIS not accredited to handle NR information

26.15.1. Security requirements, specific to interconnection scenarios, are listed in the latest versions of the NATO documents entitled “INFOSEC Technical and Implementation Directive for the Interconnection of Communications and Information Systems (CIS)” (current reference AC/322-D/0030-REV5) and “Supporting Document on the Interconnection of NR Communications and Information Systems (CIS) to the Internet” (current reference AC/322-D(2010)0058). These Directives may be obtained from the Contracting Authority.

26.15.2. Interconnection to another CIS, especially the internet, will significantly increase the threat to a contractor’s CIS and therefore the risk to the security of the NR information handled by the contractor’s CIS. A security risk assessment shall be performed to identify the additional security requirements that need to be implemented as part of the security accreditation process. Security requirements can also be found in the latest version of the NATO document entitled “INFOSEC Technical & Implementation Directive for Computer and Local Area Network (LAN) Security” (current reference AC/322-D/0048-REV2). This Directive may be obtained from the Contracting Authority.

26.15.3. When performed, the security risk assessment shall be included with the statement of compliance to the Contracting Authority.

26.16 Disposal of IT Storage Media

26.16.1. For IT storage media that has at any time held NR information the following sanitisation shall be performed to the entire storage media prior to disposal:

- EEPROM and Flash Memory (e.g. USB sticks, SD cards, solid state drives, hybrid hard drives): overwrite with random data at least three times, then verify storage content matches the random data;
- Magnetic Media (e.g. hard disks): overwrite or degauss;
- Optical Media (e.g., CDs and DVDs): shred or disintegrate into pieces of $10mm^2$ or less;
- Other storage media: seek security requirements from the Security Accreditation Authority.

26.17 Portable Computing Devices (laptops, tablets, etc)

26.17.1. Portable computing devices not using approved encryption shall only be used or stored in an appropriately secure location. Portable computing devices and drives containing NR information that do not use approved encryption shall not be taken outside the contractor’s premises unless held under personal custody. The term “drives” includes all removable media. Any authentication token and/or password(s) associated with the encryption product shall be kept separate from portable computing devices whenever it is not in use, left unattended or in transit.

Physical Security of CIS Handling NR information

27. Areas in which CIS are installed to display, store, process, or transmit NR information shall be established, as a minimum, as Administrative Zones. For mobile solutions (e.g. laptop) used outside of Administrative Zones, the user shall ensure that the displayed content is protected in a way that NR information is not exposed to unauthorised individuals.

28. CIS areas housing servers, network management system, network controllers and communications controllers should be established as separate and controlled areas with an appropriate access control system. Access to these CIS areas should be limited to only specifically authorised persons.

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

Security of NR Removable Computer Storage Media

29. Removable computer storage media containing NR information are required to be labelled with that classification marking. Measures shall be in place to prevent unauthorised access to NR removable computer storage media in order to maintain the need-to-know principle.

Use of CIS Equipment Privately Owned by Contractor's Personnel

30. The use of privately-owned equipment of contractor's personnel (hardware and software) for processing NR information shall not be permitted.

CIS Users' responsibilities

31. CIS users (e.g. end users, administrators) involved in the handling of NR information within the CIS shall be made aware of their responsibilities and the procedures to be followed. The responsibilities and the procedures to be followed shall be documented and acknowledged by CIS users in writing.

Advice

32. Advice or clarification of the provisions of this contract security clause shall be obtained from the Contracting Authority.

Audit/inspection

33. At the request of the contracting authority or relevant NSA/DSA/SAA, the contractor shall provide evidence of compliance with this Contract Security Clause and permit an audit of inspection of the Contractors processes and facilities by representatives of the contracting authority or the contractors NSA/DSA or relevant NATO security authorities to ensure compliance with these requirements.

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

SECURITY ASPECTS LETTER (SAL)

1. In the performance of this contract, the prime Contractor and any Sub-contractor(s) are required to comply with NATO security regulations as implemented by the NSA/DSA of the nation in which the work is performed or in the contracts involving NR information only as established in the Contract Security Clause.

2. All classified information and material shall be protected in accordance with the requirements established by the NSA/DSA of the nation in which the work is performed or in the case of NR information as may also be established in the Contract Security Clause.

3. In particular, the Contractor shall:

(a) appoint an officer to be responsible for supervising and directing security measures in relation to the Request for Proposals (RFP), contract or sub- contract;

(b) submit in due time to the NSA/DSA the personal particulars of the person the contractor wishes to employ on the project with a view to obtaining PSCs at the required level where NC and above is involved;

(c) maintain, preferably through this officer responsible for security measures, a continuing relationship with the NSA/DSA and /or the Contracting Authority in order to ensure that all NATO classified information involved in the bid, contract or sub-contract is properly safeguarded;

(d) limit the copying of any classified materiel (including documents) to the absolute minimum to perform the contract;

(e) supply the NSA/DSA, when so requested by the latter, with any information on the persons who will be required to have access to NATO classified information;

(f) maintain a record of his employees taking part in the project and who have been cleared for access to NATO classified information. This record must show the period of validity and the level of the clearances;

(g) deny access to NATO classified information to any persons other than those authorised to have access by the NSA/DSA or in the case of NR information as determined by the need-to-know;

(h) limit the dissemination of NATO classified information to the smallest number of persons as is consistent with the proper execution of the contract or sub- contract;

(i) comply with any request that persons to be entrusted with NATO classified information sign a statement undertaking to safeguard that information and signifying their understanding of their obligations under national legislation on the safeguarding of classified information, and that they recognise that they may have comparable obligations under the laws of the other NATO nations in which they may have access to classified information;

(j) report to the Security Officer and to his NSA/DSA any breaches or suspected breaches of security, suspected sabotage or subversive activity, any breach giving rise to doubts as to the trustworthiness of an employee, any changes in the ownership, supervisory or managerial staff of the facility or any changes that affect the security arrangements and security status of the facility, and any other information which may be required by the NSA/DSA, such as reports on holdings of NATO classified information or materiel;

(k) obtain the approval of (programme/project office and NSA/DSA) before beginning negotiations with a view to sub-contracting any part of the work which would involve the Sub-contractor having possible access to NATO classified information, and to place

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

the Sub-contractor under appropriate security obligations which in no case may be less stringent than those provided for his own contract;

(l) undertake not to utilise, other than for the specific purpose of the bid, contract or sub-contract, without the written permission of (programme/project office) or the prime Contractor, any NATO classified information supplied to him, and return to (programme/project office) all classified information referred to above, as well as that developed in connection with the contract or sub-contract unless such information has been destroyed, or its retention has been duly authorised by the contracting office or the sub-contracting officer. Such NATO classified information shall be returned at such time as the contracting office may direct; and

(m) comply with any procedure established with respect to the dissemination of NATO classified information in connection with the contract or sub-contract.

4. Any person taking part in the performance of work the classified parts of which are to be safeguarded, must possess the appropriate NATO security clearance issued by his NSA/DSA. The level of this clearance must be at least equal to the security category of the materiel, the related information or specifications where NC or above is involved.

5. Unless specifically authorised to do so by (programme/project office), the Contractor may not pass on any NATO classified information to any third party to whom a request to supply goods or services has been submitted.

6. No change in level of classification or de-classification of documentation or materiel may be carried out unless written authority in this respect is obtained from (programme/project office).

7. No CIS may be used for processing classified information without prior accreditation by the responsible authorities. At the level of NR, such accreditation can be under delegated authority of the responsible accreditation authority or the contracting authority in accordance with Appendix 4.

8. Failure to implement these provisions and the security regulations established by the NSA of the nation where the contractual work is being performed may result in termination of this contract without reimbursement to the Contractor or claim against NATO, (programme/project office) or the national government of the said nation.

9. The (programme/project office) security classification check list indicates the degree of classification of the data and materiel (equipment, information, technical manuals, specifications) which may be handled in the performance of work under this contract and which must be safeguarded in accordance with the provisions of this letter.

10. The contractor shall destroy or return any classified information provided or generated under the contract unless the contracting authority has given written approval to retain such classified information, e.g. for warranty purposes.

11. The Contractor shall be required to acknowledge receipt of an accompanying SAL or Program Security Instruction (PSI) that is made part of the applicable contract and confirm that it understands the security aspects defined. With respect to contracts involving only NR information the Contractor shall also be required to confirm that it will comply with the provisions of the Contract Security Clause and specifically that any company CIS used to handle or process NR classified information has been appropriately security accredited.

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

Project Security Instructions (PSIs) - Structure and Content

The following is provided as guidance for the structure and content of Project Security Instructions (PSIs).

Section	Content
1 Document Control	• The issue number; • the date of issue; • the reference and details of the latest Change Proposal; • any related Contract Amendment; • index of amendments; • PSIs index of contents.
2 Introduction / Definitions	• The purpose of the PSIs; • the authority of the PSIs (for example, Project Security Group); • definitions of frequently used terms in NATO contracts involving classified information.
3 National/NATO/ Industry Officials	• The contact details (name, address, telephone / fax number, e-mail address) for the national / NATO officials involved in the project/programme, who are responsible for the following: - administration and policy; - technical security; - CIS Security. <u>Note</u>: This may be included as an Annex to the PSIs.
4 Security Instructions	• General aspects relating to the exchange of NATO classified information and the responsibilities of the NSAs/DSAs; • definition of the security classifications and markings appropriate to the project/programme; • explanation of terms - classified information, material and documents. • storage and transmission of NATO classified information; • disposal / destruction of NATO classified information; • breaches of security; instructions relating to the loss, compromise or possible compromise of NATO classified information; • instructions relating to the unauthorised release of NATO information.

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

Section	Content
5 Release of Information	Definitions of terms, for example, public release, marketing release, sales release, project information, participants, authorities, and approval; • a release statement, for example, "the release of project information (classified or non-classified) to authorities or persons outside of the project (non-participants) without prior approval is strictly prohibited". • release of project information: - general information - NATO/National policies, required Facility Security Clearances, contractual requirements, security agreements for marketing activities; - release of project information to non-participating bodies; - release in connection with sub-contracting; - public release - general instructions, management of public releases; - sales releases - general instructions, management of sales releases; - marketing releases - general instructions, management of marketing releases; • formats for request for release of project information to non-participants, for use at symposia, seminars, etc., and for public release.
6 Change Procedures	• Procedures for changes to security instructions, including the PSIs; • procedures for changes to the Security Classification Guide; • the use of interim procedures.
7 International Hand Carriage of NATO Classified Documents	• Classification of documents for hand carriage; • conditions when hand carriage of documents is permitted; • courier certificate; • responsibilities of Security Offices in the NPA/NPO, Government bodies and industry - administrative procedures, packaging; • responsibilities of the courier; • instructions in the event of loss of documents; • format for "document transmission notification"; • format for "instructions to persons who are authorised to hand-carry NATO classified documents"; • format for "instructions to prevent customs examination".

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

Section	Content
8 International Visit Control Procedures	• General instructions for international visits; • procedures for one-time and recurring visits, including use of the standard "Request for Visit" format, and lead times; • procedures for emergency visits; • instructions for the use and completion of the standard "Request for Visit" format; • list of authorities concerned with International Visit Control Procedures (Note: This may be included as an Annex to the PSIs).
9 Sub-Contracting	• Definitions of terms, for example, negotiations, Contractor, Sub-contractor, classified contract, and facility security clearance; • security instructions relating to the negotiation of a NATO classified contract; • permission to negotiate contracts; • security classification of contracts.
10 International Transportation	• Security procedures relating to the international transportation of NATO classified material. • Transportation Plan to be established if required.
11 Communication and Information Systems (CIS)	• Security procedures for the accreditation and use of CIS (or reference to a specific document dealing with project-related CIS).
12 Security Classification Guide	• A document which outlines classifications applicable to the programme/project as allocated and approved by the participants (background and/or foreground information, procedures for downgrading and declassification, caveats).

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

FACILITIES/ORGANISATIONS LIST

From: (Letterhead of Management Office/Agency)

To: (Relevant NSA/DSA or NATO Civil or Military Body)

List of government departments, establishments, Contractors and Sub-contractors in (insert country) employed on NATO programme/project (insert name) classified NATO……..

Serial Number	Facilities/ Organisations	Address Telephone/Fax/Email of Security Officer	Security facilities for holding NATO classified information YES (+ level)/NO
1	Example British Aerospace Aircraft Group, Warton Division	Warton Aerodrome, Preston, Lancs. UK Tel.: (+44) XXX XXX XXX FAX: (+44) XXX XXX XXX E-mail:	YES (NATO SECRET)
2	……..	……	……..
3	……..	……	……..

The Security Officer:

---------- (Name)

---------- (Signature)

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

NATO INTERNATIONAL VISIT CONTROL PROCEDURES (IVCPs)

1. INTRODUCTION

1.1 When NATO international visits involve access to information subject to government approval or when or unescorted access to security areas (e.g. Class I/II Security Areas) is necessary, a visit request will be submitted by the visitor through his/her Security Officer, certifying/requesting NSA/DSA and receiving NSA/DSA to the agency, organisation, or facility to be visited. These visit requests are formalized in the standard Request for Visit (RFV) procedure. However specific rules apply for NU or NR visits.

1.2 While in principle the requirement for applying the RFV procedure starts with the classification level NC for information as well as unescorted access to security areas, Appendix 9 identifies nations that require by their laws and regulations a RFV submission for NU or NR visits to their country.

1.3 Visits involving NU or NR information will be arranged directly between the SO responsible for the visitor and the SO of the facility to be visited without formal requirements The SO of the facility to be visited shall submit a visit request to its NSA/DSA as identified in Appendix 9 on behalf of the visitor. However, visitors are not required to hold a PSC.

1.4 Where international visits involve access by the visitor to NATO classified information at the level NC or above or unescorted access to security areas, such visits shall be subject to a formal request for visit and approval by the NSA/DSA of the facility to be visited following procedures as defined in this Appendix.

2. SCOPE

General

2.1 The attached standard procedures have been approved for visits by personnel to facilities of another country. They may also be applied to visits within a country. Member nations also have agreed to include the procedures in their national regulations that govern international visits. Notwithstanding the procedures agreed in this document NSAs/DSAs may for national security reasons refuse a RFV for a visit to one of its facilities.

Special Arrangements for specific programmes/Projects

2.2. While the NATO IVCPs will normally be those defined in this Appendix, in the case of a specific programme/project, when all NSAs/DSAs involved, in co-ordination with the responsible NPA/NPO, determine that these general procedures would not be the best suitable for their specific requirements, they are authorized to establish other procedures, which will be set out in the PSI, that provide a level of protection no less stringent than the principles set out in this Appendix.

2.2.1 Accordingly, where permitted by national rules and regulations, visits involving access to information classified up to and including NATO SECRET may be arranged by exception, directly between the FSOs of the sending and receiving facility, acting on behalf of the NSAs/DSAs involved, provided that such an arrangement is approved by the relevant national authorities.

2.2.2 International Visits to Non-NATO Nations and International Organisations concerning contracts/sub-contracts involving classified NATO information have to adhere to the respective provisions of the relevant Security Agreement or Arrangement in place.

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

Personnel on Loan within a NATO programme/Project

2.3 When an individual (not Contractors) who has been cleared for access to NATO classified information is to be loaned within a NATO programme/project or other classified contract from one Contractor's facility to another one located in another NATO country, or to a NATO body, the individual may be assigned, or have access to NATO classified information at the facility the individual is to be loaned on the basis of a RFV, PSCC or an Attestation of Security Clearance, as appropriate. The RFV, PSCC or Attestation of Security Clearance shall be provided by the parent facility to the facility the individual is to be loaned via its respective NSA/DSA.

3. TYPES OF VISITS AND PROCEDURES

3.1 There are four types of international visit requests. They are as follows:

(a) one-time;

(b) recurring;

(c) emergency; and

(d) amendment.

4. ONE-TIME VISIT

4.1 A one-time visit is a single visit for a specific purpose and to a specific site or sites, which is not anticipated to be repeated within the same calendar year. The duration of the visit will never be longer than the validity of the personnel security clearance of the visitor(s).

4.2 Depending on the laws/regulations of the countries involved, a one-time visit request which is issued for the posting of personnel may require additional information/documents to be included with the RFV Form.

5. RECURRING VISIT

5.1 A recurring visit is for intermittent visits over a specified period of time to a specific site or sites and for a specific purpose. A recurring visit covers normally the duration of a government approved programme, project or contract that requires participating personnel to make intermittent (recurring) visits to military, government, *NATO* or industrial facilities of another country participating in the programme. Visits covering a period of more than one year may be subject to annual review, as agreed by the participating countries NSA/DSA. The duration of the visit will never be longer than the validity of the personnel security clearance of the visitor(s).

6. LEAD TIMES FOR ONE-TIME AND RECURRING VISITS

6.1 The lead time to process one-time and recurring visits is depicted in Appendix 9 which identifies the number of working days to the starting date of the one-time or the starting date of the first of the recurring visit that the request should be in the possession of the receiving NSA/DSA.

7. EMERGENCY VISIT

7.1 An emergency visit is for a one-time visit that must take place as a matter of urgency and importance and as such that the normally required lead time identified in Appendix 9 cannot be met.

7.2 Such unplanned or emergency visits should be arranged only in exceptional circumstances. To qualify as an emergency visit at least one of the following conditions must be met:

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

(a) the proposed visit is related to an official military, government, *NATO* request for proposal/request for tender offer (e.g. submission of, or amendment to, a bid or proposal; attendance at pre-contract negotiations or bidder's conference);

(b) the visit is to be made in response to the invitation of a host government, military, *NATO* official or host contract official and is in connection with an official military, government, international organisations project, programme or contract;

(c) a programme, project, contract opportunity or otherwise significant financial interest will be placed in jeopardy if the visit request is not approved; or

(d) operations and/or personnel are placed in direct jeopardy if the visit is not approved.

7.3 Emergency visit requests shall be critically reviewed, fully justified and documented by the Security Officer of the requesting military, government agency, NATO or industrial facility. Therefore, the requestor must complete the remarks portion in item 15 of the RFV Form to fully explain the reasons behind the emergency RFV.

7.4 When the Security Officer is satisfied that the conditions cited in paragraph 7.2 of this document have been met, the Security Officer will contact a knowledgeable person at the government agency, organisation, or industrial facility to be visited (host facility), directly by telephone, facsimile or email, to obtain tentative agreement for the proposed visit. If tentative agreement is provided to proceed with the visit request, the Security Officer of the military, government agency, international organisations or industrial facility to be visited (host facility) shall then immediately notify its NSA/DSA that an emergency visit request will be submitted by the government agency, organisation, or industrial facility requiring to make the visit (requesting facility) and explain the reason for the emergency. Furthermore, the Security Officer will then follow regular RFV procedures and send the emergency RFV to his/her NSA/DSA.

7.5 As there are no lead times for emergency RFV procedures, it is assumed that mutual understanding between the involved countries about the importance of the emergency RFV will result in adequate processing terms.

8. AMENDMENT

8.1 When an already approved or pending RFV needs to be changed regarding dates, visitors and/or locations, an amendment referring to the original RFV must be submitted.

8.2 Amendments to approved or pending one-time and recurring visits are authorized, provided that the amendments are limited to:

(a) change of dates of visit;

(b) addition and/or deletion of visitors; and

(c) change of location.

8.3 For amendments, the standard RFV Form should be used. The type of visit cannot be changed via the amendment procedure. Amendments should refer to the original request that is still pending or already approved by the receiving NSA/DSA.

8.4 Changes to the dates of a visit, the addition or deletion of visitors or a change of location to be visited should be reported immediately to the receiving NSA/DSA via the standard procedure. Amendments will be accepted by the receiving NSA/DSA up to the number of working days (assuming that there are 5 working days in one calendar week) prior to the approved or pending visit. The lead time to process amendments is depicted in Appendix 9.

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

9. **USE OF THE STANDARD REQUEST FOR VISIT FORM**

9.1 For all types of visit, the standard RFV Form (Attachment 1 to this document) should be used.

9.2 This RFV Form has been designed for automated as well as manual use; however, the use of an electronic form and the transmission via e-mail are strongly encouraged. It is therefore essential that the detailed instructions for completion of a RFV Form described at Appendix A to Attachment 1 of this document be used to fill in each data element. To fulfil this requirement it is advised that Attachment 1 with its two Appendices be used as a hand-out to the visitor through the Security Officer of the agency, organisation or facility. Furthermore, it is advisable to translate those instructions for the use and completion of the RFV Form in the language of the user.

9.3 The completed RFV is normally an unclassified document.

9.4 Completion of the RFV Form should be in one of the official NATO languages.

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

ATTACHMENT 1

STANDARD FORM FOR REQUEST FOR VISIT

1. The attached guidance contains the instructions for the use and completion of a Request for Visit (RFV) Form when a visit authorization is required by the receiving organisations or governments. This form standardizes the elements required for a RFV and places them in a logical order. The RFV Form can be used for manual as well as automated processing; however, the use of an electronic form and the transmission via e-mail are strongly encouraged.

2. It is advisable to use this Attachment and its two Appendices as a hand-out to the visitor. The general principle of this RFV is that only one format will be used when a visit request is necessary.

3. The following Appendices are contained in this Attachment:

(a) Appendix A: Instructions for the use and completion of a Request for Visit; and

(b) Appendix B: Request for Visit Form (and Annexes thereto).

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

APPENDIX A to ATTACHMENT 1

INSTRUCTIONS FOR USE AND COMPLETION OF A REQUEST FOR VISIT

1. GENERAL INSTRUCTION

1.1 The Request for Visit (RFV) must be completed without misstatement or omission. Failure to provide all requested information will delay the processing and possibly lead to the denial of the request.

1.2 This RFV should be typed. Electronic processing and transmitting of the RFV is encouraged. The completed RFV is normally an unclassified document. The completion of the RFV Form should be in either one of the official NATO languages.

1.3 The RFV must be in the possession of the receiving host NSA/DSA in accordance with the RFV lead times detailed in Appendix 9.

1.4 The completed RFV has to be submitted to the Security Officer of the requesting agency, organisation or facility. After completion by the Security Officer of the requesting agency, organisation or facility, the RFV should be sent to the following national agency's address that will process the request (to be inserted by issuing NSA/DSA):

Name of Agency	
Address:	
Fax no:	
E-mail address:	

2. DETAILED INSTRUCTIONS FOR COMPLETION OF REQUEST FOR VISIT

2.1 These detailed instructions are guidance for the visitors and the Security Officers who complete the RFV.

HEADER	Insert full country or international organisation name (e.g. NATO CI Agency, NATO International Military Staff, SHAPE, etc) of the host.
1. TYPE OF VISIT REQUEST	Select the appropriate checkbox for the type of visit request. If the Emergency checkbox is selected, complete the remarks portion in item 15 of the RFV Form to explain the reasons behind the emergency RFV. If the Amendment checkbox is selected, mark the appropriate checkbox for the type of amendments and insert the reference number provided by the NSA/DSA of the original RFV that the amendment is made to. Depending on the laws/regulations of the countries involved, a one-time visit request which is issued for the posting of personnel may require additional information/documents to be included with the RFV Form.

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

2. **TYPE OF INFORMATION/ MATERIAL OR SITE ACCESS**	Select the appropriate checkbox for the type of information/material or site access. The first box covers direct access to information/material classified NC or above. The second box shall be checked when unescorted access to Security Areas (e.g. Class I/II) is required but no direct access to information/material classified NC or above is anticipated.
3. **SUMMARY**	Insert the number of sites to be visited and the number of visitors.
4. **ADMINISTRATIVE DATA**	DO NOT FILL IN - LEAVE BLANK *To be completed by requesting NSA/DSA if required.*
5. **REQUESTING GOVERNMENT AGENCY, ORGANISATION OR INDUSTRIAL FACILITY**	Select the appropriate checkbox (only one box) for the entity of the requesting government agency, organisation or industrial facility. Insert the full name, full postal address (include city, province/state, and postal zone), e-mail address, facsimile number and telephone number.
6. **GOVERNMENT AGENCY(IES), ORGANISATION(S) OR INDUSTRIAL FACILITY(IES) TO BE VISITED**	Complete Annex 1 to the RFV Form to include information on all of the sites to be visited.
7. **DATE OF VISIT**	Insert the period of the visit by using numeral “day/month/year” (dd/mm/yyyy).
8. **TYPE OF INITIATIVE**	Select one item from each column as indicated.
9. **IS THE VISIT PERTINENT TO**	Select the appropriate checkbox and specify the full name of the government project/programme. Foreign Military Sales-case, etc., or request for proposal or tender offer. Abbreviations should be avoided.
10. **SUBJECT TO BE DISCUSSED/ JUSTIFICATION/ PURPOSE**	Give a brief description of the subject(s) motivating the visit. If known, include the details of the host Government/Project Authority and solicitation/ contract number. Abbreviations should be avoided. Remarks: (1) In case of a recurring visit, this item of the RFV Form should state "Recurring Visits" as the first words in the data element (e.g. Recurring Visits to discuss...). (2) It is strongly advised to repeat the subject to be discussed and/or the justification of the visit in the language of the receiving country. (3) Make sure to describe the subject to be discussed in a way that it does not reveal any classified information since the completed RFV is considered to be an Unclassified document.

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

11. **ANTICIPATED HIGHEST LEVEL OF INFORMATION/ MATERIAL OR UNESCORTED ACCESS TO SECURITY AREAS**	Select the appropriate checkbox for the anticipated highest level of information/material or unescorted access to security areas. If the box “Other” is checked, it shall be specified.
12. **PARTICULARS OF VISITOR(S)**	Complete Annex 2 to the RFV Form to include information on all of the visitors. When there is more than one visitor, enter the visitors’ surnames in alphabetic order if possible.
13. **THE SECURITY OFFICER OF THE REQUESTING AGENCY, ORGANISATION OR INDUSTRIAL FACILITY**	This item requires the name, telephone number, e-mail address, and signature of the requesting Security Officer.
14. **CERTIFICATION OF SECURITY CLEARANCE LEVEL**	DO NOT FILL IN - LEAVE BLANK To be completed by government/NATO certifying authority only. In accordance with the laws/regulations of the countries involved, government certifying authority must also complete this item for RESTRICTED. Note for the certifying authority: (1) Insert name, address, telephone number, and e-mail address. (2) Date and signature. (3) If the certifying authority corresponds with the requesting National Security Authority, insert in this item: “See item 14 of the RFV Form”. Remark: Items 13 and 14 of the RFV Form may be completed by the appropriate official of the Embassy of the requesting country as per national legislations, policies or directives.
15. **REQUESTING SECURITY AUTHORITY**	DO NOT FILL IN - LEAVE BLANK To be completed by the requesting NSA/DSA or responsible NATO security office only as per below instructions. (1) Insert name, address, telephone number, and e-mail address. (2) Date and signature.

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

16. **REMARKS**	(1) In case of an emergency visit, it is mandatory to give the reasons for the emergency visit in this field of the RFV Form. The particulars of the knowledgeable person, see paragraph 7.4, should also be identified in this field of the RFV Form. (2) This item can be used for certain administrative requirements (e.g. proposed itinerary, request for hotel, and/or transportation, etc.). (3) This space is also available for the receiving NSA/DSA for processing (e.g., “no security objections”, etc.). (4) In case a special briefing is required, the type of briefing and the date that the briefing was given should be stated.

ANNEX 1 TO RFV FORM	
GOVERNMENT AGENCY(IES), ORGANISATION(S) OR INDUSTRIAL FACILITY(IES) TO BE VISITED	Select the appropriate checkbox (only one box) for the government agency, organisation or industrial facility to be visited. Repeat for every site to be visited. Insert the full name, full physical address (include city, province/state, and postal zone), telephone number and facsimile number. Insert the name, e-mail and telephone number of the main point of contact or the person with whom the appointment for the visit was made. Insert the name, e-mail and telephone number of the Security Officer or the secondary point of contact. <u>Remarks</u>: (1) For visits to the United States, one RFV Form with Annexes for each agency/organisation/facility to be visited should be filled in. (2) For visits to military sites in the United States, it is mandatory to specify which military unit will be visited (e.g. Army, Air Force, Navy, Marine Corps or Defence Intelligence Agency).

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

ANNEX 2 TO RFV FORM	
PARTICULARS OF VISITOR(S)	Select the appropriate checkbox (only one box) for the type of employment of the visitor (e.g. military, defence public servant, government, industry/embedded Contractor, international organisation employee (e.g. NATO, EU, etc.). Repeat for every visitors. Surname: Family name. Forenames: As per passport. Rank: Insert the rank of the visitor if applicable. DOB: Insert date of birth by using numeral "day/month/year" (dd/mm/yyyy). POB: Place of birth (city-province/state-country). Nationality: Insert nationality as per passport. Security clearance level: Actual security clearance status (e.g. TS, S, C). Indicate NATO clearance (CTS, NS, NC) if the visit is related to NATO business. PP/ID Number: Enter the passport number or identification card number, as required by host government. Position: Insert the position the visitor holds in the organisation (e.g., director, product manager, etc.) Company/Agency: Insert the name of the government agency, organisation, or industrial facility that the visitor represents.

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

APPENDIX B to ATTACHMENT 1

All fields must be completed

REQUEST FOR VISIT **TO:** _____ **(Country/NATO body)**		
1. TYPE OF VISIT REQUEST	**2. TYPE OF INFORMATION/ MATERIAL OR SITE ACCESS**	**3. SUMMARY**
☐ One-time ☐ Recurring ☐ Emergency ☐ Amendment ☐ Dates ☐ Visitors ☐ Agency/Facility For an amendment, insert the NSA/DSA original RFV Reference No._____	☐ NATO CONFIDENTIAL or above, or ☐ access to security areas.	No. of sites: _____ No. of visitors: _____

4. ADMINISTRATIVE DATA:	
Requestor: To:	NSA/DSA RFV Reference No._____ Date *(dd/mm/yyyy)*: _____/_____/_____

5. REQUESTING GOVERNMENT AGENCY, ORGANISATION OR INDUSTRIAL FACILITY:

☐ Military ☐ Government ☐ Industry ☐ NATO ☐ *Other:* _____

NAME:

POSTAL ADDRESS:
E-MAIL ADDRESS:

FAX NO: TELEPHONE NO:

6. GOVERNMENT AGENCY(IES) , ORGANISATION(S) OR INDUSTRIAL FACILITY(IES) TO BE VISITED - *(Annex 1 to be completed)*

7. DATE OF VISIT *(dd/mm/yyyy)*: FROM _____/_____/_____ TO _____/_____/_____

8. TYPE OF INITIATIVE *(Select one from each column)*:

☐ Government initiative	☐ Initiated by requesting agency or facility
☐ Commercial initiative	☐ By invitation of the facility to be visited

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

9. IS THE VISIT PERTINENT TO:

☐ Specific equipment or weapon system
☐ Foreign military sales or export licence
☐ A programme or agreement
☐ A defence acquisition process
☐ Other

Specification of the selected subject:

10. SUBJECT TO BE DISCUSSED/JUSTIFICATION/PURPOSE *(To include details of host Government/Project Authority and solicitation/contract number if known and any other relevant information. Abbreviations should be avoided)*:

11. ANTICIPATED HIGHEST LEVEL OF INFORMATION/ MATERIAL OR UNESCORTED ACCESS TO SECURITY AREAS

☐ NATO CONFIDENTIAL ☐ NATO SECRET

☐ COSMIC TOP SECRET ☐ Other

If other, specify:_____

12. PARTICULARS OF VISITOR(S) - *(Annex 2 to be completed)*

13. THE SECURITY OFFICER OF THE REQUESTING GOVERNMENT AGENCY, ORGANISATION OR INDUSTRIAL FACILITY:

NAME:

TELEPHONE NO:

E-MAIL ADDRESS:

SIGNATURE:

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

14. CERTIFICATION OF SECURITY CLEARANCE LEVEL:

NAME:

ADDRESS:

TELEPHONE NO:

E-MAIL ADDRESS:

SIGNATURE: DATE *(dd/mm/yyyy)*: _____/_____/_____

15. REQUESTING NATIONAL SECURITY AUTHORITY/DESIGNATED SECURITY AUTHORITY/*NATO security office*:

NAME:

ADDRESS:

TELEPHONE NO:

E-MAIL ADDRESS:

SIGNATURE: DATE *(dd/mm/yyyy)*: _____/_____/_____

16. REMARKS *(*Mandatory justification required in case of an emergency visit):

ANNEX 1 to RFV FORM

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

GOVERNMENT AGENCY(IES), ORGANISATION(S) OR INDUSTRIAL FACILITY(IES) TO BE VISITED
1. ☐ Military ☐ Government ☐ Industry ☐ *NATO* ☐ *Other:* _____ NAME: ADDRESS: TELEPHONE NO: FAX NO: NAME OF POINT OF CONTACT: E-MAIL: TELEPHONE NO: NAME OF SECURITY OFFICER OR SECONDARY POINT OF CONTACT: E-MAIL: TELEPHONE NO:
2. ☐ Military ☐ Government ☐ Industry ☐ *NATO* ☐ *Other:* _____ NAME: ADDRESS: TELEPHONE NO: FAX NO: NAME OF POINT OF CONTACT: E-MAIL: TELEPHONE NO: NAME OF SECURITY OFFICER OR SECONDARY POINT OF CONTACT: E-MAIL: TELEPHONE NO:

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

GOVERNMENT AGENCY(IES), ORGANISATION(S) OR INDUSTRIAL FACILITY(IES) TO BE VISITED
3. ☐ Military ☐ Government ☐ Industry ☐ *NATO* ☐ *Other:* _____ NAME: ADDRESS: TELEPHONE NO: FAX NO: NAME OF POINT OF CONTACT: E-MAIL: TELEPHONE NO: NAME OF SECURITY OFFICER OR SECONDARY POINT OF CONTACT: E-MAIL: TELEPHONE NO:
4. ☐ Military ☐ Government ☐ Industry ☐ *NATO* ☐ *Other:* _____ NAME: ADDRESS: TELEPHONE NO: FAX NO: NAME OF POINT OF CONTACT: E-MAIL: TELEPHONE NO: NAME OF SECURITY OFFICER OR SECONDARY POINT OF CONTACT: E-MAIL: TELEPHONE NO: ***(Continue as required)***

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

ANNEX 2 to RFV FORM

PARTICULARS OF VISITOR(S)
1. ☐ Military ☐ Government ☐ Contractor's Personnel ☐ NATO ☐ Other IO (Specify: _____) SURNAME: FORENAMES *(as per passport)*: RANK *(if applicable)*: DATE OF BIRTH *(dd/mm/yyyy)*:____/____/____ PLACE OF BIRTH: NATIONALITY: SECURITY CLEARANCE LEVEL: PP/ID NUMBER: POSITION: COMPANY/AGENCY:
2. ☐ Military ☐ Government ☐ Contractor's Personnel ☐ NATO ☐ Other IO (Specify: _____) SURNAME: FORENAMES *(as per passport)*: RANK *(if applicable)*: DATE OF BIRTH *(dd/mm/yyyy)*:____/____/____ PLACE OF BIRTH: NATIONALITY: SECURITY CLEARANCE LEVEL: PP/ID NUMBER: POSITION: COMPANY/AGENCY:

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

PARTICULARS OF VISITOR(S)
3. ☐ Military ☐ Government ☐ Contractor's Personnel ☐ NATO ☐ Other IO (Specify: _____) SURNAME: FORENAMES *(as per passport)*: RANK *(if applicable)*: DATE OF BIRTH *(dd/mm/yyyy)*:____/____/____ PLACE OF BIRTH: NATIONALITY: SECURITY CLEARANCE LEVEL: PP/ID NUMBER: POSITION: COMPANY/AGENCY:
4. ☐ Military ☐ Government ☐ Contractor's Personnel ☐ NATO ☐ Other IO (Specify: _____) SURNAME: FORENAMES *(as per passport)*: RANK *(if applicable)*: DATE OF BIRTH *(dd/mm/yyyy)*:____/____/____ PLACE OF BIRTH: NATIONALITY: SECURITY CLEARANCE LEVEL: PP/ID NUMBER: POSITION: COMPANY/AGENCY: ***(Continue as required)***

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

Annex 3 to Appendix 8

LIST of Authorities concerned with IVCPs

COUNTRY	OFFICE	E-mail
Albania	NSA	E-mail: Sektretaria.nsa@mod.gov.al Tel: +335 4 224 5995
Belgium		
Bulgaria	State Commission on Information Security (NSA)	E-mail: dksi@government.bg
Canada	Industrial Security Sector, Public Works and Government Services Canada, Designated Security Authority (DSA).	E-mail: ssivisites.issvisits@pwgsc.gc.ca
Croatia	NSA/DSA, Office of the National Security Council	E-mail: ivcp@uvns.hr
Czech Republic	NSA	E-mail: posta@nbu.cz
Denmark	Danish Defence Intelligence Service (NSA for the Military Sphere)	E-mail: fe4222@fe-ddis.dk
Estonia	NSA	E-mail: nsa@mod.gov.ee
France	MOD acting as DSA	E-mail: In: Bagneux.sdi–sii@dga.defense.gouv.fr Out: bagneux.sdi-visit@dga.defense.gouv.fr
Germany	RFV's relating to military projects: Federal Office of Bundeswehr Equipment, Information Technology and In-Service Support Division Z1.3 RFV's relating to civil projects: Federal Ministry for Economic Affairs and Energy (DSA) Division - ZB2	E-mail: baainbwZ1.3-bkv@bundeswehr.org Tel.: +49.261.400.13190/13192 Fax: +49.261.400.13189 E-mail: zb2-international@bmwi.bund.de Tel.: +49 228 99615 3621/3605 Fax: +49 228 99615 2603

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

COUNTRY	OFFICE	E-mail
Greece	Hellenic National Defence General Staff F' Division Security Directorate - Industrial Security Office	E-mail: daa.industrial@hndgs.mil.gr Tel: 00 30 210 6572022 Fax: 0030 210 6527612
Hungary	NSA	E-mail: nbf@nbf.hu Tel.: +36.17.95.23.03 Fax: +36.17.95.03.44
Iceland		
Italy	Dipartimento delle Informazioni per la Sicurezza – Ufficio Centrale per la Segretezza	E-mail: mg3437.a03@alfa.gov.it
Latvia	The Constitution Protection Bureau (SAB)	E-mail : ndi@sab.gov.lv
Lithuania	Commission for Secrets Protection Co-ordination	E-mail: nsa@vsd.lt Tel.: +370 706 66701(03) +370 706 66708 Fax: +370 706 66700
Luxembourg	Autorité nationale de Sécurité 207, route d'Esch L-1471 Luxembourg	E-mail: ans@me.etat.lu Tel.: +352.24.78.2210 Fax.: +352.24.78.2243
Netherlands	NSA/DSA	E-mail: NSA: NIVCO@minbzk.nl DSA: indussec@mindef.nl*
Norway	The Norwegian Defence Security Agency	E-mail: fsa.kontakt@mil.no
Poland	NSA	E-mail: nsa@abw.gov.pl
Portugal	NSA/GNS –Rua da Junqueira, 69, 1300-342 Lisboa	E-mail: geral@gns.gov.pt
Romania	National Registry Office for Classified Information (ORNISS)	E-mail: relatii.publice@orniss.ro
Slovakia	NSA	E-mail: podatelna@nbusr.sk

* For visits of military and civilian personnel of NLD MoD and for visits to NLD military premises'

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

COUNTRY	OFFICE	E-mail
Slovenia	NSA	E-mail: gp.uvtp@gov.si
Spain	NSA	E-mail: sp-ivtco@areatec.com
Turkey		
United Kingdom	Defence Equipment and Support PSyA, Ministry of Defence, International Visits Control Office, Poplar-1 # 2004, Abbey Wood, Bristol, England, BS34 8JH, UK	Email: Desinfra-ivco@mod.uk Tel.: + 44 117 91 33840 Fax.: + 44 117 91 34924
United States	For Department of Defense: Mr. Mario Rubio International Security Directorate Office of the Under Secretary of Defense (Policy) Defense Technology Security Administration 4800 Mark Center Drive Suite 07E12 Alexandria, VA 22350	E-mail : Mario.rubio@dtsa.mil Tel.: +1.571.372.2561 Fax.: +1 571.372.2559

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

INTERNATIONAL VISITS PROCESSING TIMES/LEAD TIMES
And
NU OR NR NOTIFICATION REQUIREMENTS

The national requirements for RFV for NU or NR notification shall not put additional obligations on other NATO nations or Contractors under their jurisdiction.

1. The following table depicts the number of working days prior to the date of the one-time visit or the date of the first recurring visit that the request should be in the possession of the receiving host NSA/DSA.

2. Visits involving NR information will be arranged directly between the SO responsible for the visitor and the SO of the facility to be visited without formal requirements. The SO of the facility to be visited should be asked if a request for visit is required to be provided to its NSA/DSA and if so, the SO of the facility to be visited should submit a visit request to its NSA/DSA on behalf of the visitor. However, visitors are not required to hold a PSC.

COUNTRY	RFV REQUIRED		NUMBER OF WORKING DAYS	
	Unclassified Visits	Restricted Visits	Request	Amendment/ Change
Albania	No	Yes	20	10
Belgium	No	No	20	09
Bulgaria	No	Yes	20	No deadline
Canada	Yes 1. May be required for governmental facilities 2. Required for military facilities	Yes 1. May be required for governmental facilities 2. Required for military facilities	20	10
Croatia	No	No	20	7
Czech Republic	No	Yes	20	10
Denmark	No	No	07	05
Estonia	No	Yes	20	05
France	No	No	15	05
Germany	No	No	20	10
Greece	Yes 1. May be required for governmental facilities 2. Required for military facilities	Yes 1. May be required for governmental facilities 2. Required for military facilities	20	10
Hungary	No	No	20	10
Iceland	-	-	-	-
Italy	No	Yes	20	07
Latvia	No	No	20	05
Lithuania	No	Yes	20	10
Luxembourg	No	Yes	20	09
Netherlands	No	Yes required for military facilities only	10	05
Norway	No	Yes	10	05
Poland	No	No	25	10
Portugal	No	No	21	07

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

COUNTRY	RFV REQUIRED		NUMBER OF WORKING DAYS	
	Unclassified Visits	Restricted Visits	Request	Amendment/ Change
Romania	No	No	25	10
Slovakia	No	No	20	10
Slovenia	No	Yes	21	07
Spain	No	No	20	08
Turkey	Yes For military facilities only	Yes For military facilities only	21	10
United Kingdom	No	No	20	05
United States	No	Yes	21	05

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

NATO Agency	NUMBER OF WORKING DAYS	
	Request	Amendment/ Change
NATO Allied Ground Surveillance Management Agency (NAGSMA)	3	2
NATO Helicopter Design & Development Production & Logistics management (NAHEMA)	3	
NATO Medium Extended Air Defence System Design & Development, Production & Logistics Management Agency (NAMEADSMA)	3	
NATO AEW&C Programme Management Agency (NAPMA)	3	1
NATO Communications and Information Agency (NCIA)	3	
NATO EF2000 & TORNADO Development, Production & Logistics Management Agency (NETMA)	3	1
NATO Support Agency (NSPA)	3	1

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

SECURITY ACKNOWLEDGEMENT
(in case of Hand Carriage)

[LETTERHEAD]

SECURITY ACKNOWLEDGEMENT

DECLARATION

(name, forename)

(name of company)

(position in company)

I have been briefed on and provided with instructions concerning the handling and custody of classified documents/equipment to be carried by me. I have read and understood their contents.

I shall always retain en route the classified documents/equipment and shall not open the package unless required by the Customs Authorities.

Upon arrival, I shall hand over the classified documents/equipment intended for the receiving company/organisation, against receipt, to the designated consignee.

(**Place and date**) (**Signature of courier**)

Witnessed by:

(**Security Officer's signature**)

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

COURIER CERTIFICATE

[LETTERHEAD] COURIER

CERTIFICATE **PROGRAMME**

TITLE (optional)

COURIER CERTIFICATE NO. …….. (*)

FOR THE INTERNATIONAL HAND CARRIAGE OF CLASSIFIED DOCUMENTS, EQUIPMENT AND/OR COMPONENTS

This is to certify that the bearer:

Mr./Ms. (**name/title**):

born on: (**day/month/ year**), in (**country**):

a national of (**country**):

holder of passport/identity card no.: (**number**)

issued by: (**issuing authority**)

on: (**day/month/year**)

employed with: (**company or organisation**)

is authorised to carry on the journey detailed below the following consignment:

(**Number and particulars of the consignment in detail, i.e., No. of packages, weight and dimensions of each package and other identification data as in shipping documents**)

…….
…….

* May also be used by security guards.

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

The attention of Customs, Police, and/or Immigration Officials is drawn to the following:

- The material comprising this assignment is classified in the interests of the security of:

(NATO, the country of origin of the shipment and that of the destination shall be indicated. The country(ies) to be transited also may be indicated).

- It is requested that the consignment will not be inspected by other than properly- authorised persons or those having special permission.

- If an inspection is deemed necessary, it is requested that it be carried out in an area out of sight of persons who do not belong to the service and, in the presence of the courier.

- It is requested that the package, if opened for inspection, be marked after re-closing, to show evidence of the opening by sealing and signing it and by annotating the shipping documents (if any) that the consignment has been opened.

- Customs, Police, and/or Immigration Officials of countries to be transited, entered or exited are requested to give assistance, if necessary, to ensure successful and secure delivery of the consignment.

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

ITINERARY

From: (**originating country**) …….

To: (**country of destination**) …….

Through: ……. (**list intervening countries**)

Authorised stops: ……. (**list locations**)

Date of beginning of journey: ……. (**day/month/year**)

Signature of Security Officer of the facility	Signature of the Designated Security Authority
……. (name)	……. (name)
Facility's stamp	Official stamp or NSA/DSA's seal
…….	…….

NOTE: To be signed on completion of journey:

I declare in good faith that, during the journey covered by this "Courier Certificate", I am not aware of any occurrence or action, by myself or by others, that could have resulted in the compromise of the consignment.

Courier's signature: …….

Witnessed by: …….
(signature of Security Officer of the facility)

Date of return of the "Courier Certificate": …….
(day/month/year)

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

[LETTERHEAD]

Annex to the "Courier Certificate", No. …….
for the International Hand Carriage of Classified Material

INSTRUCTIONS FOR THE COURIER ([6])

1. You have been appointed to carry/escort a classified consignment. Your "COURIER CERTIFICATE"/"MULTI-TRAVEL COURIER CERTIFICATE" has been provided. Before starting the journey, you will be briefed on the security regulations governing the hand carriage of the classified consignments and on your security obligations during the specific journey (behaviour, itinerary, schedule, etc.). You will also be requested to sign a declaration that you have read and understood and will comply with prescribed security regulations.

2. The following general points are brought to your attention:

(a) you will be held liable and responsible for the consignment described in the Certificate;

(b) throughout the journey, the classified consignment must stay under your personal control;

(c) the consignment will not be opened en route except in the circumstances described in sub-paragraph (j) below;

(d) the classified consignment is not to be discussed or disclosed in any public place;

(e) the classified consignment is not, under any circumstances, to be left unattended. During overnight stops, military facilities or industrial companies having appropriate security clearance may be utilised. You are to be instructed on this matter by your facility Security Officer;

(f) while hand carrying a classified consignment, you are forbidden to deviate from the travel schedule provided;

(g) in cases of emergency, you must take such measures as you consider necessary to protect the consignment, but on no account will you allow the consignment out of your direct personal control; to this end, your instructions include details on how to contact the security authorities of the countries you will transit as listed in sub-paragraph (l) below. If you have not received these details, ask for them from your facility Security Officer;

(h) you and the facility Security Officer are responsible for ensuring that your personal expatriation and travel documentation (passport, currency and medical documents, etc.) are complete, valid and current;

(i) if unforeseen circumstances make it necessary to transfer the consignment to other than the designated representatives of the company or government you are to visit, you will give it only to authorised employees of one of the points of contact listed in sub-paragraph (l);

[6] May also be used by security guards.

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

(j) there is no assurance of immunity from search by the Customs, Police, and/or Immigration Officials of the various countries whose borders you will be crossing; therefore, should such officials enquire into the contents of the consignment, show them your Certificate and this note and insist on showing them to the actual senior Customs, Police, and/or Immigration Official; this action should normally suffice to pass the consignment through unopened. However, if the senior Customs, Police, and/or Immigration Official demands to see the actual contents of the consignments you may open it in his presence, but this should be done in an area out of sight of the general public;

You should take precautions to show officials only as much of the contents as will satisfy them that the consignment does not contain any other item and ask the official to repack or assist in repacking it immediately upon completion of the examination.

You should request the senior Customs, Police, and/or Immigration Official to provide evidence of the opening and inspection of the packages by signing and sealing them when closed and confirming in the shipping documents (if any) that the consignment has been opened.

If you have been required to open the consignment under such circumstances as the foregoing, you must notify the receiving facility Security Officer and the dispatching facility Security Officer, who should be requested to inform the NSA/DSA of their respective government.

(k) upon your return, you must produce a bona fide receipt for the consignment signed by the Security Officer of the facility or agency receiving the consignment or by an NSA/DSA of the receiving government;

(l) along the route you may contact the following officials to request assistance :

…….

……...

……...

……...

…….

…….

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

Multi-Travels Courier Certificate

[LETTERHEAD]

PROGRAMME TITLE (optional)

MULTI-TRAVELS COURIER CERTIFICATE N° …….

FOR INTERNATIONAL HAND CARRIAGE OF CLASSIFIED DOCUMENTS, EQUIPMENTS AND/OR COMPONENTS

This is to certify that the bearer

Mr/Ms (name/title)

born on (day/month/year) ……. in (country) ……..……,

a national of (country) ……..

holder of passport or identity card n° …….

issued by (issuing authority): …….

on (day/month/year):…….

employed with (facility): ……..……...

is authorized to carry the classified documents, equipments and/or components between the following countries:
……...

The bearer above is authorized to use the present certificate as many times as necessary, for classified shipments between the countries here above until (day / month / year): …….

Each sending is attached with the shipment description.

The attention of Customs, Police and/or Immigration Officials is drawn to the following:

- The material comprising each consignment is classified in the interest of the security of:

(**NATO, the country of origin of the shipment and that of the destination shall be indicated. The country(ies) to be transited also may be indicated).**

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

- It is requested that the consignment will not be inspected by other than properly authorized persons or those having special permission.
- If an inspection is deemed necessary, it is requested that it be carried out in an area out of sight of persons who do not belong to the service and, in the presence of the courier.

It is requested that the package, if opened for inspection, be marked after re-closing, to show evidence of the opening by sealing and signing it and by annotating the shipping documents (if any) that the consignment has been opened.

Customs, Police and/or Immigration Officials of countries to be transited, entered or exited are requested to give assistance, if necessary, to ensure successful and secure delivery of the consignment.

Instructions for the Courier (Attachment 1 of this Appendix) are also applicable.

ATTACHMENT 2
APPENDIX 11
ANNEX 1
AC/35-D/2003-REV5

Attachment to multi-travels courier certificate No:.....

Description of consignment nr: ……..

Transport from (**day/month/year**): ……. to (**day/month/year**): …….

Bearer (name): ……

Itinerary: from (originating country) …… to (destination country) …….
through (crossed countries) …….
authorized stops (list of locations): ……

References of receipt or inventory list:

Description of the consignment (number of package, dimensions and, if needed, weight of each package):

Officials you may contact to request assistance

Signature of the consignor's security officer ……..	Signature of the NSA/DSA ……..
Facility stamp ……..	Official stamp or NSA/DSA's seal ……..

Note to be signed on completion of each journey:

I declare in good faith that, during the journey covered by this "shipment consignment", I am not aware of any occurrence or action, by myself or by others, that could have resulted in the compromise of the consignment.

Courier's signature: ……..

Witnessed by (name and signature of consignor's security officer): ……..

Date of return of the "shipment consignment" (day/month/year): …….

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

INTERNATIONAL TRANSPORTATION PLAN

[LETTERHEAD]

TRANSPORTATION PLAN
FOR THE MOVEMENT OF CLASSIFIED CONSIGNMENTS
(INSERT NAME OF PROGRAMME OR PROJECT)

1. INTRODUCTION

This transportation plan lists the procedures for the movement of classified (**insert Programme/Project/Contract name**) consignments between (**insert Programme Participants**).

2. DESCRIPTION OF CLASSIFIED CONSIGNMENT

Provide a general description of the consignment to be moved. If necessary, a detailed, descriptive listing of items to be moved under this plan, including military nomenclature, may be appended to this plan as an annex. Include in this section a brief description as to where and under what circumstances transfer of custody will occur.

3. IDENTIFICATION OF AUTHORISED PARTICIPATING GOVERNMENT REPRESENTATIVES

This Section should identify by name, title and organisation, the authorised representatives of each Programme/Project participant who will receipt for and assume security responsibility for the classified consignment. Mailing addresses, telephone numbers, fax numbers and network addresses should be listed for each country's representatives.

4. DELIVERY POINTS

(a) Identify the delivery points for each participant (e.g., ports, railheads, airports, etc.) and how transfer is to be effected;

(b) describe the security arrangements that are required while the consignment is located at the delivery points; and

(c) specify any additional security arrangements, which may be required due to the unique nature of the movement or of a delivery point (e.g., an airport freight terminal or port receiving station).

5. IDENTIFICATION OF CARRIERS

Identify the commercial carriers, freight forwarders and transportation agents, where appropriate, that might be involved to include the level of security clearance and storage capability.

6. STORAGE/PROCESSING FACILITIES AND TRANSFER POINTS

(a) List, by participants, the storage or processing facilities and transfer points that will be used; and

(b) describe specific security arrangements necessary to ensure the protection of the classified consignment while it is located at the storage / processing facility or transfer point.

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

7. ROUTES

Specify in this section the routes for movements of the classified consignments under the plan. This should include each segment of the route from the initial point of movement to the ultimate destination including all border crossing. Routes should be detailed for each participant in the logical sequence of the shipment from point to point. If overnight stops are required, security arrangements for each stopping point should be specified. Contingency stop-over locations should also be identified as necessary.

8. PORT SECURITY AND CUSTOMS OFFICIALS

In this section, identify arrangements for dealing with customs and port security officials of each participant. The facility must verify that the courier has been provided with the necessary documentation and is aware of the rules necessary to comply with customs and security requirements. Prior co-ordination with customs and port security agencies may be required so that the Project/Programme movements will be recognised.

Procedures for handling custom searches and points of contact for verification of movements at the initial despatch points should also be included here.

9. COURIERS

When couriers are to be used, relevant provisions specified in Appendix 10 and 11 apply.

10. RECIPIENT RESPONSIBILITIES

Describe the responsibilities of each recipient to inventory the movement and to examine all documentation upon receipt of the movement and:

(a) notify the dispatcher of any deviation in routes or methods prescribed by this plan;

(b) notify the dispatcher of any discrepancies in the documentation or shortages in the shipment; and

(c) clearly state the requirement for recipients to promptly advise the NSA/DSA of the dispatcher of any known or suspected compromise of classified consignment or any other exigencies which may place the movement in jeopardy.

11. DETAILS OF CLASSIFIED MOVEMENTS

This section should include the following items:

(a) identification of dispatch assembly points;

(b) packaging requirements that conform to the national security rules of the Project/Programme participants. The requirements for dispatch documents seals, receipts, and storage and security containers should be explained. Any unique requirement of the Projects/Programme participants should also be stated; documentation required for the dispatch points;

(c) courier authorisation documentation and travel arrangements;

(d) procedures for locking, sealing, verifying and loading consignments. Describe procedures at the loading points, to include tally records, surveillance responsibilities and witnessing of the counting and loading arrangements;

(e) procedures for accessibility by courier to the shipment en route;

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

(f) procedures for unloading at destination, to include identification of recipients and procedures for change of custody, and receipt arrangements;

(g) emergency communication procedures. List appropriate telephone numbers and points of contact for notification in the event of emergency; and

(h) procedures for identifying each consignment and for providing details of each consignment (see Attachments); the notification should be transmitted no less than six working days prior to the movement of the classified consignment.

12. RETURN OF CLASSIFIED MATERIAL

This section should identify requirements for return of classified material to the manufacturer or sending country (e.g., warranty, repair, test and evaluation, etc.).

(a) Samples of these forms should be included, as appropriate, as enclosures to the plan as necessary.

(1) packing list;

(2) classified material receipts;

(3) bills of lading;

(4) export declaration;

(5) waybills;

(6) other nationally-required forms.

(b) NSAs/DSAs reserve their right to add additional measures in the course of establishing the Transportation Plan if required.

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

NOTICE OF CLASSIFIED CONSIGNMENT

NOTICE OF (INSERT PROGRAMME/PROJECT NAME)

CONSIGNMENT APPROVED TRANSPORTATION PLAN REFERENCE No.
(INSERT REFERENCE)

REPLY BEFORE: (insert date)

1. Consignor / consignee:
(include the name, telephone number and address of the person(s) responsible for the consignment at both locations).

2. Government Designated Personnel:
(include name, telephone number and address of releasing and receiving authorised representatives, as applicable).

3. Description of consignment:

   (a) contract or Tender Number;

   (b) export licence or other applicable export authorisation citation;

   (c) consignment description:
   (describe items to be shipped and their classification);

   (d) package description:
   - type of package (wood, cardboard, metal, etc.);
   - number of packages;
   - number of enclosed classified items in each package;
   - package dimensions/weight:
     (include length, width, height and weight);

   (e) indicate if package contains any hazardous material.

4. Routing of consignment:

   (a) date / time of departure;

   (b) date / estimated time of arrival;

   (c) routes to be used between point of origin, point of export, point of import and ultimate destination:
   (identify specific transfer points; use codes that appear in transportation plan, if applicable);

   (d) method of transport for each portion of the shipment:
   (include names and addresses of all carriers and flight, rail or ship numbers, as applicable);

   (e) freight forwarders/transportation agents to be used:
   (include name, telephone number, address of companies if not specified in transportation plan);

   (Note: ***Consignor must re-verify clearance and safeguarding capability of these entities prior to releasing shipments*****);**

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

(f) customs or port security contacts:
(list names and telephone numbers, if different from approved transportation plan procedures).

5. Name(s) and identification of authorised courier.

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

AUTHORISATION FOR SECURITY GUARDS

Valid until ……

This is to certify that Mr./Ms. ……..

a member of the (firm/establishment) ……..

……

holder of Passport No. ……. is authorised to act as security guard on the journey detailed below for transportation by:

- air*
- rail*
- road*
- sea*

of a classified consignment relating to the work carried out by the above-mentioned firm/ establishment in the interests of the **North Atlantic Treaty Organisation**.

ITINERARY

From … ……. To … ……. Approximate Date …….

Stamp of Firm/Establishment Signature of Authorising Official

Stamp of Government Agency Signature of Authorising Official

* Delete as applicable

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

NATO PERSONNEL SECURITY CLEARANCE CERTIFICATE (PSCC)

1. Certification is hereby given that:

Full Name:

.....

Date and Place of Birth:

.....

has been granted a personnel security clearance by the Government of:

.....

in accordance with current NATO regulations, including the Security Annex to C-M(64)39 in the case of ATOMAL information, and is, therefore, declared suitable to be entrusted with information classified up to and including[1]:
.....
.....

2. The validity of this certificate will expire not later than[2]:
.....

Signed:

Title: Official government stamp

Date of Issue:

Contact details of the issuing authority (Phone, e-mail, fax):
.....

---

1 Insert, as appropriate, one or more of the following:

(a) COSMIC TOP SECRET
(b) NATO SECRET
(c) NATO CONFIDENTIAL
(d) COSMIC TOP SECRET ATOMAL
(e) NATO SECRET ATOMAL
(f) NATO CONFIDENTIAL ATOMAL

2. The date of expiry shall conform with the provisions of paragraph 18 of the Directive on Personnel Security.

(*) The marking is not part of the template.

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2017)0008(INV) - DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

ATTESTATION OF NATO PERSONNEL SECURITY CLEARANCE (APSC)

1. Attestation is hereby given that:

Full Name ……

Date of Birth ……

Place of Birth ……..

Nationality ……

Where employed ……

Purpose and Duration of Visit ……..
……..
……..

Holder of Passport/Identity Card No. .....……
Issued at ..... Dated .....……

Military Rank and Number (where applicable) .....
.....
has been granted access to NATO information classified up to and including
..... in accordance with current NATO security regulations, including the Security Annex to C-M(64)39 in the case of ATOMAL information, and has been briefed accordingly by
.....

Signed:

Title: Official stamp

Date of Issue:

2. The validity of the attestation will expire no later than:
.....……...……...

3. Issued by ……
(Member nation or NATO civil or military body)

Date and Place of Issue:
.....

Contact details of the issuing authority (Phone, e-mail, fax):
.....

(*) The marking is not part of the template.

DECLASSIFIED - PUBLICLY DISCLOSED - AC/35-D/2004-REV2-AS1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

NATO OTAN
NORTH ATLANTIC COUNCIL
CONSEIL DE L'ATLANTIQUE NORD

NATO UNCLASSIFIED

15 November 2013

DOCUMENT
AC/35-D/2004-REV3

SECURITY COMMITTEE

Primary Directive on CIS Security

Note by the Chairman

1. At Annex 1 is the third revision of the "Primary Directive on CIS Security".

2. This directive, approved by both SC in CIS Security format SC(CISS) and C3B under silence procedure, will be subject to periodic review.

3. The Primary Directive is published jointly by the Security Committee (SC) and the C3 Board (C3B) in support of NATO Security Policy (C-M(2002)49).

4. This document replaces AC/35-D/2004-REV2 which should be destroyed.

(Signed) Stephen F. Smith

1 Annex

Action officer: Mr. M. C[illegible]

NATO HQ - QG OTAN
DMS 1992254
DOCUMENT

DECLASSIFIED - PUBLICLY DISCLOSED - AC/35-D/2004-REV2-AS1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

Primary Directive on Communication and Information System Security

Contents

1. Introduction 1-2
2. Purpose 1-2
3. Scope 1-3
4. Security Objectives 1-3
5. Security Principles 1-4
6. Minimum security requirements 1-4
7. CIS Security controls 1-5
7.5. CIS Security Policy Governance 1-6
7.6. Risk management 1-6
7.6.5. Threats and vulnerabilities 1-7
7.7. Security Accreditation 1-8
7.8. Security audit 1-9
7.9. Business continuity 1-10
7.10. Trustworthiness management 1-10
7.11. Security design of CIS 1-12
7.11.3. Security Modes of Operation 1-12
7.12. Interconnection of CIS 1-13
7.13. Application security 1-15
7.14. Cryptographic security 1-15
7.15. Emission security 1-15
7.16. Third party service delivery 1-15
7.17. Security related logs 1-15
7.18. Security baselines 1-16
7.19. Malware defence 1-16
7.20. Access control 1-17
7.21. Incident response 1-18
7.22. Security Management Infrastructure 1-19
7.23. CIS Security Training and Awareness 1-19

Appendix 1 - Roles and Responsibilities of NATO and national bodies involved in CIS Security 1-21

Appendix 2 - CIS Security-related Activities in the CIS Life Cycle 1-24
1. Introduction 1-24
2. CIS Planning 1-25
3. CIS Development and Procurement 1-28
4. CIS Implementation and Security Accreditation 1-32
5. CIS Operation 1-34
6. CIS Enhancement 1-36
7. CIS Withdrawal from Service and Disposal of Equipment 1-39

Appendix 3 - NATO CIS Security Documentation Structure 1-40

DECLASSIFIED - PUBLICLY DISCLOSED - AC/35-D/2004-REV2-AS1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

1. Introduction

1.1. The requirement to protect NATO information, supporting system services and resources as well as supporting communication and information systems and other electronic systems (hereafter referred to CIS) is based upon the principles set out in the following policies:

(a) NATO Information Management Policy (NIMP) (C-M(2007)0118);

(b) Security within the North Atlantic Treaty Organisation (C-M(2002)49);

(c) NATO Policy on Cyber Defence (C-M(2011)0042).

1.2. In particular, Enclosure “B” of the Policy on Security within the North Atlantic Treaty Organisation defines Communication and Information System (CIS) Security as the application of security measures for the protection of CIS, and the information that is stored, processed or transmitted[1] in these systems with respect to confidentiality, integrity, availability, authentication and non-repudiation.

2. Purpose

2.1. The Primary Directive on CIS Security is published by the Security Committee (SC) and the Consultation, Command and Control Board (C3B), for the following purpose:

(a) to support the implementation of the NIMP, Enclosure "F" of the Policy on Security within the North Atlantic Treaty Organisation and the NATO Policy on Cyber Defence;

(b) to provide the relation among the NIMP, the Policy on Security within the North Atlantic Treaty Organisation, the NATO Policy on Cyber Defence, the CIS Security management directives and guidance published by the SC, and the CIS Security technical and implementation directives and guidance published by C3B;

(c) to set out the CIS Security activities in the life-cycle of CIS which are essential to identify an appropriate level of protection for CIS handling NATO information, cope with the evolving threat environment and enable organisations to fulfil their mission by aligning security with their business objectives;

(d) to identify NATO committees, NATO civil and military bodies, and National bodies with a responsibility on CIS Security.

[1] Hereafter referred to within this Directive as handled.

DECLASSIFIED - PUBLICLY DISCLOSED - AC/35-D/2004-REV2-AS1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

3. **Scope**

3.1. This Primary Directive is mandatory and binding upon CIS handling NATO classified information. It is supported by management and technical and implementation directives and guidance on CIS Security. In this directive, where it states “for NATO CIS”, it is only mandatory and binding upon CIS in NATO civil and military bodies and NATO CIS extended into national or multi-national bodies.

3.2. The Policy on Security within the North Atlantic Treaty Organisation and its Enclosure “F” on CIS Security are applicable exclusively to NATO classified information and supporting CIS while the NATO Information Management Policy and the NATO Policy on Cyber Defence require that appropriate protection is provided as well to NATO information and CIS other than classified.

3.3. As this Directive supports collectively the NATO Information Management Policy, the NATO Policy on Cyber Defence and the Policy on Security within the North Atlantic Treaty Organisation, it defines also CIS Security requirements for NATO Civil and Military Bodies to protect NATO CIS handling non-classified information.

3.4. National Security Authorities (NSAs), Designated Security Authorities (DSAs), Strategic Command Security Authorities, and the NATO Office of Security (NOS) are responsible for ensuring the implementation of this directive. The NATO CIS Security Accreditation Board (NSAB) shall ensure a consistent implementation of this directive for NATO CIS.

4. **Security Objectives**

4.1. Enclosure “F” of the Policy on Security within the North Atlantic Treaty Organisation sets the following five security objectives:

(a) confidentiality - to ensure the confidentiality of information by controlling the disclosure of, and access to, NATO classified information, and supporting system services and resources;

(b) integrity - to ensure the integrity of NATO classified information, and supporting system services and resources;

(c) availability - to ensure the availability of NATO classified information, and supporting system services and resources;

(d) authentication - to ensure the reliable identification and authentication of persons, devices and services accessing CIS handling NATO classified information;

(e) non-repudiation - to ensure appropriate non-repudiation for individuals and entities having processed the information.

4.2. The degree of applicability of these security objectives is specific to any CIS and shall be determined by a number of factors including the mission objectives, the minimum security requirements established by the Policy on Security within the North Atlantic Treaty

DECLASSIFIED - PUBLICLY DISCLOSED - AC/35-D/2004-REV2-AS1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

Organisation and supporting Directives and, where appropriate, the results of the security risk management process.

5. Security Principles

5.1. In order to meet the security objectives the following security principles shall be followed:

(a) Security Risk Management - for NATO CIS, security risk management processes shall be applied throughout the lifecycle to monitor, reduce, eliminate, avoid or accept risks;

(b) Minimality - only the functions, protocols, and services required to carry out the operational mission shall be installed and used;

(c) Least Privilege – entities using CIS shall only be given privileges and authorisations they require to perform their tasks and duties;

(d) Self-protecting CIS - each CIS shall treat other CIS as un-trusted and implement protection measures to control the exchange of information with other CIS;

(e) Defence-in-Depth - protection measures shall be designed using an architectural approach and implemented in CIS components, in security products and in data to the extent possible, so that there are multiple lines of defence;

(f) Up-to-date Security Posture - secure configuration of CIS shall evolve to maintain the required level of security while addressing changes in the threat environment;

(g) Resilience - mission critical CIS shall have the ability to quickly adapt to and/or recover from any type of disruption in order to continue operations at an acceptable level based on the mission objectives and the security impact of the disruption;

(h) Security Functionality Assurance - the security functionality of mechanisms and products enabling or providing security services to CIS shall be assured by a qualified authority;

(i) Security Compliance - the application of these principles and the subsequent implementation of the protection measures shall be initially verified, continuously monitored, and periodically assessed by the SAA; results shall be reported to senior management commensurate with evolving risks and where deficiencies are identified, these shall be addressed.

6. Minimum security requirements

6.1. For CIS handling NATO information, there are minimum security requirements to be implemented in order that the security objectives are achieved. These minimum security requirements are set out in Enclosure “F” of the Policy on Security within the North Atlantic Treaty Organisation, the Primary Directive on CIS Security and the directives and supporting documents on the management, technical and implementation aspects of CIS Security issued by SC and C3B.

DECLASSIFIED - PUBLICLY DISCLOSED - AC/35-D/2004-REV2-AS1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

6.2. For NATO CIS and other CIS handling NATO classified information[2], when not in contradiction with higher policies and directives, exceptional deviations from the minimum security requirements defined by SC and C3B in their Directives related to the management, technical and implementation aspects of CIS security shall only be authorised by SAAs or for NATO CIS handling non-classified information by designated NATO authorities. In both cases the following conditions apply:

(a) a formal security risk assessment is mandated to prove that mitigating measures have reduced the risk of not implementing the minimum security requirements to a level considered acceptable by the SAA or designated authority for non-classified CIS;

(b) the deviation from the minimum security requirements is positively assessed in the context of the overall security architecture which considers a balanced set of security measures to achieve an appropriate level of protection.

7. CIS Security controls

7.1. Security is dynamic in nature and shall be considered throughout the CIS life-cycle. Its requirements and effects shall be reviewed in each stage of the CIS life-cycle, from inception to disposal, through an iterative approach which allows deriving specific security measures from high level security controls of policy, organisational, procedural and technical nature.

7.2. Security is an enabler of an organization's requirements for secure, reliable information-sharing, even though it may constrain the solutions that can be implemented. It has an impact on the associated civil works, the organisation of the operation and maintenance, on personnel requirements and costs. Security planning shall therefore involve the close interaction between the operational user, CIS planning and implementation authorities (CISPIA) (e.g. system architects), CIS Providers (CISP) and the appropriate SAAs.

7.3. In order to counter threats and reduce or eliminate vulnerabilities, security shall be addressed at project inception, starting from the conception of the CIS, so that cost-effective countermeasures can be provided to minimize the security risks anticipated during the development and operation phases of the CIS life-cycle. Countermeasures introduced retrospectively will inevitably be more expensive, and may well be less effective, than those identified and addressed at the inception of the project. Nevertheless, just as security risks evolve, based on changing CIS value, threats and vulnerabilities, so too do countermeasures evolve. CIS planners therefore shall ensure that sufficient funding and resources are available and allocated for the security aspects of the CIS, at all stages. CIS planners shall also ensure that the requirements for products related to CIS Security are clearly identified.

---

[2] In this Directive the description "NATO CIS and other CIS handling NATO classified information" refers to all NATO CIS including those handling non-classified information.

DECLASSIFIED - PUBLICLY DISCLOSED - AC/35-D/2004-REV2-AS1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

7.4. In order to guarantee that NATO information and CIS are protected by a balanced set of security measures in a cost-effective manner, CIS Security policies, processes, roles and measures shall be designed and managed to mutually complement and integrate with those related to personnel security, physical security, security of information and, where appropriate, industrial security.

7.5. CIS Security Policy Governance

7.5.1. Governing CIS Security includes establishing strategic direction, through policies, directives and guidance on the protection of CIS handling NATO information, as well as defining related roles and responsibilities. In this context, the following authorities are identified:

(a) the SC responsible for the Enclosure “F” (CIS Security) of the Policy on Security within the North Atlantic Treaty Organisation;

(b) the SC in CIS Security Format (SC(CISS)), responsible for the Primary Directive on CIS Security as well as for directives, supporting documents and guidance on the management aspects of CIS Security;

(c) the C3B and its substructure, responsible for directives, supporting documents and guidance on the technical and implementation aspects of CIS Security;

(d) the Defence Policy and Planning Committee in reinforced format (DPPC(R)), responsible for the Cyber Defence Policy;

(e) the Military Committee (NAMILCOM) for military requirements;

(f) various NATO civil committees for their civil requirements.

7.5.2. Additional NATO and national bodies directly or indirectly involved in CIS Security matters are listed at Annex I.

7.6. Risk management

7.6.1. Security risk management is a systematic approach to determine which security counter-measures are required to protect information and CIS, based upon an assessment of the assets value, threats, vulnerabilities and impact on the mission objectives. Risk management involves planning, organising, directing and controlling resources to ensure that the risk remains within acceptable bounds.

7.6.2. Security risk management processes shall be applied to monitor, reduce, eliminate, avoid or accept risks associated with NATO CIS. The aim is to select a solution which results in a satisfactory trade-off between user requirements, resources and residual security risk whilst ensuring that minimum security requirements are applied for the protection of NATO information, in accordance with the requirements of NATO security policies and supporting directives.

DECLASSIFIED - PUBLICLY DISCLOSED - AC/35-D/2004-REV2-AS1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

7.6.3. For NATO CIS, security risk assessment, as part of security risk management, shall be embedded in the system development process. It is conducted jointly by representatives of the CIS Operational Authority (CISOA), CISPIA, CISP and SAA or designated NATO authority for non-classified CIS, using an agreed security risk assessment methodology. It involves assessment of existing, enhanced or new options, including balanced sets of technical and non-technical security measures.

7.6.4. The residual security risk is the risk which remains after implementing the security measures in a CIS, based on the understanding that not all threats can be countered and not all vulnerabilities can be eliminated or reduced. Threats and vulnerabilities are dynamic, therefore the residual risk changes. For this reason, risk shall be managed throughout the life-cycle of NATO CIS, implying that resources will be required to address security risk management through, by example, maintaining secure configuration baselines, analyzing the security impact of system changes, and reporting security compliance.

7.6.5. **Threats and vulnerabilities**

7.6.5.1. The security risk assessment shall be based on a current and up-to-date threat assessment and address the impact of threats and vulnerabilities on the achievement of the security objectives. A threat may be defined, in general terms, as the potential for the accidental or deliberate compromise of security. In the case of CIS Security, such a compromise involves loss of one or more of the security objectives of CIS Security.

7.6.5.2. A vulnerability may be defined as a weakness or lack of controls that would allow or facilitate a threat actuation against a specific asset or target. A vulnerability may be an omission or it may relate to a deficiency in a control's strength, completeness or consistency and may be technical, procedural or operational in nature.

7.6.5.3. Within NATO, there are a significant number of CIS handling NATO information, ranging from stand-alone computers and mobile devices, through small Local Area Networks (LANs), to large and complex Wide Area Networks (WANs). NATO information, in a concentrated form designed for rapid retrieval, communication and use, may be vulnerable to access by unauthorised users, to denial of access to authorised users, and to corruption, unauthorised modification and unauthorised deletion. Furthermore, the complex and sometimes fragile system equipment is expensive and often difficult to repair or replace rapidly.

7.6.5.4. CIS are attractive targets for intelligence gathering operations, especially if security measures are ineffective. They can enable large quantities of NATO information to be obtained quickly and surreptitiously. Any operation carried out by hostile intelligence services (or subversive organisation's and terrorist group's members or sympathisers) targeting NATO and its member nations is likely to be well planned and executed. Denial of authorised access to CIS or corruption of the data within them may be an equally attractive target, and no less harmful to NATO's missions, whether or not the information involved is classified.

DECLASSIFIED - PUBLICLY DISCLOSED - AC/35-D/2004-REV2-AS1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

7.6.5.5. The insider represents a unique threat vector to any organisation because of its privileged position in respect to physical and logical access to its CIS and the information within them. In contrast to an outsider, an insider has better situational awareness (e.g. knowledge of weaknesses), more time, fewer security controls to bypass and legitimate privileges for access to secure areas, CIS and information, by virtue of his/her role within the organisation (e.g. system administrator). These factors, combined with the possibility for an insider to commit any type of malicious act, would certainly magnify the impact of any incident.

7.6.5.6. Therefore, in order to deter, prevent and counter such a particular threat a set of specific security measures, shall be applied to CIS handling NATO information. In the selection of these measures, organisations shall take into account also the following:

(a) security measures shall be specifically designed to cope with the insider threat and support incident response and investigative procedures;

(b) close coordination and information sharing among the internal or external organisational elements (e.g. Personnel Security, Physical Security, Human Resources, Intelligence) which can contribute managing properly the insider threat shall be established.

7.7. Security Accreditation

7.7.1. The security accreditation process shall determine the extent to which CIS Security measures are to be relied upon for the protection of NATO information and CIS, during the process of establishing the security requirements.

7.7.2. The security accreditation process shall determine that an adequate level of protection has been achieved and is being maintained. Central to this process is the identification of an acceptable level of residual risk which needs to be monitored throughout the CIS life-cycle.

7.7.3. The security accreditation process shall be carried out for NATO CIS and other CIS handling NATO classified information, in accordance with the requirements of the relevant CIS Security management directives.

7.7.4. The responsibility for the security accreditation process is assigned to:

(a) SAAs for CIS handling NATO classified information and non-classified NATO CIS providing services essential to achieve the security objectives of NATO classified CIS (e.g. non-classified network providing bearer service to classified CIS);

(b) Heads of NATO Civil and Military Bodies for NATO CIS handling only non-classified information.

7.7.5. Security accreditation of NATO CIS handling non-classified information may involve the SAA as a result of a joint decision between the Head of a NATO Body and the relevant SAA, considering aspects such as the criticality and sensitivity of the CIS,

DECLASSIFIED - PUBLICLY DISCLOSED - AC/35-D/2004-REV2-AS1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

the overall impact that a compromise of the security objectives would have, the need for a more independent and thorough approach to security accreditation and resource implications.

7.7.6. Where the involvement of the SAA is deemed necessary, this shall be formalised in the Security Accreditation Plan (SAP) which shall be approved by both the Head of the NATO Body and the relevant SAA.

7.7.7. For NATO CIS handling non-classified information, the SAA retains authority to verify that these CIS are built and maintained conformant to the relevant NATO policies, directives and supporting documents addressing CIS Security.

7.7.8. Where a NATO CIS handling non-classified information falls under the responsibility of more than one NATO Body, a joint security accreditation board shall be established or identified, following advice by the NSAB.

7.7.9. Security-related documentation shall be established and maintained in accordance with the requirements of the relevant CIS Security management directives and the SAA. Security-related documentation shall be required throughout the CIS life-cycle, from the planning stage until the disposal stage. The security-related documentation shall be developed in an iterative process throughout the CIS life-cycle.

7.8. Security audit

7.8.1. Security audits shall be performed to verify that NATO CIS and other CIS handling NATO classified information comply with NATO policies, directives and supporting documents on CIS Security, and operate in accordance to the security baselines defined by the CISP, in conjunction with the SAA or designated authority for NATO CIS handling non-classified information. Security audits may also be used to support prevention or investigation of incidents.

7.8.2. Security audit methods include security inspections, reviews, interviews and tests. Whenever possible, reviews and tests shall be supported by automated tools.

7.8.3. Security audits shall be conducted in accordance with the requirements set in the appropriate directives on the management aspects of CIS Security and under the authority of the SAA.

7.8.4. For NATO CIS, security audits shall be carried out as well to:

(a) verify that the security measures, resultant from the security risk management process, are correctly implemented and maintained;

(b) validate the appropriateness of the security risk management process and results;

(c) verify that security standards (e.g. security baselines, security architectures) are consistently adopted throughout NATO;

DECLASSIFIED - PUBLICLY DISCLOSED - AC/35-D/2004-REV2-AS1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

(d) assess the maturity of CIS Security capabilities and the status of implementation of related programmes/projects;

(e) assess the effectiveness of CIS Security processes and capabilities by means of measures and measurement.

7.9. Business continuity

7.9.1. Business continuity is a key process that identifies potential impacts threatening an organisation's mission. It also provides a framework for building resilience with the capability for an effective response that minimises disruption to the organisation and its mission objectives in the event of an incident.

7.9.2. In the context of business continuity, the security measures necessary to support resilience in a NATO CIS, including plans and procedures, shall be identified through security risk assessment and business impact analysis and formalised in the context of the overall Business Continuity Plan (BCP) of an organisation. While the security risk assessment shall identify the critical functions and assets and the risks that can cause interruptions to the organisation's mission, a business impact analysis shall be undertaken to identify the potential damage or loss in the event of an incident, the form that the damage may take and how the degree of damage may increase over time.

7.10. Trustworthiness management

7.10.1. Trustworthiness in CIS Security is a complex issue that regards CIS, their components and the supply chain through which these are acquired as well as other parties that may have an impact on CIS Security. Managing trustworthiness is a key element as this allows determining the extent to which CIS, their components and related supply chains are to be relied upon for the protection of NATO information and supporting CIS. Evidence of trustworthiness can be produced using specific and formal assurance techniques, such as certification of products or vendors' processes, or less rigorous means such as information about the manufacturer (e.g. reputation).

7.10.2. Security functionalities of NATO CIS and national CIS handling NATO classified information and related products shall be assured by trusted authorities through formal assurance techniques.

7.10.3. Formal assurance techniques for products include:

(a) Evaluation as the detailed technical examination, by the appropriate national, international or NATO evaluation authority, of the security aspects of a product. The evaluation confirms the presence of required security functionality, the absence of compromising side-effects from such functionality and makes an assessment of the incorruptibility of such functionality. The evaluation determines the extent to which the security claims for a product are satisfied and establishes the conformance of the product's trusted function.

DECLASSIFIED - PUBLICLY DISCLOSED - AC/35-D/2004-REV2-AS1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

(b) Certification as the issue, by an appropriate national, international or NATO evaluation authority, of a formal statement, as a result of a successful evaluation as described above;

(c) Approval as the issue, by an appropriate authority, of a formal statement, supported by an independent review of the conduct and results of an evaluation and/or a certification, approving the use of a product for a specific purpose and under specific conditions.

7.10.4. Formal assurance techniques for CIS include:

(a) Evaluation as the independent examination, by the appropriate national or NATO authority, of the security aspects of a CIS. The evaluation determines whether the CIS satisfies its pre-defined security requirements;

(b) Security accreditation as the process which, supported by the results of an evaluation, determines that an adequate level of protection has been achieved and is being maintained for a CIS.

7.10.5. Assurance requirements for NATO CIS and other CIS handling NATO classified information shall be identified in the CIS Planning phase by the CISPIA, in conjunction with the SAA or designated NATO authority for NATO CIS handling non-classified information. This shall take into account the requirements set in the Enclosure “F” of the Policy on Security within the North Atlantic Treaty Organisation and supporting Directives, and, where applicable, an assessment of the security architecture and the outcome of the security risk management process.

7.10.6. Assurance requirements for cryptographic products or mechanisms shall be in accordance with the provisions of Enclosure “F” of the Policy on Security within the North Atlantic Treaty Organisation and relevant technical and implementation directives and supporting documents on CIS Security.

7.10.7. When evaluation and certification of products are required, the Common Criteria methodology (or national or international equivalent) shall, where appropriate[3], be used.

7.10.8. The use of security-enforcing hardware, firmware and software[4], which has been subject to a detailed design specification, should be limited to that designed and manufactured in NATO member nation(s). Where these are designed and/or manufactured in a non-NATO nation, they shall be subject to the approval of a NATO Nation.

7.10.9. For the procurement of general purpose security-related and security enforcing products, the NATO Information Assurance Products Catalogue should be consulted.

---

[3] Not applicable to cryptographic and TEMPEST products.

[4] Procurement requirements for cryptographic products or mechanisms are specifically defined in relevant Technical and Implementation directives developed by C3B.

DECLASSIFIED - PUBLICLY DISCLOSED - AC/35-D/2004-REV2-AS1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

7.10.10. Managing trustworthiness in the supply chain, through which CIS handling classified information and related components are acquired, requires also that NATO classified information disseminated to industry, generated as a result of a contract with industry, and classified contracts with industry shall be protected in accordance to the requirements set in Enclosure "F" of the Policy on Security within the North Atlantic Treaty Organisation and supporting directives.

7.11. Security design of CIS

7.11.1. Security models and security architectures shall be used to specify how the Policy on Security within the North Atlantic Treaty Organisation and supporting directives are enforced in NATO CIS and how the security objectives are achieved.

7.11.2. For CIS handling NATO classified information the indication of the security mode of operation shall be used to describe the security conditions under which the system operates.

7.11.3. Security Modes of Operation

7.11.3.1. NATO CIS handling information classified NATO CONFIDENTIAL and above, or Special Category information shall operate in one, or where warranted by requirements during different time periods, more than one, of the following security modes of operation:

(a) "dedicated" – a mode of operation in which all individuals with access to the CIS are cleared to the highest classification level of information handled within the CIS, and with a common need-to-know for all of the information handled within the CIS;

(b) "system high" - a mode of operation in which all individuals with access to the CIS are cleared to the highest classification level of information handled within the CIS, but not all individuals with access to the CIS have a common need-to-know for the information handled within the CIS; approval to access information may be granted at an informal or individual level;

(c) "compartmented" - a mode of operation in which all individuals with access to the CIS are cleared to the highest classification level of information handled within the CIS, but not all individuals with access to the CIS have a common need-to-know and formal authorisation[5] to access all of the information handled within the CIS;

(d) "multi-level" - a mode of operation in which not all individuals with access to the CIS are cleared to the highest classification level of information handled within the CIS, and not all individuals with access to the CIS have a common need-to-know for all of the handled within the CIS.

[5] Formal authorisation indicates that there is a formal central management of access control as distinct from an individual's discretion to grant access.

DECLASSIFIED - PUBLICLY DISCLOSED - AC/35-D/2004-REV2-AS1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

7.11.3.2. NATO CIS handling NATO RESTRICTED or below information shall operate in one, or where warranted by requirements during different time periods, more than one, of the following security modes of operation[6]:

(a) "dedicated" - a mode of operation in which all individuals with access to the CIS have a common need-to-know for all of the information handled within the CIS;

(b) "system high" - a mode of operation in which all individuals with access to the CIS do not have a common need-to-know for all of the information handled within the CIS;

(c) "compartmented" - a mode of operation in which all individuals with access to the CIS do not have a common need-to-know and formal authorisation to access all of the information handled within the CIS.

7.11.3.3. The Information Category Designation, US-Single Integrated Operation Plan (SIOP), shall only be processed in the "dedicated" security mode of operation.

7.12. Interconnection of CIS

7.12.1. Very often, in order to fulfil their mission, organisations require interconnecting their CIS to CIS of different organisations, communities of interest, security classifications and security postures. In order to safeguard the security principle of self-protecting CIS, it is necessary addressing the potential risks posed by interconnecting, directly or through a cascading interconnection, a CIS handling NATO information to another CIS and implementing specific security measures to control the interconnection.

7.12.2. For all interconnections of NATO CIS and other CIS handling NATO classified information, the following shall be subject to the approval of the SAA or designated NATO authority for NATO CIS handling non-classified information:

(a) the method of interconnection and services provided;

(b) where appropriate, the security risk assessment and risk management methodology to be utilised, and the results of the security risk assessment;

(c) the security architecture and security measures for ensuring the achievement of the security objectives;

(d) the security-related documentation, including the security test plan and the results of the security testing.

7.12.3. The supporting CIS Security Management directive sets out the specific security accreditation requirements and the supporting technical and implementation directives on CIS Security define the specific measures to be implemented.

---

[6] These interpretations of the modes of operation are included to show that a security clearance is not required for access to NATO RESTRICTED information.

DECLASSIFIED - PUBLICLY DISCLOSED - AC/35-D/2004-REV2-AS1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

7.12.4. The requirement for protective measures for CIS handling NATO information which are interconnected to Internet or similar networks in the public domain arises from the exceptional security risks posed by these types of public networks through their pervasive uncontrollable world-wide accessibility and the inherent susceptibility of their connectionless-oriented protocols and the vulnerabilities of the end CIS to exploitation. Especially CIS handling NATO classified information are at unacceptable security risk unless specifically protected.

7.12.5. The direct or cascaded interconnection to Internet or similar networks in the public domain of NATO CIS and other CIS handling NATO classified information up to and including NATO SECRET shall be:

(a) strictly controlled;

(b) be subject to the requirements of the SAA or designated NATO authority for NATO CIS handling non-classified information;

(c) be subject to evaluation and certification and/or approval of the security enforcing mechanisms as identified by relevant technical and implementation directives on CIS Security issued by C3B and by the SAA or designated NATO authority for NATO CIS handling non-classified information;

(d) be subject to periodic and formal vulnerability assessments.

7.12.6. The direct or cascaded interconnection of CIS handling information classified COSMIC TOP SECRET, and/or Special Category information, to Internet or similar networks in the public domain is prohibited.

7.12.7. **NATO information on Internet or similar networks in the public domain**

7.12.7.1. CIS handling NATO classified information may use the Internet or similar networks in the public domain purely as a bearer, provided that the appropriate cryptographic protection is implemented. In this instance, all security objectives shall be seriously considered.

7.12.7.2. The only information which may be transmitted in clear (i.e., non-encrypted) text is the following:

(a) open source and public information, or NATO information specifically approved for disclosure to the public; and

(b) non-sensitive NATO UNCLASSIFIED; i.e., information that, as determined by the originator(s), bears no additional administrative marking (for example, medical,) or dissemination limitation marking to indicate the sensitivity of the information.

7.12.7.3. Only open source and public information, or NATO information specifically approved for disclosure to the public, may be posted on publicly-accessible bulletin boards or web pages and shall be subject to the integrity requirements of the originator(s) of the information.

DECLASSIFIED - PUBLICLY DISCLOSED - AC/35-D/2004-REV2-AS1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

7.13. Application security

7.13.1. Security shall be embedded in the life-cycle (design, development, deployment, maintenance) of bespoke software purposely developed to handle NATO information, by taking into account the security objectives defined for the CIS.

7.13.2. Applications shall be subject to security testing, configuration management (e.g. baselines) and change control (e.g. patching), processes which shall be designed and managed by the CISP, in close coordination with the SAA or designated NATO authority for NATO CIS handling non-classified information, to ensure that the CIS Security objectives are properly taken into account.

7.13.3. On NATO CIS, CISPs shall maximise the use of automated tools to support application white listing and vulnerability detection.

7.14. Cryptographic security

7.14.1. The requirements relevant to cryptographic security are set in Enclosure “F” of the Policy on Security within the North Atlantic Treaty Organisation and in the related technical and implementation directives issued by C3B.

7.15. Emission security

7.15.1. The requirements relevant to emission security are set in Enclosure “F” of the Policy on Security within the North Atlantic Treaty Organisation and in the related technical and implementation directives issued by C3B.

7.16. Third party service delivery

7.16.1. For NATO CIS and other CIS handling NATO classified information, especially when outsourced, the CISP and the CISOA, in coordination with the SAA or designated NATO authority for NATO CIS handling non-classified information, shall formally agree (e.g. service level agreements, contracts) the requirements for implementation, management, monitoring and change management of CIS Security measures.

7.17. Security related logs

7.17.1. NATO CIS and other CIS handling NATO classified information shall be protected by security measures for the detection of malicious activities and faults, through the collection, review and storage of information for security related events.

DECLASSIFIED - PUBLICLY DISCLOSED - AC/35-D/2004-REV2-AS1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

7.17.2. Measures are required in order to provide sufficient information, including traceability of events, to be able to investigate a deliberate, accidental or attempted compromise of the security objectives of a CIS, commensurate with the damage that would be caused.

7.17.3. The requirements for collection of information for security related events shall also be defined by taking into account that security logs are fundamental to support the activity of security audit by SAAs.

7.17.4. The review and retention period for security logs shall be defined by the SAA or designated NATO authority for NATO CIS handling non-classified information, in coordination with the CISP and CISOA, based on a risk management approach which considers, among any other factor considered relevant by the authority responsible of the security accreditation, the following:

(a) security objectives of the CIS;

(b) threat environment;

(c) type of logs and data collected;

(d) frequency of log reviews;

(e) use of automated tools in support of log verification;

(f) investigative, audit and legal requirements.

7.18. Security baselines

7.18.1. On NATO CIS and other CIS handling NATO classified information, security baselines for CIS and critical hardware and software shall be defined, enforced and kept up-to-date through configuration management and change control during the entire CIS life-cycle.

7.18.2. Security baselines shall include security settings required to harden the configuration of critical components before deployment and requirements for security updates for components in operation.

7.18.3. On NATO CIS, CISPs shall maximize the use of automated tools for vulnerabilities discovery and remediation as well as produce implementation plans relevant to security baselines for the SAA's approval.

7.19. Malware defence

7.19.1. Although malicious software has always been recognised as a challenging threat, its evolution in sophistication and its ability to execute targeted attacks require high attention.

DECLASSIFIED - PUBLICLY DISCLOSED - AC/35-D/2004-REV2-AS1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

7.19.2. On NATO CIS and other CIS handling NATO classified information, dependent upon the security objectives of the CIS, malicious code detection solutions shall be utilised to block installation, prevent execution, quarantine malicious software and alert personnel responsible for incident response related activities.

7.20. Access control

7.20.1. Access control is a first line of defence as it allows the identification, authentication, authorisation and accountability of any entity (e.g. person, device, service) requesting access to a CIS and its elements.

7.20.2. On NATO CIS and other CIS handling NATO classified information, access control measures shall be implemented to prevent unauthorised operations on the CIS and related elements (e.g. data, devices, services).

7.20.3. In the selection of an access control model and its related security measures, CISPIA shall consider the following factors:

(a) the way and the extent to which an organisation implements information management may have an impact on the design of access control measures;

(b) technical measures shall be designed in the context of the overall security environment of a CIS to work in a coherent and coordinated manner with physical and administrative access control measures;

(c) technical measures shall enable secure and granular access to information based on the security mode of operation for which the CIS has been intended and on the validated requirements for the sharing of information among the communities of interests within the CIS and with other CIS.

7.20.4. Traditional network boundaries are a major element for the security design of a CIS infrastructure. However CISPIA shall also take into account that these boundaries cannot be considered an exhaustive point of reference when protecting NATO classified information handled in CIS with complex information sharing and access control requirements. This is typical of CIS such as those hosting communities of interest of different trust categories, federating with other CIS or implementing new concepts as in the case of cloud-computing.

7.20.5. Particularly in such scenarios, CISPIA shall adopt defence in-depth strategies which include security policies and measures specific for the protection of information objects based on the identity and other relevant attributes of the entity requesting access to the object as well as the properties of that object, commonly termed metadata labels.

7.20.6. Where access by non-NATO nationals to NATO CIS is authorised, measures shall be applied to restrict access only to the NATO classified information essential to NATO's mission. The appropriate NATO SAA shall exercise oversight of those measures,

DECLASSIFIED - PUBLICLY DISCLOSED - AC/35-D/2004-REV2-AS1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

including the review of the periodic reassessment of the security risks associated with access by non-NATO nationals to NATO CIS.

7.20.7. In the context of access control, Identity and Access Management (IAM) plays a fundamental role as it comprises of the people, processes and products necessary to manage digital identities (e.g. person, device, service and data), throughout their life-cycle, and the access to CIS resources.

7.20.8. For NATO CIS, access to CIS resources shall be managed through enterprise IAM capabilities that

(a) manage digital identities and their attributes, privileges and credentials;

(b) provide authentication services, including strong authentication, when indicated by risk management;

(c) prevent credential theft and reuse;

(d) provide granular authorization based on access policies;

(e) audit users and systems activities.

7.20.9. Minimum requirements for identification and authentication on NATO CIS and other CIS handling NATO classified information are set in the technical and implementation directives on CIS Security issued by C3B and shall, where appropriate, be determined as a result of a risk management process. Requirements for identification and authentication shall define the characteristics of the mechanisms and the extent to which these mechanisms shall be implemented and assured.

7.21. Incident response

7.21.1. A CIS Security incident is any detected anomaly compromising or that has the potential to compromise communication, information or other electronic systems or the information that is stored, processed or transmitted in these systems.

7.21.2. Technically oriented security management staff shall be designated and available to address security incidents.

7.21.3. Incidents related to CIS Security shall be reported for response, investigative and inspection purposes in accordance with the requirements of relevant CIS Security directives and of the SAA or designated NATO authority for NATO CIS handling non-classified information.

7.21.4. CIS Security related incidents affecting NATO CIS shall be notified to the NATO Computer Incident Response Capability (NCIRC) and/or the responsible CIS Security Officer, in compliance with the Internal Security Instructions (ISIs) or Security Operating Procedures (SecOPs) of NATO civil or military bodies and in accordance with the incident reporting formats and guidelines defined by the NCIRC and/or security investigative authorities.

DECLASSIFIED - PUBLICLY DISCLOSED - AC/35-D/2004-REV2-AS1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

7.21.5. The Directive on the Security of Information describes the conditions under which NOS shall be immediately notified that an incident has occurred for security investigative purposes and shall receive relevant reports. For NATO CIS, the Primary Directive on CIS Security extends these conditions to the following cases:

(a) Security breach involving COSMIC TOP SECRET, NATO SECRET and Special Category information

(b) Unauthorised disclosure of NATO classified information to media (e.g. press, blogs, websites) or other entities (e.g. political, terrorist and criminal groups);

(c) Unauthorised major data harvesting;

(d) Suspected espionage;

(e) Internal malicious activity (e.g. insider threat);

(f) Incidents involving privileged access to CIS;

(g) Incidents involving cryptographic elements;

(h) Incidents causing a significant impact to the organisation.

7.21.6. All other CIS Security incidents affecting NATO CIS and investigated by the relevant NATO security authorities shall be notified to NOS for oversight, analytical and statistical purposes.

7.21.7. Identification, collection, acquisition and preservation of potential digital evidence shall be undertaken by personnel trained in forensics procedures, in a systematic and impartial manner for preserving its integrity, authenticity and admissibility in accordance with relevant legal and policy requirements.

7.22. Security Management Infrastructure

7.22.1. Enclosure “F” of the Policy on Security within the North Atlantic Treaty Organisation requires that security management mechanisms and procedures shall be in place to deter, prevent, detect, withstand and recover from, the impact of incidents affecting NATO classified information and CIS. To this end, a Security Management Infrastructure (SMI) shall be established to ensure that the capabilities managing CIS Security related services, processes and devices across NATO bodies are managed as an enterprise.

7.23. CIS Security Training and Awareness

7.23.1. A major factor in achieving an adequate security posture of a CIS is an active security education and awareness programme for all CIS users.

7.23.2. Security education and awareness programme shall make users aware of the general threats and vulnerabilities applicable to the CIS they use, in order that they understand the rationale for, and acknowledge their responsibility to maintain,

DECLASSIFIED - PUBLICLY DISCLOSED - AC/35-D/2004-REV2-AS1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

the protective security measures in place. Special care shall be given to emergent and particular threats (e.g. targeted attacks, social engineering and insider threat) as these exploit the weaknesses of the human behaviours.

7.23.3. CIS Security education and awareness shall be provided to senior level management, CIS planning, implementing and operating staffs, security staffs and users to ensure that security responsibilities are clearly understood. To this end, minimum CIS security training standards for personnel shall be identified.

DECLASSIFIED - PUBLICLY DISCLOSED - AC/35-D/2004-REV2-AS1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

Appendix 1 - Roles and Responsibilities of NATO and national bodies involved in CIS Security

1. National authorities and agencies

(a) National Security Authorities (NSA);

(b) Designated Security Authorities (DSA);

(c) National Communication Security Authorities (NCSA);

(d) National Tempest Authorities (NTA);

(e) National Distribution Authorities (NDA);

(f) National Security Accreditation Authorities (SAA).

2. NATO bodies

2.1. Under the ultimate authority of the North Atlantic Council (NAC), NATO Committees and their sub-structures, Commands, Agencies and Staffs may be identified as follows:

(a) NATO bodies directly responsible for CIS Security policy, directives and guidance:

i. the Security Committee (SC) and the Security Committee in CIS Security Format (SC(CISS)) where National Security Authorities (NSAs) and Designated Security Authorities (DSAs) are represented;

ii. the C3 Board (C3B), and its Capability Panel on Information Assurance and Cyber Defence (CaP4);

iii. the Military Committee (NAMILCOM) for military requirements;

iv. various NATO civil committees for their civil requirements.

(b) NATO bodies indirectly concerned with CIS Security resources:

i. the financial committees, Senior Resource Board (SRB), the Resource Policy and Planning Board (RPPB), the Budget Committee (BC) and the Investment Committee (IC);

ii. the NATO Defence Manpower Committee for personnel aspects, in military establishments.

(c) NATO staff support in NATO Headquarters:

i. the NATO Office of Security (NOS);

ii. the NATO Headquarters C3 Staff (NHQC3S) and its Information Assurance and Cyber Defence Branch;

DECLASSIFIED - PUBLICLY DISCLOSED - AC/35-D/2004-REV2-AS1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

iii. the International Staff (IS), including the Emerging Security Challenges Division (ESC) and its Cyber Defence Section, and International Military Staff (IMS).

(d) NATO bodies representing the users:

i. Supreme Headquarters Allied Powers Europe (SHAPE) and HQ Supreme Allied Commander Transformation (SACT) for users in military establishments;

ii. specific civil agencies for civil users.

(e) NATO bodies responsible for operational and technical support to CIS Security policy, direction and implementation bodies:

i. Supreme Headquarters Allied Powers Europe (SHAPE) and HQ Supreme Allied Commander Transformation (SACT) for military establishments;

ii. the four nationally manned Military Committee agencies, for security evaluation of cryptographic products, vulnerability assessment of CIS, keying material distribution and accounting:

- Communications and Information Systems Security and Evaluation Agency (SECAN) - organised and staffed by the United States;
- Distribution and Accounting Agency (DACAN) - organised and staffed by the United States;
- European Communications Security and Evaluation Agency (EUSEC) - organised and staffed by the United Kingdom;
- European Distribution and Accounting Agency (EUDAC) - organised and staffed by the United Kingdom.

iii. the NATO Communications and Information Agency (NCI Agency) for the provision of communications and information systems and services;

iv. the NATO School (NSO) and the NATO CIS School (NCISS) for education and training;

v. the NATO Public Key Infrastructure (PKI) Management Authority (NPMA);

vi. the NATO CIS Security Accreditation Board (NSAB);

vii. the NATO Cyber Defence Management Board (CDMB).

2.2. Security responsibilities

2.2.1. The security responsibilities of the Security Committee (SC), the NATO Office of Security (NOS), the NATO Military Committee (NAMILCOM) and NATO Military bodies, the C3 Board (C3B), NATO Civil bodies, National Security Authorities (NSAs) and

DECLASSIFIED - PUBLICLY DISCLOSED - AC/35-D/2004-REV2-AS1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

Designated Security Authorities (DSAs) are addressed in the Policy on Security within the North Atlantic Treaty Organisation. The responsibilities of NATO committees, NATO Civil and Military bodies, and National bodies with NATO CIS Security responsibilities are addressed in the appropriate NATO and National documents, including official Terms of Reference (TORs).

DECLASSIFIED - PUBLICLY DISCLOSED - AC/35-D/2004-REV2-AS1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

Appendix 2 - CIS Security-related Activities in the CIS Life Cycle

1. Introduction

1.1. This section addresses the essential activities related to CIS Security, and their associated responsible authorities and staffs, which shall be undertaken during the life-cycle of NATO CIS and other CIS handling NATO classified information. These activities are based upon the requirements established in more detail in the supporting directives. The following generic stages of the CIS life-cycle are identified, which may be adapted according to NATO and national requirements:

(a) CIS planning;

(b) CIS development and procurement;

(c) CIS implementation and security accreditation;

(d) CIS operation

(e) CIS enhancement;

(f) CIS withdrawal from service, and disposal of equipment.

1.2. The activities related to CIS Security highlight the context in which the Policy on Security within the North Atlantic Treaty Organisation and its supporting directives and guidance on management as well as technical and implementation aspects are to be utilised, in order to assess the security accreditation, and implementation requirements.

DECLASSIFIED - PUBLICLY DISCLOSED - AC/35-D/2004-REV2-AS1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

2. **CIS Planning**

2.1. The following activities related to CIS Security and responsible authorities are associated with the planning stage of a CIS:

Activity	Responsible Authority / Staffs
1. Identify and notify the appropriate SAA, or designated NATO authority for NATO CIS handling non-classified information[7], of CIS plans	CISPIA
2. Establish or identify a CIS security framework necessary to meet security objectives of the CIS in questions and identify the tasks related to CIS Security	CISPIA, coordinating with CISP and SAA
3. Establish the basis for security accreditation through the development of a security accreditation plan or security accreditation strategy	CISPIA in close coordination with SAA
4. Approve the security accreditation plan or security accreditation strategy	SAA
5. For NATO CIS, identify the security risk assessment requirement and the security risk assessment and management methodology to be utilised	SAA, coordinating with CISPIA
6. For NATO CIS, undertake an initial security risk assessment in accordance with the requirements of the SAA	CISPIA in conjunction with CIS operational authority (CISOA), coordinating with the SAA

[7] For readability reason, from now on the term SAA is utilised to refer as well to the designated NATO authority for NATO CIS handling non-classified information, unless differently indicated.

DECLASSIFIED - PUBLICLY DISCLOSED - AC/35-D/2004-REV2-AS1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

Activity	Responsible Authority / Staffs
7. For NATO CIS, develop an initial security architecture based on the mission objectives and the findings of the initial security risk assessment	CISPIA in conjunction with CISOA, coordinating with SAA
8. For NATO CIS, approve the results of the initial security risk assessment	SAA, in coordination with CISOA
9. Identify initial requirement for products requiring evaluation and certification and/or approval (e.g. cryptographic products) and identify supply chain security requirements	CISPIA and, where appropriate, coordinating with SAA For NATO CIS this may require coordination also with C3B and its substructure
10. Identify initial requirement for security baselines, configuration management and change control	CISPIA, coordinating with the CISP and appropriate SAA
11. Identify initial requirement for training and awareness	CISPIA, coordinating with the appropriate SAA
12. Identify initial requirement for business continuity	CISPIA, in conjunction with the CISOA and in coordination with the SAA
13. Identify initial requirement for security logs retention	CISPIA, in conjunction with CISOA, CISP and SAA
14. Develop the initial Security Requirement Statements (SRS(s)) (or national equivalent(s)), or, where appropriate for NATO CIS, address the required CIS Security aspects of Capability Packages (CPs) and associated documents; using, where appropriate, applicable Protection Profiles (e.g. collaborative PP)	CISPIA, coordinating with SAA

DECLASSIFIED - PUBLICLY DISCLOSED - AC/35-D/2004-REV2-AS1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

Activity	Responsible Authority / Staffs
15. Approve the initial SRS(s) (or national equivalent(s)) or, where appropriate for NATO CIS, approve the required CIS Security aspects of Capability Packages (CPs) and associated documents	SAA

DECLASSIFIED - PUBLICLY DISCLOSED - AC/35-D/2004-REV2-AS1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

3. **CIS Development and Procurement**

3.1. The following activities related to CIS Security and responsible authorities are associated with the development and procurement stage of a CIS:

Activity	Responsible Authority / Staffs
1. For NATO CIS, refine the security risk assessment	CISPIA, in conjunction with SAA
2. Develop the security architecture and check it against reference security architecture(s) to ensure, where possible, security interoperability and integration of new CIS in existing infrastructure(s)	CISPIA
3. For NATO CIS, approve the results of the refined security risk assessment	SAA, in coordination with CISOA
4. Approve the security architecture	SAA
5. Develop a detailed specification of security measures covering personnel, physical, and security of information aspects	CISPIA, coordinating with CISP, site Security Authority, and SAA
6. Develop a detailed specification of CIS Security measures, in accordance with the requirements of the SAA, addressing security functionality and assurance and, where appropriate, the interconnection of CIS.	CISPIA, coordinating with CISP and SAA
7. Refine requirement for products requiring evaluation and certification and/or approval and security requirements for supply chain	CISPIA and, where appropriate, coordinating with appropriate SAA For NATO CIS this may require coordination also with C3B and its substructure

DECLASSIFIED - PUBLICLY DISCLOSED - AC/35-D/2004-REV2-AS1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

Activity	Responsible Authority / Staffs
8. Refine requirement for security baselines, configuration management and change control	CISPIA, in conjunction with the CISP and in coordination with appropriate SAA
9. Refine requirement for training and awareness	CISPIA, in coordination with the appropriate SAA
10. Refine requirement for business continuity	CISPIA, in conjunction with the CISOA and coordinating with appropriate SAA
11. Refine requirement for security logs retention	CISPIA, in conjunction with CISOA, CISP and SAA
12. Approve requirement for security baselines, configuration management and change control	SAA
13. Approve requirement for training and awareness	CISOA, in coordination with appropriate SAA
14. Approve requirement for business continuity	CISOA, in coordination with appropriate SAA
15. Approve requirement for security logs retention	SAA, in coordination with the CISOA
16. Approve security requirements for assured products and supply chain	SAA and, where appropriate, C3B

DECLASSIFIED - PUBLICLY DISCLOSED - AC/35-D/2004-REV2-AS1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

Activity	Responsible Authority / Staffs
17. Review CIS Security products lists for assured products which can meet the CIS security requirement(s) (e.g. NATO Information Assurance Product Catalogue)	CISPIA, coordinating with CISP and SAA
18. Where appropriate, develop the operational requirements for cryptographic products and mechanisms using, where appropriate, applicable protection profiles. For NATO CIS under NATO common funding, notify C3B and its substructure of requirements	CISPIA, coordinating with the CISP and SAA
19. Where appropriate, for NATO CIS under NATO common funding, develop the technical characteristics for cryptographic products and mechanisms	C3B and its substructure
20. Where appropriate, advise NCSAs, through C3B, of the requirement for cryptographic products and mechanisms	CISPIA
21. Where appropriate, establish an evaluation / selection timetable for cryptographic products and mechanisms	Supporting staffs of C3B and its substructure, coordinating with the NCSAs, SECAN, CISPIA, and CISP
22. Where appropriate, undertake evaluation, approval and selection of cryptographic products and mechanisms.	Supporting staffs of C3B and its substructure (supported by NCI Agency), in conjunction with SECAN, with approval by NAMILCOM
23. Establish requirement for Security Test and Verification (ST&V) of the CIS or, where appropriate, of the interconnection of CIS	SAA, coordinating with CISPIA.

DECLASSIFIED - PUBLICLY DISCLOSED - AC/35-D/2004-REV2-AS1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

Activity	Responsible Authority / Staffs
24. For NATO CIS, ensure that the Type “B” Cost Estimate (TBCE) identifies any requirement for all CIS Security related activities, including security accreditation and assurance activities (e.g. evaluation, certification, approval) in order to establish the appropriate funding	CISPIA, coordinating with SAA
25. On-going development of the SRS(s) (or national equivalent(s)); using, where appropriate, applicable Protection Profiles	CISPIA, coordinating with SAA
26. On-going approval of the SRS(s) (or national equivalent(s))	SAA
27. Ensure that the Service Level Agreement (SLA), established between the CISP and the CISOA for the provision of CIS services, addresses, as a minimum, the requirements for implementation and management of security measures as well as for monitoring and change management.	CISPIA, coordinating with SAA

DECLASSIFIED - PUBLICLY DISCLOSED - AC/35-D/2004-REV2-AS1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

4. **CIS Implementation and Security Accreditation**

4.1. The following activities related to CIS Security and responsible authorities are associated with the implementation and security accreditation stage of a CIS:

Activity	Responsible Authority / Staffs
1. Refine Security Test and Verification (ST&V) requirements of the CIS or, where appropriate, the interconnection of CIS	SAA, coordinating with CISPIA and CISP
2. Develop Security Test and Verification (ST&V) plan	CISPIA, coordinating with CISP and SAA
3. Undertake, where required, all activities necessary to obtain assured products, in accordance with, where appropriate, the evaluation methodologies approved by C3B or nationally or internationally equivalent methodologies	NATO or National[8] Authority responsible for evaluation, certification and/or approval of products, coordinating with the CISPIACISP
4. Undertake security testing, in accordance with an agreed ST&V plan	CISP, coordinating with the CISPIA and SAA
5. Review results of security testing	SAA
6. Identify any additional security countermeasures to be implemented if the result of the security testing is not satisfactory	CISPIA, coordinating with CISP and SAA
7. For NATO CIS, identify and agree the residual risks to be accepted	CISOA

[8] As determined by the National Security Authority.

DECLASSIFIED - PUBLICLY DISCLOSED - AC/35-D/2004-REV2-AS1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

Activity	Responsible Authority / Staffs
8. For NATO CIS, identify and agree the on-going security risk management processes	SAA, in conjunction with CISOA
9. Complete the SRS(s) (or national equivalent(s))	CISPIA, coordinating with SAA
10. Approve the SLA, established between the CISP and the CISOA for the provision of CIS services	CISOA and CISP
11. Formulate the Security Operating Procedures (SecOPs) (or national equivalent(s)) for the CIS	CISP, coordinating with security management staffs[9]
12. Approve the SRS(s) and SecOPs (or national equivalent(s))	SAA
13. Provide initial training and awareness	CISPIA or CISOA or CISP as appropriate
14. Accredit the CIS or, where appropriate, the interconnection of CIS and issue an accreditation statement which includes the period of validity of the accreditation	SAA
15. Establish the re-accreditation conditions	SAA

[9] Security Officer, CIS Security Officer, System and Network Administrator.

DECLASSIFIED - PUBLICLY DISCLOSED - AC/35-D/2004-REV2-AS1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

5. **CIS Operation**

5.1. The following activities related to CIS Security and responsible authorities are associated with the operation stage of a CIS:

Activity	Responsible Authority / Staffs
1. Authorise CIS to operate	CISOA
2. Store, process or transmit NATO information in the operational environment in accordance with the approved SecOPs (or national equivalent(s)), including system and security administration and in accordance to the specific service requirements included in relevant SLAs	CISP, coordinating with security management staffs
3. Maintain security baselines through configuration management and change control	CISP, in coordination with SAA
4. For NATO CIS, perform on-going security risk management, in accordance with the requirements of the SAA. This includes reporting to senior management and the SAA on changes in the risk posture due to evolving threats and vulnerabilities as well as to changes of the CIS status (e.g. value, configuration, compliance to security baselines, physical and personnel security measures).	CISOA, coordinating with CISP and SAA

DECLASSIFIED - PUBLICLY DISCLOSED - AC/35-D/2004-REV2-AS1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

Activity	Responsible Authority / Staffs
5. Detect, react to and report on CIS Security incidents, in accordance with the requirements of relevant NATO security policies and directives, the SecOPs (or national equivalent(s)) and with relevant procedures established by the Cyber Defence Management Board and/or security investigative authorities.	CISOA and CISP, coordinating with SAA
6. Provide regular training and awareness	CISOA or CISP as appropriate
7. Undertake, in accordance with the requirements of the SAA, periodic vulnerability assessments and, on NATO CIS, maximise the use of automated tools to continuously assess CIS compliance to security baselines.	CISP or a separately established vulnerability assessment team, coordinating with SAA and CISOA
8. Undertake, in accordance with NATO security policy, periodic security audits of the CIS or, where appropriate, the interconnection of CIS	SAA, coordinating with CISOA and CISP

DECLASSIFIED - PUBLICLY DISCLOSED - AC/35-D/2004-REV2-AS1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

6. **CIS Enhancement**

6.1. The following activities related to CIS Security and responsible authorities are associated with the enhancement stage of a CIS:

Activity	Responsible Authority / Staffs
1. Undertake, where required by an update of an assured product, all activities necessary to obtain re-assurance (e.g. evaluation, certification and approval) for the new product, in accordance with, where appropriate, the evaluation methodologies approved by C3B or nationally or internationally equivalent methodologies	NATO or National[10] Authority responsible for evaluation, certification and/or approval of products, coordinating with CISPIA, CISP and SAA
2. For NATO CIS, refine the security risk assessment	CISPIA, in conjunction with the CISOA, CISP and SAA
3. Revise the security architecture and check it against reference security architecture(s) to ensure, where possible, security interoperability and integration of new CIS in existing infrastructure(s)	CISPIA
4. For NATO CIS, approve the results of the refined security risk assessment	SAA, in coordination with CISOA
5. Re-approve the security architecture	SAA
6. Identify any required changes to security countermeasures.	CISPIA, in conjunction with CISP and SAA
7. Identify required changes to training and awareness	CISPIA or CISOA or CISP as appropriate

[10] As determined by the National Security Authority.

DECLASSIFIED - PUBLICLY DISCLOSED - AC/35-D/2004-REV2-AS1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

Activity	Responsible Authority / Staffs
8. Identify required changes to business continuity requirements	CISOA in coordination with appropriate SAA
9. Identify required changes to security logs retention requirements	CISPIA, in conjunction with CISOA, CISP and SAA
10. Establish requirement for ST&V of the CIS or, where appropriate, of the interconnection of CIS	SAA, coordinating with CISPIA and CISP
11. Develop ST&V plan	CISPIA, coordinating with CISP and SAA
12. Undertake security testing, in accordance with an agreed ST&V plan	CISP, coordinating with CISPIA and SAA
13. Review results of security testing	SAA
14. Identify, as a result of the security testing, any additional security countermeasures to be implemented	CISPIA, coordinating with SAA and CISP
15. For NATO CIS, review and agree the residual risks to be accepted	CISOA
16. For NATO CIS, review and agree the on-going security risk management processes	SAA, in conjunction with CISOA
17. Revise the SRS(s) (or national equivalent(s)); using, where appropriate, applicable Protection Profiles	CISP, coordinating with SAA

DECLASSIFIED - PUBLICLY DISCLOSED - AC/35-D/2004-REV2-AS1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

Activity	Responsible Authority / Staffs
18. Revise the SecOPs (or national equivalent(s)) for the CIS	CISP, coordinating with the security management staffs and SAA
19. Re-approve the SRS(s) and SecOPs (or national equivalent(s))	SAA
20. Re-accredit the CIS or, where appropriate, the interconnection of CIS; and re-publish an accreditation statement	SAA
21. Review and re-establish the re-accreditation conditions	SAA

DECLASSIFIED - PUBLICLY DISCLOSED - AC/35-D/2004-REV2-AS1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

7. **CIS Withdrawal from Service and Disposal of Equipment**

7.1. The following activities related to CIS Security and responsible authorities are associated with the withdrawal from service, and disposal of equipment stage of a CIS:

Activity	Responsible Authority / Staffs
1. Identify items that require archiving and/or de-classification and/or disposal and/or destruction and related requirements	CISOA and/or CISP
2. Initiate the appropriate archiving or de-classification and destruction of associated fixed and removable computer storage media, and information required for accounting purposes	CISOA and/or CISP
3. Initiate the appropriate procedures for the disposal and/or destruction of special purpose equipment including cryptographic products and systems and their associated material	CISOA and/or CISP
4. Initiate the appropriate archiving or destruction of associated hard copy documentation	CISOA and/or CISP

DECLASSIFIED - PUBLICLY DISCLOSED - AC/35-D/2004-REV2-AS1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

Appendix 3 - NATO CIS Security Documentation Structure

1. This “Primary Directive on CIS Security” is supported by a number of CIS Security directives and guidance documents addressing CIS Security management, and CIS Security technical and implementation aspects. A "Roadmap" to the Policy on Security within the North Atlantic Treaty Organisation, supporting directives, supporting documents and guidance documents is published by the NATO Office of Security and the NATO HQ C3 Staff respectively on behalf of SC and the C3B. The Roadmap may also be accessed on the NATO SECRET Wide Area Network (WAN) at the NOS portion of the NATO HQ web site.

2. The "Roadmap" provides access to the following :

(a) NATO UNCLASSIFIED and NATO RESTRICTED documents published by the NAC, DPPC, the SC and the C3B, with respect to information management, security and cyber defence;

(b) contact information of NATO and National Security Authorities.

DECLASSIFIED/DECLASSIFIEE - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

17 June 2002

INCLUDING COR 1 TO 12

DOCUMENT
C-M(2002)49

SECURITY WITHIN THE NORTH ATLANTIC TREATY ORGANISATION (NATO)

Note by the Secretary General

Reference: C-M(2002)23 and its Action Sheet

1. This document is the result of a Fundamental Review by the NATO Security Committee (NSC) and it was approved by Council under the silence procedure on 26th March 2002 (reference refers).

2. This present document, in conjunction with C-M(2002)50, "Protection Measures for NATO Civil and Military Bodies, deployed NATO Forces and Installations (Assets) against Terrorist Threats", supersedes C-M(55)15(Final). With the exception of Enclosure "A", the "Security Agreement by the Parties to the North Atlantic Treaty" which is still valid for those nations which have not yet ratified the "Agreement between the Parties to the North Atlantic Treaty for the Security of Information", all previous versions of C-M(55)15(Final) should now be destroyed.

3. The following Directives support this present document:

AC/35-D/2000	Directive on Personnel Security
AC/35-D/2001	Directive on Physical Security
AC/35-D/2002	Directive on Security of Information
AC/35-D/2003	Directive on Industrial Security
AC/35-D/2004	Primary Directive on INFOSEC
AC/35-D/2005	INFOSEC Management Directive for CIS

(The first four directives (AC/35-D/2000-2003) were approved by Council (reference refers) and the remaining two AC/35-D/2004 and D/2005) were approved by the NATO Security Committee (NSC) and the NATO C3 Board.

4. For ease of reference, a compendium, containing the two security policy documents (C-M(2002)49 and C-M(2002)50) and the above-mentioned supporting directives, will be distributed in the near future to all current holders of C-M(55)15(Final).

(Signed) George Robertson

Original: English

NHQD15853
No.1127448
HQ . NATO . IS . CENTRAL . DMS PRODUCTION LIBRARY

DECLASSIFIED/DECLASSIFIEE - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

RECORD OF AMENDEMENTS

Strike out corresponding number
as each amemdment is inserted

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50

DECLASSIFIED/DECLASSIFIEE - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

TABLE OF CONTENTS

Note by the Secretary General

Record of Amendements

Table of Contents

Enclosure "A" - Security Agreement

Enclosure "B" - Basic Principles of Security

Enclosure "C" - Personnel Security

Enclosure "D" - Physical Security

Enclosure "E" - Security of Information

Enclosure "F" - ~~INFOSEC~~ - CIS Security (COR.9; COR.11)

Enclosure "G" - ~~Industrial Security~~ CLASSIFIED PROJECT AND INDUSTRIAL SECURITY (COR.12)

Glossary

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2010)0003-ADD1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

ENCLOSURE "A"

AGREEMENT BETWEEN THE PARTIES TO THE NORTH ATLANTIC TREATY FOR THE SECURITY OF INFORMATION

The Parties to the North Atlantic Treaty, signed at Washington on 4th April, 1949.

Reaffirming that effective political consultation, cooperation and planning for defence in achieving the objectives of the Treaty entail the exchange of classified information among the Parties.

Considering that provisions between the Governments of the Parties to the North Atlantic Treaty for the mutual protection and safeguarding of the classified information they may interchange are necessary.

Realising that a general framework for security standards and procedures is required.

Acting on their own behalf and on behalf of the North Atlantic Treaty Organization, have agreed as follows:

ARTICLE 1

The Parties shall:

(i) protect and safeguard:

(a) classified information (see ANNEX 1), marked as such, which is originated by NATO (see ANNEX 2) or which is submitted to NATO by a member state;

(b) classified information, marked as such, of the member states submitted to another member state in support of a NATO programme, project, or contract,

(ii) maintain the security classification of information as defined under (i) above and make every effort to safeguard it accordingly;

(iii) not use classified information as defined under (i) above for purposes other than those laid down in the North Atlantic Treaty and the decisions and resolutions pertaining to that Treaty;

(iv) not disclose such information as defined under (i) above to non-NATO Parties without the consent of the originator.

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2010)0003-ADD1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

ARTICLE 2

Pursuant to Article 1 of this Agreement, the Parties shall ensure the establishment of a National Security Authority for NATO activities which shall implement protective security measures. The Parties shall establish and implement security standards which shall ensure a common degree of protection for classified information.

ARTICLE 3

(1) The Parties shall ensure that all persons of their respective nationality who, in the conduct of their official duties, require or may have access to information classified CONFIDENTIAL and above are appropriately cleared before they take up their duties.

(2) Security clearance procedures shall be designed to determine whether an individual can, taking into account his or her loyalty and trustworthiness, have access to classified information without constituting an unacceptable risk to security.

(3) Upon request, each of the Parties shall cooperate with the other Parties in carrying out their respective security clearance procedures.

ARTICLE 4

The Secretary General shall ensure that the relevant provisions of this Agreement are applied by NATO (see ANNEX 3).

ARTICLE 5

The present Agreement in no way prevents the Parties from making other Agreements relating to the exchange of classified information originated by them and not affecting the scope of the present Agreement.

ARTICLE 6

(a) This Agreement shall be open for signature by the Parties to the North Atlantic Treaty and shall be subject to ratification, acceptance or approval. The instruments of ratification, acceptance or approval shall be deposited with the Government of the United States of America;

(b) this Agreement shall enter into force thirty days after the date of deposit by two signatory States of their instruments of ratification, acceptance or approval. It shall enter into force for each other signatory State thirty days after the deposit of its instrument of ratification, acceptance or approval;

(c) this Agreement shall with respect to the Parties for which it entered into force supersede the "Security Agreement by the Parties to the North Atlantic Treaty Organization" approved by the North Atlantic Council in Annex A (paragraph 1) to Appendix to Enclosure to D.C. 2/7, on 19th April, 1952, and subsequently incorporated in Enclosure "A" (paragraph 1) to C-M(55)15(Final), approved by the North Atlantic Council on 2nd March, 1955.

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2010)0003-ADD1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

ARTICLE 7

This Agreement shall remain open for accession by any new Party to the North Atlantic Treaty, in accordance with its own constitutional procedures. Its instrument of accession shall be deposited with the government of the United States of America. It shall enter into force in respect of each acceding State thirty days after the day of the deposit of its instrument of accession.

ARTICLE 8

The Government of the United States of America shall inform the Governments of the other Parties of the deposit of each instrument of ratification, acceptance, approval or accession.

ARTICLE 9

This Agreement may be denounced by written notice of denunciation by any Party given to the depository which shall inform all the other Parties of such notice. Such denunciation shall take effect one year after receipt of notification by the depository, but shall not affect obligations already contracted and the rights or prerogatives previously acquired by the Parties under the provisions of this Agreement.

In witness whereof the undersigned, duly authorized to this effect by their respective Governments, have signed this Agreement.

Done in Brussels, this ..... day of ..... xxxx in a single copy in the English and French languages, each text being equally authoritative, which shall be deposited in the archives of the Government of the United States of America and of which certified copies shall be transmitted by that Government to each of the other signatories.

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2010)0003-ADD1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

ANNEX 1

This Annex forms an integral part of the Agreement.

NATO classified information is defined as follows:

(a) information means knowledge that can be communicated in any form;

(b) classified information means information or material determined to require protection against unauthorized disclosure which has been so designated by security classification;

(c) the word "material" includes documents and also any item of machinery or equipment or weapons either manufactured or in the process of manufacture;

(d) the word "document" means any recorded information regardless of its physical form or characteristics, including, without limitation, written or printed matter, data processing cards and tapes, maps, charts, photographs, paintings, drawings, engravings, sketches, working notes and papers, carbon copies and ink ribbons, or reproductions by an means or process, and sound, voice, magnetic or electronic or optical or video recordings in any form, and portable ADP equipment with resident computer storage media, and removable computer storage media.

ANNEX 2

This Annex forms an integral part of the Agreement.

For the purposes of the present Agreement, the term "NATO" denotes the North Atlantic Treaty Organization and the bodies governed either by the Agreement on the status of the North Atlantic Treaty Organization, National Representatives and International Staff, signed in Ottawa on 20th September, 1951 or by the Protocol on the status of International Military Headquarters set up pursuant to the North Atlantic Treaty, signed in Paris on 28th August, 1952.

ANNEX 3

This Annex forms an integral part of the Agreement.

Consultation takes place with military commanders in order to respect their prerogatives.

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2010)0003-ADD1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

ENCLOSURE "B"

BASIC PRINCIPLES AND MINIMUM STANDARDS OF SECURITY

1. INTRODUCTION

1.1. This C-M establishes the basic principles and minimum standards of security to be applied by NATO nations and NATO civil and military bodies in order to ensure that a common degree of protection is given to classified information exchanged among the parties. NATO security procedures only operate to the best advantage when they are based upon and supported by a national security system having the characteristics set out in this Enclosure. This Enclosure also addresses security responsibilities in NATO.

2. AIMS AND OBJECTIVES

2.1. NATO nations and NATO civil and military bodies shall ensure that the basic principles and minimum standards of security set forth in this C-M are applied to safeguard classified information from loss of confidentiality, integrity and availability.

2.2. NATO nations and NATO civil and military bodies shall establish security programmes that meet these basic principles and minimum standards to ensure a common degree of protection for classified information.

3. APPLICABILITY

3.1. These basic principles and minimum standards shall be applied to:

(a) classified information originated by NATO, originated by a member nation and submitted to NATO or submitted by a member nation to another member nation in support of a NATO programme, project or contract;

(b) classified information received by NATO from non-NATO sources; and

(c) classified information entrusted to individuals and organisations outside a government (or a NATO civil or military body), e.g., consultants, industry, universities, which shall protect it according to the same standards applied by the government or NATO civil or military body.

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2010)0003-ADD1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

3.2. Access to, and the protection of, ATOMAL information are subject to the Agreement between the Parties to the North Atlantic Treaty for Co-operation regarding Atomic Information - C-M(64)39. The Administrative Arrangements to implement the Agreement between the Parties to the North Atlantic Treaty for Co-operation regarding ATOMAL Information - the current version of C-M(68)41 - shall be applied to control access to, to handle and protect such information.

3.3. Access to, and protection of, US-SIOP information are subject to the provisions of C-M(71)27(Revised), "Special Procedures for the Handling of United States Single Integrated Operational Plan (US-SIOP) Information within NATO".

3.4. The sensitive nature of cryptographic information, measures, and products requires the application of stringent security precautions, often beyond those set forth in this C-M. Therefore, access to, and protection of, cryptographic information, measures and products that are nationally - or NAMILCOM - approved, shall be in accordance with Enclosure "F", supporting directives and procedures established by the appropriate authority.

3.5. The sensitive nature of Signals Intelligence (SIGINT) information, operations, sources and methods require the application of stringent security regulations and procedures often beyond those set forth in this C-M. Therefore, access to and protection of, SIGINT information, operations, sources and methods are subject to national regulations and the provisions laid down in MC 101 (NATO Signals Intelligence Policy) and its companion Allied Joint Publication (AJP).

4. AUTHORITY

4.1. The North Atlantic Council (NAC) has approved this document which implements the Agreement Between the Parties to the North Atlantic Treaty for the Security of Information (reproduced at Enclosure "A"), and thereby establishes NATO Security Policy.

5. BASIC PRINCIPLES

5.1. The following basic principles shall apply:

(a) NATO nations and NATO civil and military bodies shall ensure that the agreed minimum standards set forth in this C-M are applied to ensure a common degree of protection for classified information exchanged among the parties;

(b) classified information shall be disseminated solely on the basis of the principle of need-to-know to individuals who have been briefed on the relevant security procedures; in addition, only security cleared individuals shall have access to information classified CONFIDENTIAL and above;

(c) security risk management shall be mandatory within NATO civil and military bodies. Its application within NATO nations shall be optional;

(d) classified information shall be safeguarded by a balanced set of security measures, including personnel security, physical security, security of information, Communication and Information System Security (CIS Security), which shall extend to all individuals having access to classified information, all media-carrying information, and to all premises containing such information;

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2010)0003-ADD1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

(e) Coordinating the management of the Insider Threat with the appropriate national authorities and NATO Civil and Military Bodies;

(f) NATO Nations and NATO Civil and Military Bodies shall establish Security Awareness and Training Programmes related to all security aspects as described in paragraph 5.1 (d) above;

(g) all suspected breaches of security shall be reported immediately to the appropriate security authority. Reports shall be evaluated by appropriate officials to assess the resulting damage to NATO and to take appropriate action. Enclosure "E" provides details;

(h) originators release classified information to NATO and to NATO nations in support of a NATO programme, project or contract on the understanding that it will be managed and protected in accordance with the NATO Information Management Policy (NIMP) and NATO Security Policy;

(i) classified information shall be subject to originator control;

(j) the release of classified information shall be in accordance with the requirements of Enclosure "E" to this C-M, and supporting directives; and

(k) subject to the consent of the originator and in accordance with Enclosure "E" to this C-M, NATO classified information shall only be released to non-NATO nations and organisations that have either signed a Security Agreement with NATO or that have provided a Security Assurance to NATO, either directly or through the NATO nation or NATO civil or military body sponsoring the release. In all cases, a degree of protection, no less stringent than that specified in this C-M, shall be required for any NATO classified information released.

5.2. The foundations of sound national security are:

(a) a security organisation responsible for:

(i) the collection and recording of intelligence information regarding espionage, terrorist, sabotage and subversive threats; and

(ii) the centralisation of such information so that it can be applied to any situation relating to the employment of individuals in government departments and agencies and by contractors; and

(iii) the provision of information and advice to governments on the nature of the threats to security and the means of protection against them; and

(b) the regular collaboration among government departments and agencies to:

(i) identify classified information that needs to be protected; and

(ii) establish and apply common degrees of protection as set forth in this C-M.

5.3. Personnel Security

5.3.1. Personnel security procedures shall be designed to assess whether an individual can, taking into account his loyalty, trustworthiness and reliability, be authorised to have initial and continued access to classified information without constituting an unacceptable risk to security. All individuals,

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2010)0003-ADD1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

civilian and military, who require access to, or whose duties or functions may afford access to information classified CONFIDENTIAL or above, shall be appropriately cleared and briefed before such access is authorised. Individuals shall only have access to NATO classified information for which they have a need-to-know.

5.3.2. A security clearance is not required for access to RESTRICTED information; individuals shall be briefed about their responsibilities for the protection of RESTRICTED information.

5.3.3. Personnel security is addressed further at Enclosure "C" of this C-M and in the supporting personnel security directive.

5.4. Physical Security

5.4.1. Physical security is the application of physical protective measures to sites, buildings or facilities that contain information requiring protection against loss or compromise. Physical security programmes, consisting of active and passive security measures, shall be established to provide levels of physical security consistent with the threat, security classification and quantity of the information to be protected.

5.4.2. Physical security is addressed further at Enclosure "D" of this C-M and in the supporting physical security directive.

5.5. Security of Information

5.5.1. Security of information is the application of general protective measures and procedures to prevent, detect and recover from the loss or compromise of information. Classified information shall be protected throughout its life cycle to a level commensurate with its level of classification. It shall be managed to ensure that it is appropriately classified, is clearly identified as classified and remains classified only as long as this is necessary.

5.5.2. Security classifications shall be applied to information to indicate the possible damage to the security of NATO and/or its member nations if the information is subjected to unauthorised disclosure. NATO security classifications shall be applied in accordance with Enclosure "E" to this C-M. It is the prerogative of the originator of the information to determine or modify the security classification.

5.5.3. NATO security classifications and their significance are:

(a) COSMIC TOP SECRET (CTS):
unauthorised disclosure would result in exceptionally grave damage to NATO;

(b) NATO SECRET (NS):
unauthorised disclosure would result in grave damage to NATO;

(c) NATO CONFIDENTIAL (NC):
unauthorised disclosure would be damaging to NATO; and

(d) NATO RESTRICTED (NR):
unauthorised disclosure would be detrimental to the interests or effectiveness of NATO.

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2010)0003-ADD1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

5.5.4. When classifying information, the originator shall take account of the damage if the information is subjected to unauthorised disclosure, and shall indicate, where possible, whether their information can be downgraded or declassified on a certain date or event.

5.5.5. NATO UNCLASSIFIED information - policy and procedures for the management and protection of non-classified information marked NATO UNCLASSIFIED are contained in the NATO Information Management Policy (NIMP).

5.5.6. Security of Information is addressed further at Enclosure "E" of this C-M and in the supporting security of information directive.

5.5.7. The planning, preparation, execution and support relating to NATO Operations, Training, Exercises, Transformation and Cooperation (OTETC) may require specific additional security aspects to be addressed; the Supporting Document on Information and Intelligence Sharing with Non-NATO Entities (NNEs) contains security provisions and guidance applicable in these circumstances.

5.6. CIS Security

5.6.1. CIS Security is the application of security measures for the protection of communication, information and other electronic systems, and the information that is stored, processed or transmitted in these systems with respect to confidentiality, integrity, availability, authentication and non-repudiation.

5.6.2. In order to achieve the security objectives of confidentiality, integrity, availability, authentication and non-repudiation a balanced set of security measures (physical, personnel, information, CIS) shall be implemented to create a secure environment in which to operate a communication, information or other electronic system.

5.6.3. CIS Security is addressed further at Enclosure "F" of this C-M and in supporting Management and Technical and Implementation directives on CIS Security.

5.7. Industrial Security

5.7.1. Industrial security is the application of protective measures and procedures to prevent, detect and recover from the loss or compromise of classified information handled by industry in contracts. NATO classified information disseminated to industry, generated as a result of a contract with industry, and classified contracts with industry shall be protected in accordance with NATO Security Policy and supporting directives.

5.7.2. Before a facility or its employees, managers or owners can have access to classified information or be invited to bid, negotiate or perform on a classified contract or work on a classified study involving access to information classified CONFIDENTIAL or above, the facility shall be granted a facility security clearance issued by the National Security Authority (NSA) (or, if appropriate, the Designated Security Authority (DSA)) of its nation of origin, that is to say, the nation in which the facility is located and incorporated to do business.

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2010)0003-ADD1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

5.7.3. Facilities shall be required to protect classified information in accordance with the basic principles and minimum standards contained in this C-M. NSAs shall ensure that they have the means to make their industrial security requirements binding upon industry and that they have the right to inspect and approve the measures taken in industry for the protection of classified information.

5.7.4. Industrial security is addressed further at Enclosure "G" of this C-M and in the supporting industrial security directive.

6. PROTECTION OF INFORMATION ON KEY POINTS

6.1. The publication of information about civilian installations (defence supplies, energy supply, etc.) of military significance in times of tension or war may assist bombing, sabotage or terrorist attack by allowing potential enemies to compile a key points list, and to identify points vulnerable to sabotage or terrorism within individual key points. Policy should be designed to hamper the compilation by potential enemies of a Key Points List, to allow the invocation of security exemptions from publication of relevant data, and to encourage awareness of the risks among installation owners and operators.

7. SECURITY RESPONSIBILITIES

7.1. National Security Authority (NSA)

7.1.1. Each member nation shall establish a National Security Authority (NSA) responsible for the security of NATO classified information.

7.1.2. The NSA is responsible for:

(a) the maintenance of security of NATO classified information in national agencies and elements, military or civil, at home or abroad;

(b) ensuring that periodic and appropriate inspections are made of security arrangements for the protection of NATO classified information in all national organisations at all levels, both military and civil, to determine that such arrangements are adequate and in accordance with current NATO security regulations. In the case of organisations holding CTS or ATOMAL information, security inspections shall be made at least every 24 months, unless, during that period, they are carried out by the NOS;

(c) ensuring that a security determination of eligibility has been made in respect of all nationals who are required to have access to information classified NC and above, in accordance with NATO Security Policy;

(d) ensuring that such national emergency security plans as are necessary to prevent NATO classified information from falling into unauthorised or hostile hands have been prepared; and

(e) authorising the establishment (or dis-establishment) of national Cosmic Central Registries. The establishment (or dis-establishment) of Cosmic Central Registries shall be notified to the NOS.

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2010)0003-ADD1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

7.2. Designated Security Authority (DSA)

7.2.1. Each member nation may designate one or more DSAs responsible to the NSA. In this case the DSA of a NATO nation is responsible for communicating to industry the national policy in all matters of NATO industrial security policy and for providing direction and assistance in its implementation. In some nations, the functions of a DSA may be carried out by the NSA.

7.3. Security Committee (SC)

7.3.1. The SC is established by the NAC and is composed of representatives from each member nation's National Security Authorities (NSAs) supported, where required, by additional member nation security staff. Representatives of the International Military Staff, Strategic Commands and C3 Board shall be present at the meetings of the SC. Representatives of NATO civil and military bodies may also be present when matters of interest to them are addressed.

7.3.2. The SC is responsible directly to the NAC for:

(a) reviewing NATO Security Policy (as set forth in C-M(2002)49 and C-M(2002)50) and making recommendations for change / endorsement to the NAC;

(b) examining questions concerning NATO Security Policy;

(c) reviewing and approving the supporting directives and guidance documents published by the SC in the areas of personnel security, physical security, security of information, industrial security and CIS Security (Note: a nation may request that a supporting directive also be approved by the NAC); and

(d) considering security matters referred to it by the NAC, a member nation, the Secretary General, the Military Committee, the C3 Board or the heads of NATO civil and military bodies and preparing appropriate recommendations thereon.

7.4. NATO Office of Security (NOS)

7.4.1. The NOS is established within the NATO International Staff. It is composed of personnel experienced in security matters in both military and civil spheres. The Office maintains close liaison with the NSA of each member nation, and with NATO civil and military bodies. The Office may also, as required, request member nations and NATO civil and military bodies to provide additional security experts to assist it for limited periods of time when full-time additions to the Office would not be justified. The Director, NOS, serves as Chairman to the SC.

7.4.2. The NOS is responsible for:

(a) the examination of any questions affecting NATO security;

(b) identifying means whereby NATO security might be improved;

(c) the overall co-ordination of security for NATO among member nations and NATO civil and military bodies;

(d) ensuring the implementation of NATO security decisions, including the provision of such advice as may be requested by member nations and NATO civil and military bodies either in their application of the basic principles and the standards of security described in this Enclosure, or in the implementation of the specific security requirements;

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2010)0003-ADD1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

(e) informing, as appropriate, the SC, the Secretary General and the Chairman of the Military Committee of the state of security within NATO, and the progress made in implementing NAC decisions regarding security;

(f) carrying out periodic surveys of security systems for the protection of NATO classified information in member nations, NATO civil bodies, and SHAPE and HQ SACT;

(g) carrying out periodic surveys of security systems for the protection of released NATO classified information in non-NATO nations and international organisations with whom NATO has signed a Security Agreement;

(h) co-ordinating, with NSAs and NATO civil and military bodies, the investigation into cases of lost, compromised or possibly compromised NATO classified information;

(i) informing NSAs of any adverse information which comes to light concerning their nationals;

(j) devising security measures for the protection of the NATO Headquarters, Brussels and ensuring their correct implementation; and

(k) carrying out, under the direction and on behalf of the Secretary General, acting in the name of the NAC and under its authority, responsibilities for supervising the application of the NATO security programme for the protection of ATOMAL information under the provisions of the Agreement and supporting Administrative Arrangements referenced at paragraph 3.2 above.

7.5. NATO Military Committee and NATO Military Bodies

7.5.1. As the highest military authority in NATO, the NAMILCOM is responsible for the overall conduct of military affairs. The NAMILCOM is consequently responsible for all security matters within the NATO military structure including centralised overall cognisance of measures necessary to assure the adequacy of cryptographic techniques and materials used for transmitting NATO classified information, including the security approval of NATO funded cryptographic equipment as defined in Enclosure "F". In accordance with previously agreed policy and in compliance with its Terms of Reference in paragraph 7.4.2 above, the NOS carries out the executive functions for security within the NATO military structure and keeps the Chairman of the NAMILCOM informed.

7.5.2. The Heads of NATO military bodies established under the aegis of the NAMILCOM are responsible for all security matters within their establishment. This includes responsibility for ensuring that a security organisation is set up, that security programmes are devised and executed in accordance with NATO Security Policy and that the security measures are inspected periodically at each command level. In cases of organisations holding COSMIC TOP SECRET (CTS) or ATOMAL information, security inspections are to be made at least every 24 months, unless, during that period, an inspection has been carried out by the NOS.

7.6. NATO Civil Bodies

7.6.1. The NATO International Staff and NATO civil agencies are responsible to the NAC for the maintenance of security within their establishment. This includes responsibility for ensuring that a security organisation is set up, that security programmes are devised and executed in accordance with NATO Security Policy and that the security measures are inspected periodically at each command level. In cases of organisations holding COSMIC TOP SECRET (CTS) or ATOMAL

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2010)0003-ADD1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

information, security inspections are to be made at least every 24 months, unless, during that period, an inspection has been carried out by the NOS.

7.7. CIS Security

7.7.1. Principal organisations with responsibilities for CIS Security (for example, the C3B, NCSAs and NDAs) are described in Enclosure "F".

8. SECURITY CO-ORDINATION

8.1. Any NATO security problem necessitating co-ordination between NSAs of member nations, and NATO civil and military bodies, shall be referred to the NATO Office of Security (NOS). In cases where such reference is by military authorities, this shall be made through command channels. Any unresolved differences arising in the course of such co-ordination shall be submitted by the NOS to the Security Committee (SC) for consideration.

8.2. Any proposals by member nations and NATO civil and military bodies involving modification of NATO security procedures shall be referred in the first instance to the NOS. Any proposals made by the military authorities shall be transmitted through command channels. If the NATO security problems giving rise to such proposals cannot be resolved except by modification of NATO Security Policy, the proposals shall be referred to the SC, and if necessary, by it to the NAC.

DECLASSIFIED/DECLASSIFIEE - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

ENCLOSURE "C"

PERSONNEL SECURITY

INTRODUCTION

1. This Enclosure sets out the policy and minimum standards for personnel security. Amplifying details are found in the supporting directive on personnel security.

2. There shall be an agreed standard of confidence about the loyalty, trustworthiness and reliability of all individuals granted access to, or whose duties or functions may afford access to, NATO classified information. All individuals, civilian and military, whose duties require access to information classified NC and above shall be sufficiently investigated to give a satisfactory level of confidence as to their eligibility for access to such information.

3. Individuals authorised to have access to information classified NC and above shall have been granted an appropriate personnel security clearance (PSC), granted by their NSA or other competent authority, valid for the duration of the authorised access, and have a need-to-know. The extent of security clearance procedures shall be determined by the classification of the NATO information to which the individual is to have access. Security clearance procedures shall be in accordance with NATO security policy and supporting directives.

4. Individuals who require access to information classified NC and above shall have been granted an appropriate personnel security clearance (PSC) , shall have been briefed on NATO security procedures, shall have acknowledged their responsibilities, and shall have a need-to-know. Individuals who require access to only information classified NR shall have been briefed on their security responsibilities, and shall have a need-to-know. Unless specifically required by national security rules and regulations, a security clearance is not required for access to information classified NR.

5. The granting of a PSC should not be considered as a final step in the personnel security process; there is a requirement to ensure an individual's continuing eligibility for access to NATO classified information. This should be achieved through continuous evaluation by security authorities and managers; and through security education and awareness programmes which remind individuals of their security responsibilities and of the need to report, to their managers or security staffs, information which may affect their security status.

DECLASSIFIED/DECLASSIFIEE - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

APPLICATION OF THE "NEED TO KNOW" PRINCIPLE

6. Individuals in NATO nations and in NATO civil and military bodies shall only have access to NATO classified information for which they have a need-to-know. No individual is entitled solely by virtue of rank or appointment or PSC to have access to NATO classified information.

PERSONNEL SECURITY CLEARANCES (PSCs)

Responsibilities

7. The PSC responsibilities of NSAs, or other competent national authorities, NATO nations and the Heads of a NATO civil or military body are set out in the supporting personnel security directive.

8. Individuals shall be made aware of their responsibilities to comply with security regulations, and act in the interests of security.

Personnel Security Directive

9. The supporting personnel security directive sets out the following :

(a) the requirements for identifying positions requiring an appropriate PSC;

(b) the criteria for assessing the loyalty, trustworthiness and reliability of an individual in order for him to be granted and to retain a PSC;

(c) the investigative requirements for NATO CONFIDENTIAL, NATO SECRET and COSMIC TOP SECRET clearances;

(d) the requirements for the provision of PSCs for employees of NATO civil and military bodies;

(e) the requirements for revalidation of PSCs;

(f) the procedures for addressing adverse information about an individual holding a PSC; and

(g) the requirements for maintaining records of PSCs granted to individuals.

SECURITY AWARENESS AND BRIEFING OF INDIVIDUALS

10. All individuals employed in positions where they have access to NR information, or hold a clearance for access to NC or above, shall be briefed on security procedures and their security obligations. All cleared individuals shall acknowledge that they fully understand

DECLASSIFIED/DECLASSIFIEE - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

their responsibilities and the consequences which the law or administrative or executive order of their nation provides when classified information passes into unauthorised hands either by intent or through negligence. A record of the acknowledgement shall be maintained by the NATO nation or NATO civil or military body authorising access to NATO classified information.

11. All individuals who are authorised access to, or required to handle NATO classified information, shall initially be made aware, and periodically reminded of the dangers to security arising from indiscreet conversation with persons having no need-to-know, their relationship with the media, and the threat presented by the activities of intelligence services which target NATO and its member nations. Individuals shall be thoroughly briefed on these dangers and must report immediately to the appropriate security authorities any approach or manoeuvre which they consider suspicious or unusual.

AUTHORISING ACCESS TO NATO CLASSIFIED INFORMATION

ACCESS BY NATO NATIONALS

12. An individual shall only be authorised access to NATO classified information after he has been granted the appropriate personnel security clearance, a determination of his need-to-know has been made, and he has been briefed on NATO security procedures and has acknowledged his security obligations.

Exceptional Circumstances

13. However, circumstances may arise when, for example for urgent mission purposes, some of the requirements in paragraph 12 above cannot be met. Details in respect to provisional appointments, one-time access, emergency access, and attendance at conferences and meetings are set out in the supporting personnel security directive.

ACCESS BY NON-NATO NATIONALS

14. Non-NATO nationals serving as integrated members of the Armed Forces of NATO member nations may be authorised access up to and including information classified CTS. In the case of such nationals it shall be incumbent upon the NSA to satisfy itself that the conditions for access stipulated in paragraphs 12 or 13 above are fulfilled.

15. Individuals who are nationals[1] of non-NATO nations may be granted access to NATO classified information on a case-by-case basis, provided that :

1 Nationals of non-NATO nations includes "nationals of a Kingdom", "citizens of a State", and "landed immigrants in Canada". "Landed immigrants in Canada" are individuals who have gone through a national screening process including residency checks, criminal records and security checks, and who are going to obtain lawful permission to establish permanent residence in the nation.

DECLASSIFIED/DECLASSIFIEE - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

(a) access is necessary in support of a specified NATO programme, project, contract, operation, or related task;

(b) the individual is granted a NATO Personnel Security Clearance (PSC) based on a clearance procedure no less rigorous than that required for a NATO national in accordance with NATO security policy and supporting directives; noting that a NATO PSC is not required for access to NR information;

(c) the prior written consent of the NATO nation or NATO civil or military body that originated the information is obtained; and

(d) the non-NATO individual in question shall have clearly understood and undertaken, by means of personally undersigning an acknowledgement of responsibilities, that NATO information that he might have access to in the context of a specified NATO programme, project, contract, operation, or related task, shall strictly and solely be used for the purposes of the entrusted task and shall not be shared with or transmitted to third persons, bodies, organisations or governments.

16. As an exception to the requirement for originator control in sub-paragraph 15(c) above, NSAs of NATO nations may approve access to NATO classified information by nationals of certain non-NATO nations who are employed by the Government of the NATO nation, or by a contractor that is located and incorporated in the NATO nation, provided that, in addition to those criteria set out in sub-paragraphs 15(a), 15(b) and 15(d) above, the criteria set out in the equivalent section of the supporting personnel security directive are applied.

DECLASSIFIED/DECLASSIFIEE - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

ENCLOSURE "D"

PHYSICAL SECURITY

INTRODUCTION

1. This Enclosure sets out the policy and minimum standards for physical security measures for the protection of NATO classified information. Amplifying details are found in the supporting directive on physical security.

2. NATO nations and NATO civil and military bodies shall establish physical security programmes that meet these minimum standards. Such programmes, which consist of active and passive security measures, shall provide a common degree of protection consistent with the security classification of the NATO information to be protected.

SECURITY REQUIREMENTS

3. All premises, buildings, offices, rooms, and other areas in which NATO classified information and material is stored and/or handled shall be protected by appropriate physical security measures. In deciding what degree of physical security protection is necessary, account shall be taken of all relevant factors, such as:

(a) the level of classification and category of information;

(b) the quantity and form of the information (hard copy/computer storage media) held;

(c) the security clearance and need-to-know of the staff;

(d) the locally-assessed threat from intelligence services which target NATO and/or its member nations, sabotage, terrorist, subversive or other criminal activities; and

(e) how the information will be stored.

4. Physical security measures shall be designed to:

(a) deny surreptitious or forced entry by an intruder;

DECLASSIFIED/DECLASSIFIEE - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

(b) deter, impede and detect actions by disloyal personnel (the spy within);

(c) allow for segregation of personnel in their access to NATO classified information in accordance with the need-to-know principle; and

(d) detect and act upon all security breaches as soon as possible.

PHYSICAL SECURITY MEASURES

5. Physical measures represent only one aspect of protective security and shall be supported by sound personnel security, security of information, and INFOSEC measures, details of which will be found respectively in Enclosures "C", "E" and "F". Sensible management of security risks will involve establishing the most efficient and cost-effective methods of countering the threats and compensating for vulnerabilities by a combination of protective measures from these areas. Such efficiency and cost-effectiveness is best achieved by defining physical security requirements as part of the planning and design of facilities, thereby reducing the need for costly renovations.

6. Physical security programmes shall be based on the principle of "defence in depth", and although physical security measures are site-specific, the following general principles shall apply. It is first necessary to identify the locations that require protection. This is followed by the creation of layered security measures to provide "defence in depth" and delaying factors. The outermost physical security measures shall define the protected area and deter unauthorised access. The next level of measures shall detect unauthorised or attempted access and alert the guard force. The innermost level of measures shall sufficiently delay intruders until they can be detained by the guard force. Consequently, there is an interrelationship between the reaction time of the guard force and the physical security measures designed to delay intruders.

7. Regular maintenance of security systems is necessary to ensure that equipments operate at optimum performance. It is also necessary to periodically re-evaluate the effectiveness of individual security measures and the complete security system. This is particularly important if there is a change in use of the site or elements of the security system. This can be achieved by exercising incident response plans.

Security Areas

8. Areas in which information classified NC and above is handled and stored shall be organised and structured so as to correspond to one of the following:

(a) **NATO Class I Security Area**: an area in which information classified NC and above is handled and stored in such a way that entry into the area constitutes, for all practical purposes, access to classified information. Such an area requires:

DECLASSIFIED/DECLASSIFIEE - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

(i) a clearly defined and protected perimeter through which all entry and exit is controlled;

(ii) an entry control system which admits only those individuals appropriately cleared and specifically authorised to enter the area;

(iii) specification of the level of classification and the category of the information normally held in the area, i.e. the information to which entry gives access;

(b) **NATO Class II Security Area**: an area in which information classified NC and above is handled and stored in such a way that it can be protected from access by unauthorised individuals by controls established internally. Such an area requires:

(i) a clearly defined and protected perimeter through which all entry and exit is controlled;

(ii) an entry control system which admits unescorted access only to those individuals who are security cleared and specifically authorised to enter the area. For all other individuals, provision shall be made for escorts or equivalent controls, to prevent unauthorised access to NATO classified information and uncontrolled entry to areas subject to technical security inspection.

9. Those areas which are not occupied by duty personnel on a 24-hour basis shall be inspected immediately after normal working hours to ensure that NATO classified information is properly secured.

Administrative Zones

10. An Administrative Zone may be established around or leading up to NATO Class I or Class II security areas. Such a zone requires a visibly defined perimeter within which the possibility exists for the control of individuals and vehicles. Only information classified up to and including NR shall be handled and stored in Administrative Zones.

Access to NATO Class II Security Areas by Individuals from Non-NATO Nations / International Organisations

11. Individuals from non-NATO nations / International Organisations who, because of their assignment and official duties, need regular interface with NATO staffs may be granted unescorted access to a NATO Class II Security Area. Such individuals may also be assigned office space within a NATO Class II Security Area in order to fulfil their assignment and official duties. The granting of unescorted access and/or the assignment of office space shall be handled on a case-by-case basis, and shall be in accordance with the criteria set out in the supporting Directive on Physical Security.

DECLASSIFIED/DECLASSIFIEE - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

Specific Measures

12. The following measures are identified to indicate examples of physical security measures that can be implemented :

(a) perimeter fence - a perimeter fence will form a useful physical barrier and will identify the boundary of an area requiring security protection. The effectiveness of any security perimeter will depend, to a large extent, on the level of security at the points of access;

(b) intruder detection system (IDS) – IDS may be used on perimeters to enhance the level of security offered by the fence, or may be used in rooms and buildings in place of, or to assist, guards;

(c) control of access – control of access may be exercised over a site, a building or buildings on a site or to areas or rooms within a building. The control may be electronic, electro-mechanical, by a guard or receptionist, or physical;

(d) guards – the employment of appropriately cleared, trained and supervised guards can provide a valuable deterrent to individuals who might plan covert intrusion;

(e) closed circuit television (CCTV) - CCTV is a valuable aid to security guards in verifying incidents and IDS alarms on large sites or perimeters; and

(f) security lighting - security lighting can offer a high degree of deterrence to a potential intruder, in addition to providing the illumination necessary for effective surveillance either directly by the guards or indirectly through a CCTV system.

Entry and Exit Searches

13. NATO establishments shall undertake random entry and exit searches which are designed to act as a deterrent to the unauthorised introduction of material into, or the unauthorised removal of NATO classified information from a site or building.

Access Control

14. A pass or personal recognition system governing the regular staff shall control entry into Class I or II security areas. Visitors shall be permitted escorted or unescorted access to a NATO establishment based upon checks on the individual and their access requirements.

DECLASSIFIED/DECLASSIFIEE - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

MINIMUM STANDARDS FOR THE STORAGE OF NATO CLASSIFIED INFORMATION

15. NATO classified information shall be stored only under conditions designed to deter and detect unauthorised access to the information.

16. **COSMIC TOP SECRET (CTS)**. CTS information shall be stored within a class I or II security area under one of the following conditions :

(a) in an IDS-equipped vault, or in a nationally-approved security container in an area which is subject to continuous protection or periodic inspection; or

(b) an IDS-protected open storage area constructed in accordance with the supporting physical security directive.

17. **NATO SECRET (NS).** NS information shall be stored within a class I or II security area under one of the following conditions :

(a) in the same manner as prescribed for CTS information; or

(b) in a nationally-approved security container or vault; or

(c) an open storage area, which is IDS-protected, or subject to continuous protection or periodic inspection.

18. **NATO CONFIDENTIAL (NC).** NC information shall be stored in the same manner as prescribed for CTS or NS information except that supplemental controls, as described in the supporting physical security directive, are not required.

19. **NATO RESTRICTED (NR).** NR information shall be stored in a locked container.

20. Amplifying details for the storage of NATO classified information are set out in the supporting directive on physical security.

PROTECTION AGAINST TECHNICAL ATTACKS

Eavesdropping

21. Offices or areas in which information classified NS and above is regularly discussed shall be protected against passive and active eavesdropping attacks, by means of sound physical security measures and access control, where the risk warrants it. The responsibility for determining the risk shall be coordinated with technical specialists and decided by the appropriate security authority.

DECLASSIFIED/DECLASSIFIEE - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

Technically Secure Areas

22. Areas to be protected against audio eavesdropping shall be designated as technically secure areas and entry to them shall be specially controlled. Rooms shall be locked and /or guarded in accordance with physical security standards when not occupied and any keys treated as security keys. Such areas shall be subject to regular physical and/or technical inspections in accordance with the requirements of the appropriate security authority, and shall also be undertaken following any unauthorised entry or suspicion of such and entry by external personnel for maintenance work or redecoration.

PHYSICAL SECURITY FOR COMMUNICATION AND INFORMATION SYSTEMS (CIS)

23. Areas in which NATO classified information is presented or handled using information technology, or where potential access to such information is possible, shall be established such that the aggregate requirement for confidentiality, integrity and availability is met. Areas in which CIS are used to display, store, process, or transmit information classified NC and above, or where potential access to such information is possible, shall be established as NATO Class I or Class II security areas or the national equivalent. Areas in which CIS are used to display, store, process or transmit information classified NR, or where potential access to such information is possible, may be established as Administrative Zones.

APPROVED EQUIPMENT

24. NSAs shall maintain lists of equipment which they or other NATO nations have approved for the protection of NATO classified information under various specified circumstances and conditions. NATO civil and military bodies shall ensure that any equipment purchased complies with the regulations of a NATO member nation(s).

OTHER PHYSICAL SECURITY MEASURES

25. Detailed requirements are set out in the supporting physical security directive, addressing, for example, rooms and locks, keys and combinations, and containers and locks.

DECLASSIFIED/DECLASSIFIEE - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

ENCLOSURE "E"

SECURITY OF INFORMATION

INTRODUCTION

1. This Enclosure sets out the policy and minimum standards for the security of NATO classified information. Amplifying details are found in the supporting security of information directive.

2. NATO classified information requires protection throughout its life-cycle. It shall be managed to ensure that it is appropriately classified, clearly identified as classified information, and remains classified only for as long as this is necessary. Security of information measures shall be complemented by personnel, physical and INFOSEC safeguards to ensure a balanced set of measures for the protection of NATO classified information.

CLASSIFICATION and MARKINGS

General

3. The originator is responsible for determining the security classification and initial dissemination of information. The classification level of NATO information shall not be changed, downgraded or declassified without the consent of the originator. At the time of its creation, originators shall indicate, where possible, whether their information can be downgraded or declassified on a certain date or event.

4. The classification assigned determines the physical security given to the information in storage and transmission, its circulation, destruction and the personnel security clearance required for access. Therefore both over-classification and under-classification should be avoided in the interests of effective security as well as efficiency.

5. NATO nations and NATO civil and military bodies shall introduce measures to ensure that information created by, or provided to NATO is assigned the correct security classification, and protected in accordance with the requirements of the supporting security of information directive.

DECLASSIFIED/DECLASSIFIEE - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

6. Each NATO civil or military body shall establish a system to ensure that CTS information which it has originated is reviewed no less frequently than every five years to ascertain whether the CTS classification still applies. Such a review is not necessary in those instances where the originator has predetermined that specific CTS information shall be automatically downgraded after two years and the information has been so marked.

7. The overall security classification of a document shall be at least as high as that of its most highly classified component. Component parts of documents classified NC and above shall, where possible, be classified (including by paragraph) by the originator to facilitate decisions on further dissemination of appropriate sections. Covering documents shall be marked with the security classification of the information contained therein when they are separated from the information they accompany.

8. When information from various sources is collated, the product shall be reviewed for overall security classification since it may warrant a higher classification than its component parts. Original security classification caveats must be retained when information is used to prepare composite documents.

Qualifying Markings

9. The terms COSMIC and NATO are qualifying markings which, when applied to classified information, signify that the information shall be protected in accordance with NATO Security Policy.

Special Category Designators

10. The term "ATOMAL" is a marking applied to special category information signifying that the information shall be protected in accordance with the Agreement and supporting Administrative Arrangements referenced in Enclosure "B", paragraph 5.

11. The term "SIOP" is a marking applied to special category information signifying that the information shall be protected in accordance with the reference cited in Enclosure "B", paragraph 6.

12. The term “CRYPTO” is a marking and a special category designator identifying all COMSEC keying material used to protect or authenticate telecommunications carrying NATO security-related information; signifying that the information shall be protected in accordance with the appropriate cryptographic security instructions.

13. The term “BOHEMIA” is a marking applied to special category information derived from or pertaining to Communications Intelligence (COMINT). All information marked COSMIC TOP SECRET - BOHEMIA will be protected in strict accordance with MC 101 (NATO Signals Intelligence Policy) and its companion Allied Joint Publication (AJP) which covers doctrinal and procedural issues.

DECLASSIFIED/DECLASSIFIEE - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

Dissemination Limitation Markings

14. As an additional marking to further limit the dissemination of NATO classified information, a Dissemination Limitation Marking may be applied by the originator.

CONTROL AND HANDLING

Objectives of Accountability

15. The primary objective of accountability is to provide sufficient information to be able to investigate a deliberate or accidental compromise of accountable information and assess the damage arising from the compromise. The requirement for accountability serves to impose a discipline on the handling of, and control of access to, accountable information.

16. Subordinate objectives are :

(a) to keep track of access to accountable information – who has, or potentially has, had access to accountable information; and who has attempted to access accountable information;

(b) to know the location of accountable information; and

(c) to keep track of the movement of accountable information within the NATO and national domains.

17. CTS and NS and ATOMAL information shall be accountable, controlled and handled in accordance with the requirements of this Enclosure and the supporting security of information directive. Where required by National rules and regulations, information bearing other classification or special category markings may be considered as accountable information.

The Registry System

18. There shall be a Registry System which is responsible for the receipt, accounting, handling, distribution and destruction of accountable information. Such a responsibility may be fulfilled either within a single registry system, in which case strict compartmentalisation of CTS information shall be maintained at all times, or by establishing separate registries and control points.

19. Each NATO member nation and NATO civil or military body shall establish a Central Registry(s) for CTS, which acts as the main receiving and despatching authority for the nation or body within which it has been established. The Central Registry(s) may also act as a registry(s) for other accountable information.

20. Registries and control points shall act as the responsible organisation for the internal distribution of CTS and NS information and for keeping records of all accountable documents held on that registry's or control point's charge; they may be

DECLASSIFIED/DECLASSIFIEE - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

established at ministry, department, or command levels. NC and NR information is not required to be processed through the Registry System unless specified by National security rules and regulations.

21. With regard to NATO accountable information, registries and control points shall be able at all times to establish its location. Infrequent and temporary access to such information does not necessarily require the establishment of a registry or control point, provided procedures are in place to ensure that the information remains under the control of the Registry System.

22. The dissemination of information classified CTS shall be through COSMIC registry channels. At least annually, each registry shall carry out an inventory of all information classified CTS for which it is accountable, in accordance with the requirements of the supporting security of information directive. Regardless of the type of registry organisation, those that handle information classified CTS shall appoint a "COSMIC Control Officer" (CCO).

23. The supporting security of information directive sets out, inter alia, the responsibilities of the CCO, the detailed registry system handling processes for CTS and NS information, the procedures for reproductions, translations and extracts, the requirements for the dissemination of transmission of information, and the requirements for the disposal and destruction of information.

24. The NAMILCOM has established a separate system for the accountability, control and distribution of cryptographic material. Material being transferred through this system do not require accountability in the Registry System.

CONTINGENCY PLANNING

25. NATO nations and NATO civil and military bodies shall prepare contingency plans for the protection or destruction, during emergency situations, of NATO classified information to prevent unauthorised access and disclosure and loss of availability. These plans shall give highest priority to the most sensitive, and mission- or time-critical information.

SECURITY INFRACTIONS, BREACHES AND COMPROMISES

26. The protection of NATO classified information depends on the design of appropriate security regulations to give effect to approved security policy, directives and guidance, and on the effective implementation of these regulations by education and supervision backed up by disciplinary and, in extreme cases, legal sanctions.

27. All breaches of security shall be reported immediately to the appropriate security authority. Each reported breach of security shall be investigated by individuals who have security, investigative and, where appropriate, counterintelligence experience, and who are independent of those individuals immediately concerned with the breach.

DECLASSIFIED/DECLASSIFIEE - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

28. The main purpose of reporting compromises of NATO classified information is to enable the originating NATO component to assess the resulting damage to NATO and to take whatever action is desirable or practicable to minimize the damage. Reports of the damage assessment and minimising action taken shall be forwarded to the NOS.

29. When a compromise of NATO classified information has to be reported to the NOS, the report shall be forwarded through the NSA or the Head of the NATO civil or military body concerned. Where possible, the reporting authority should inform the originating NATO component at the same time as the NOS, but the latter may be requested to do this when the originator is difficult to identify. The timing of the reports depends on the sensitivity of the information and the circumstances.

30. The Secretary General of NATO may request the appropriate authorities to make further investigations and to report.

31. The supporting security of information directive sets out the detailed actions, records and reporting requirements for breaches and compromises of security.

32. Separate provisions relating to the compromise of cryptographic material have been issued by the NAMILCOM to communications security authorities of member nations and NATO civil and military bodies.

SECURITY ARRANGEMENTS FOR THE RELEASE OF NATO CLASSIFIED INFORMATION TO NON-NATO NATIONS AND INTERNATIONAL ORGANISATIONS

Introduction

33. Classified information entrusted to or generated by NATO in order to enable it to perform its missions is disseminated and protected in accordance with NATO Security Policy, directives and procedures. This section sets out the policy for the release of NATO classified information to non-NATO nations and international organisations including such nations (hereinafter referred to as non-NATO recipients). This section also covers information contained in documents issued by the NAC, or by any other NATO committee or NATO civil or military body (hereinafter referred to as NATO bodies).

34. The release of NATO classified information to non-NATO recipients shall take place in the context of NATO cooperative activities approved by the NAC. Any request for the release of NATO classified information to non-NATO recipients outside such cooperative activities shall be examined and approved on a case-by-case basis.

35. ATOMAL information of any classification may not be released to any nation/organisation which is not a party to the current versions of C-M(64)39 and C-M(68)41.

DECLASSIFIED/DECLASSIFIEE - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

Principles for Authorising the Release of NATO Classified Information to Non-NATO Nations and International Organisations

36. Authorisation to release shall always be subject to the consent of the originator(s). Additionally, the following shall apply :

(a) for NATO classified information to be released under NAC-approved NATO cooperative activities, where the non-NATO participants to that activity have been endorsed by the NAC on a case-by-case basis :

(i) release decisions can either concern clearly identified information or a general category of information;

(ii) the subject matter shall be included in the general work plan or the OPLAN for the activity or in the practical measures established for cooperation;

(iii) the release of NATO classified information shall be necessary to initiate cooperation on a specific subject, and to continue cooperation within the approved activity;

(iv) a Security Agreement, signed by the Secretary General on behalf of NATO and by a representative duly mandated[2] by the non-NATO recipient, shall have been concluded. In the absence of a Security Agreement and in exceptional circumstances, in order to support specific operational requirements endorsed by the NAMILCOM / NAC (for example, in support of force protection, and the exchange of intelligence information), a Security Assurance from the non-NATO recipient, signed by a representative duly mandated[1] by the non-NATO recipient that any information received will be protected in accordance with its national laws and regulations and to a degree no less stringent than NATO minimum standards, shall have been provided to the NATO Office of Security;

(v) where a Security Agreement is in force with an international organisation, the release of information to its non-NATO members shall be in accordance with the relevant provisions of the Security Agreement as well as other established rules concerning their participation in NATO activities;

(vi) the Security Assurance provided by the non-NATO recipient shall also identify the NATO security classifications and the equivalent security classifications of the non-NATO recipient. The Security Assurance shall be forwarded to the relevant committee responsible

---

2 A "representative duly mandated" is an officially authorised representative who is either the direct recipient of released information or is a senior representative responsible for ensuring the protection of information released in support of a co-operative activity.

DECLASSIFIED/DECLASSIFIEE - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

for the approval of the release. Copies of the written Security Assurances shall be provided to the NATO Office of Security who shall maintain a database of Security Assurances;

(vii) only information classified up to and including NC may be released through Security Assurances. However, in exceptional circumstances, in order to support specific operational requirements endorsed by the NAMILCOM / NAC, NS information may be released; and

(viii) where there is a requirement to release NS information to a non-NATO nation which has signed a Security Agreement / Arrangement with a NATO sponsor, the NATO sponsor shall provide the necessary assurance that the appropriate security system is in place for the protection of such released information, and shall seek the agreement of the relevant committee responsible for the approval of the release prior to its release; and

(b) for NATO classified information to be released on special request from NATO member nations (the Sponsor) to non-NATO recipients outside NAC-approved cooperative activities :

(i) release decisions shall be taken on a case-by-case basis and can only concern clearly identified information;

(ii) a bilateral Security Agreement / Arrangement shall exist between the NATO member nation sponsoring the release and the non-NATO recipient;

(iii) the Sponsor shall be responsible for providing a written Security Assurance, signed by a representative duly mandated[3] by the non-NATO recipient, to NATO from the non-NATO recipient. The Security Assurance provided by the non-NATO recipient shall oblige the non-NATO recipient to protect NATO classified information to a degree no less stringent than the provisions contained in the bilateral Security Agreement / Arrangement for the protection of the Sponsor's classified information. The NATO security classifications shall be identified with their equivalents to the national classifications cited in the bilateral Security Agreement / Arrangement;

---

3 A "representative duly mandated" is an officially authorised representative who is either the direct recipient of released information or is a senior representative responsible for ensuring the protection of information released in support of a co-operative activity.

DECLASSIFIED/DECLASSIFIEE - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

(iv) the Sponsor shall forward this written Security Assurance to the relevant committee, together with the release request. Copies of written Security Assurances shall also be provided to the NATO Office of Security;

(v) the request shall demonstrate the advantage which would accrue to NATO. Justifications for release shall be specific, avoiding general statements;

(vi) where a Security Agreement is in force with an international organisation, the release of information to its non-NATO members shall be in accordance with the relevant provisions of the Security Agreement as well as other established rules concerning their participation in NATO activities; and

(vii) only information classified up to and including NC may be released through Security Assurances in this case. Where there is a requirement to release NS information to a non-NATO nation which has signed a Security Agreement / Arrangement with a NATO sponsor, the NATO sponsor shall provide the necessary assurance that the appropriate security system is in place for the protection of such released information, and shall seek the agreement of the relevant committee responsible for the approval of the release prior to its release.

Release Authority

37. The NAC is the ultimate authority for the release of NATO classified information to non-NATO recipients. This authority adheres to the principle of originator consent and is delegated, taking into account the principles for authorising the release identified in paragraph 36 above, to :

(a) the appropriate subject-matter committee for information classified up to and including NS which has been originated by that committee and/or bodies subordinate to it. For NR, the appropriate subject-matter committee may further delegate authority to a clearly identified staff support function or a specific role(s) within the support staffs to that committee;

(b) the NAMILCOM for information classified up to and including NS which has been originated by the NAMILCOM and/or bodies subordinate to it. For NR, the NAMILCOM may further delegate authority to a clearly identified staff support function or a specific role(s) within the support staffs to the NAMILCOM;

(c) SACEUR or D/SACEUR for information classified up to and including NS which is identified as being releasable to xFOR, or is classified NATO/xFOR SECRET (mission SECRET), under the following conditions :

DECLASSIFIED/DECLASSIFIEE - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

(i) the information is limited to NATO classified information necessary for the effective participation of non-NATO Troop Contributing Nations (NNTCN) in operations and exercises, as approved on a case-by-case by the NAC;

(ii) the information to be released is only that NATO classified information originating from within Allied Command Operations (ACO) and is directly related to specific operations and exercises where the participation of non-NATO nations to that activity has also been endorsed by the NAC on a case-by-case basis; and

(iii) the ACO Security Authority (SHAPE J2) shall implement an authoritative and auditable process for the release of classified information;

(d) the Mission Commander for an operation involving non-NATO Troop Contributing Nations, as endorsed by the NAC, for information classified up to and including NS that has already been determined as releasable to the mission (xFOR), under the following conditions :

(i) the information shall be related specifically to the Mission;

(ii) the information shall be limited to tactical information related to an ongoing operation and deemed necessary for the successful conduct of the ongoing operation;

(iii) the Mission Security Authority shall implement an authoritative and auditable process for the release of classified information; and

(iv) the NOS, in close co-ordination with SHAPE J2, reserves the right to conduct inspections of the security arrangements in place; and

(e) the NPLO, for NATO classified information originated by and belonging to one or more of the nations participating in the NPLO.

38. Authority for release shall only be delegated to an appropriate subject-matter committee on which the originator(s) is/are represented. If the originator(s) cannot be established, the appropriate subject-matter committee shall assume the responsibility of the originator. Authority for release may be delegated to the lowest committee level best suited to evaluate the importance of the classified information.

39. With the exceptions applying to NR information stated in paragraphs 37(a) and (b) above, delegated release authorities cannot further delegate their powers, although they can entrust subordinate bodies with the implementation of the release decision.

DECLASSIFIED/DECLASSIFIEE - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

40. NATO civil and military bodies shall keep control records of information classified CONFIDENTIAL and above which they have released to non-NATO recipients. These records shall be subject to inspection by the appropriate NATO security authority (for example, NOS, SHAPE J2).

Administrative Arrangements for the Implementation of a Security Agreement

41. The completion of the administrative arrangements shall be confirmed by a security survey carried out by the NOS of the relevant agencies of the non-NATO recipient. The security survey shall establish the ability of the non-NATO recipient to comply with the provisions of the Security Agreement and with the minimum standards.

42. The NOS shall produce a report of the survey and transmit a copy to the Security Authority of the non-NATO recipient. The original report shall be filed in the NOS and made available, upon request, to NATO member nations. The NATO Security Committee shall be provided with a written summary of the results of the NOS survey. The conclusion drawn from the survey as to the ability of the non-NATO recipient to protect NATO classified information shall be communicated by the NOS to the relevant NATO bodies and to NATO member nations.

43. The NOS shall carry out periodic security surveys, at least once every two years, of the relevant agencies of the non-NATO recipients to ensure that the non-NATO recipient continues to be compliant with the provisions of the Security Agreement and with the minimum standards.

44. Where a Security Assurance has been provided to NATO in respect to the protection of released classified information, an annual re-validation of that Security Assurance shall be provided, as appropriate, in accordance with the assessed continued need to receive information. The NOS shall also assess whether or not it would be more appropriate to negotiate a Security Agreement in lieu of the Security Assurance. The NOS shall keep the record of validated Security Assurances, which shall also comprise the grounds for such re-validation. The NATO member nations, on request, shall be provided with a copy of this record.

Supporting Directive on the Security of Information

45. The supporting security of information directive contains, inter alia, the :

(a) procedures for the release of NATO classified information to non-NATO recipients;

(b) specific release procedures for NATO Production and Logistics Organisations (NPLOs), international organisations and Combined Joint Task Forces (CJTFs);

DECLASSIFIED/DECLASSIFIEE - PUBLIC DISCLOSED/MISE EN LECTURE PUBLIQUE

(c) minimum standards required for the handling and protection of NATO classified information released to non-NATO recipients. The minimum standards apply to any non-NATO recipient, regardless of whether a Security Agreement has been concluded with NATO or a Security Assurance provided to NATO;

(d) detailed administrative arrangements to be implemented by all non-NATO recipients; and

(e) samples of the Security Assurance, the Personnel Security Clearance Certificate and the Certificate of Security Clearance.

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2010)0003-ADD1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

ENCLOSURE "F"

Communication and Information System Security

1. INTRODUCTION

1.1. This Enclosure sets out the policy and minimum standards for the protection of NATO classified information, and supporting system services and resources[1] in communication, information and other electronic systems storing, processing or transmitting NATO classified information.

1.2. This Enclosure supports the NATO Information Management Policy and complements the Policy on Management of Non-Classified NATO Information which addresses the basic principles and standards to be applied within NATO civil and military bodies and NATO member nations for the protection of non-classified NATO information.

1.3. Communication and Information System Security (CIS Security) is one of the elements of Information Assurance (Figure 1) and is defined as the application of security measures for the protection of communication, information and other electronic systems[2], and the information that is stored, processed or transmitted[3] in these systems with respect to confidentiality, integrity, availability, authentication and non-repudiation.

1.4. In order to achieve the security objectives of confidentiality, integrity, availability, authentication and non-repudiation[4] for classified information handled in these CIS, a balanced set of security measures (physical, personnel, information and CIS) shall be implemented to create a secure environment in which to operate a CIS. Where classified information is handled by industry in contracts, additional specific industrial security measures shall be applied in accordance with Enclosure G of this C-M and the supporting industrial security directive.

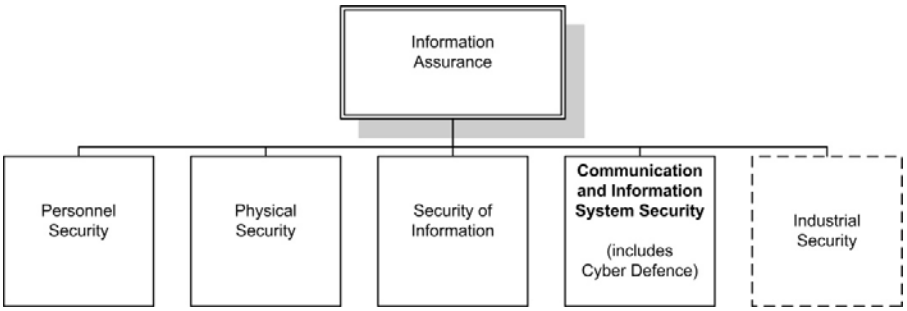

Figure 1 - Relationship between Information Assurance and CIS Security

---

1 Supporting System Services and Resources - those services and resources required to ensure that the security objectives of the CIS are achieved; to include, for example, cryptographic products and mechanisms, COMSEC materials, directory services, and environmental facilities and controls.

2 Hereafter referred to within this Enclosure as CIS.

3 Hereafter referred to within this Enclosure as handled.

4 Hereafter referred to within this Enclosure as Security Objectives

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2010)0003-ADD1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

1.5. The "Primary Directive on CIS Security", which is published by the SC and the C3B in support of this policy, addresses the CIS Security activities in the CIS life-cycle, and the CIS Security responsibilities of committees, and NATO civil and military bodies. The "Primary Directive on CIS Security" is supported by directives addressing CIS Security management (including security risk management, security accreditation, security-related documentation, and security review / inspection) and CIS Security technical and implementation aspects (including computer and local area network (LAN) security, interconnection of networks security, cryptographic security, transmission security, and emission security).

2. SECURITY OBJECTIVES

2.1. To achieve adequate security protection of NATO classified information handled in CIS, a balanced set of security measures (physical, personnel, information and CIS) shall be identified and implemented to create a secure environment in which a CIS operates, and to meet the following security objectives:

(a) to ensure the confidentiality of information by controlling the disclosure of, and access to, NATO classified information, and supporting system services and resources;

(b) to ensure the integrity of NATO classified information, and supporting system services and resources;

(c) to ensure the availability of NATO classified information, and supporting system services and resources;

(d) to ensure the reliable identification and authentication of persons, devices and services accessing CIS handling NATO classified information; and

(e) to ensure appropriate non-repudiation for individuals and entities having processed the information.

2.2. NATO classified information and supporting system services and resources, shall be protected by a minimum set of measures aimed at ensuring general protection against commonly encountered problems (whether accidental or intentional) known to affect all systems and supporting system services and resources. Additional measures shall be taken, appropriate to the circumstances, where a security risk assessment has established that NATO classified information and/or supporting system services and resources are subject to increased risks from specific threats and vulnerabilities.

2.3. Independent of the security classification of the NATO information being handled, NATO security authorities shall assess the risks and the level of damage done to NATO if the measures to achieve the non-confidentiality security objectives fail. The minimum set of measures for non-confidentiality services shall be determined in accordance with directives supporting this policy.

3. SECURITY ACCREDITATION

3.1. The extent to which the security objectives are to be met, and the extent to which CIS Security measures are to be relied upon for the protection of NATO classified information and supporting system services and resources shall be determined during the process of establishing the security requirement. The security accreditation process shall determine that an adequate level of protection has been achieved, and is being maintained.

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2010)0003-ADD1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

3.2. All CIS handling NATO classified information shall be subject to a security accreditation process, addressing the Security Objectives.

4. PERSONNEL SECURITY

4.1. Individuals authorised access to NATO classified information in any form shall be security cleared, where appropriate, taking account of their aggregate responsibility for achieving the Security Objectives of the information and the supporting system services and resources. This includes individuals who are authorised access to supporting system services and resources, or who are responsible for their protection, even if they are not authorised access to the information handled by the system.

5. PHYSICAL SECURITY

5.1. Areas in which NATO classified information is presented or handled using information technology, or where potential access to such information is possible, shall be established such that the aggregate requirement for the Security Objectives is met.

6. SECURITY of INFORMATION

6.1. All classified computer storage media shall be properly identified, stored and protected in a manner commensurate with the highest classification of the stored information.

6.2. NATO classified information recorded on re-usable computer storage media, shall only be erased in accordance with procedures approved by the appropriate security authority.

6.3. Approved security measures (confidentiality and non-confidentiality), implemented in accordance with directives supporting this policy, may be used to protect NATO classified information in computer storage media in such a manner as to reduce the physical security requirements commensurate with a lower classification level.

7. INDUSTRIAL SECURITY

7.1. A contractor facility used for contracts in which NATO classified information is handled on CIS shall be established to meet the aggregate requirement for the Security Objectives.

7.2. A consistent set of CIS security measures shall be described in contracts, Security Aspect Letters (SAL) and/or Project Security Instructions (PSI) and/or Service Level Agreements (SLA), as applicable, and be implemented by contractors to meet the NATO CIS security objectives and to protect NATO classified information and supporting services.

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2010)0003-ADD1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

8. SECURITY MEASURES

8.1. For all CIS handling NATO classified information, a consistent set of security measures shall be applied to meet the Security Objectives to protect information and supporting system services and resources. The security measures shall include, where appropriate, the following:

(a) a means to provide sufficient information to be able to investigate a deliberate, accidental or attempted compromise of the security objectives of classified information and supporting system services and resources, commensurate with the damage that would be caused;

(b) a means to reliably identify and authenticate persons, devices and services authorised access. Information and material which controls access to a CIS shall be controlled and protected under arrangements commensurate with the information to which it may give access. On NATO CIS strong authentication mechanisms for persons shall be implemented;

(c) a means to control disclosure of, and access to, NATO classified information and supporting system services and resources, based upon the need-to-know principle;

(d) a means to verify the integrity and origin of NATO classified information, and supporting system services and resources;

(e) a means to maintain the integrity of NATO classified information and supporting system services and resources;

(f) a means to maintain the availability of NATO classified information and supporting system services and resources;

(g) a means to control the connection of CIS handling NATO classified information;

(h) a determination of the confidence to be placed in the protection mechanisms of CIS Security;

(i) a means to assess and verify the proper functioning of the protection mechanisms of CIS Security over the life-cycle of the CIS;

(j) a means to investigate user and CIS activity;

(k) a means to provide non-repudiation assurances that the sender of information is provided with proof of delivery and the recipient is provided proof of the sender's identity; and

(l) a means to protect stored NATO classified information where the physical security measures do not meet the minimum standards.

8.2. Security management mechanisms and procedures shall be in place to deter, prevent, detect, withstand, and recover from, the impacts of incidents affecting the Security Objectives of NATO classified information and supporting system services and resources, including the reporting of security incidents.

8.3. The security measures shall be managed and implemented in accordance with directives supporting this policy.

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2010)0003-ADD1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

9. SECURITY RISK MANAGEMENT

9.1. CIS handling NATO classified information, in NATO civil and military bodies, shall be subject to security risk management, including security risk assessment, in accordance with the requirements of directives supporting this policy.

9.2. Security risk management of NATO CIS shall ensure continuous assessment of system vulnerabilities and security compliance and shall move towards dynamic risk management to be able to face effectively the challenges posed by today's complex operational scenarios and multifaceted threat environments.

10. ELECTROMAGNETIC TRANSMISSION [5] of NATO CLASSIFIED INFORMATION

10.1. When NATO classified information is transmitted electromagnetically, special measures shall be implemented to achieve the Security Objectives of such transmissions. NATO authorities shall determine the requirements for protecting transmissions from detection, interception or exploitation.

11. CRYPTOGRAPHIC SECURITY

11.1. When cryptographic products or mechanisms are required to provide confidentiality and non-confidentiality protection, whether during information transmission, processing or storage (data at rest), such products or mechanisms shall be specifically approved for the purpose and specific cryptographic requirements for physical, procedural and technical measures shall be implemented to achieve the required Security Objectives.

11.2. Data at rest shall be protected to a level adequate to the required Security Objectives, and, where cryptographic products and mechanisms are used, the requirements for cryptographic security shall be in accordance with the relevant NATO Technical and Implementation Directives.

11.3. During transmission, the confidentiality of information classified NS and above shall be protected by cryptographic products or mechanisms approved by the NATO Military Committee (NAMILCOM).

11.4. During transmission, the confidentiality of information classified NC or NR shall be protected by cryptographic products or mechanisms approved by either the NAMILCOM or a NATO member nation.

11.5. During transmission, the non-confidentiality requirements shall be assured in accordance with the communications system's operational requirement. The evaluation requirements and approval authority, for non-confidentiality mechanisms based on cryptography, shall be identified and agreed in conjunction with the specification of such mechanisms in the operational requirement, as agreed in technical directives.

---

[5] The term "electromagnetic transmission" covers transmission having both an electrical and magnetic character or properties, and includes, inter alia, visible light, radio waves, microwave, and infrared radiation.

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2010)0003-ADD1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

11.6. Under exceptional operational circumstances, information classified NC and NS may be transmitted in clear text provided each occasion is properly reported to the higher authorities. The exceptional circumstances are as follows:

(a) during impending or actual crisis, conflict, or war situations; and

(b) when speed of delivery is of paramount importance, means of encryption are not available and it is assessed that the transmitted information cannot be exploited in time to adversely influence operations.

11.7. Under exceptional operational circumstances, when speed is of paramount importance, means of encryption are not available and it is assessed that the transmitted information cannot be exploited in time to adversely influence operations, information classified NR may be transmitted in clear text.

11.8. During transmission between NATO and non-NATO nations / International Organisations (NNN/IO) CIS, the confidentiality of information classified NS and above shall be protected by cryptographic products or mechanisms approved by the NATO Military Committee (NAMILCOM).

11.9. During transmission within NNN/IO CIS, the confidentiality of information classified NS and above shall be protected by cryptographic products or mechanisms approved by the NATO Military Committee (NAMILCOM).

11.10. Where the requirements of paragraphs 11.8 and 11.9 above cannot be met, NATO and an IO may reach agreement on the mutual acceptance of each others' evaluation, selection and approval processes for cryptographic products or mechanisms authorised for the protection in transmission of NS information or IO information of the equivalent classification level. The conditions for such acceptance are set out in paragraph 11.12 below.

11.11. In exceptional circumstances, in order to support specific operational requirements, and where the requirements of paragraphs 11.8 and 11.9 above cannot be met, NATO may agree the NNN's evaluation, selection and approval processes for cryptographic products or mechanisms authorised for the protection in transmission of NS information or NNN information of the equivalent classification level. The conditions for such agreement are set out in paragraph 11.12 below.

11.12. The following conditions are applicable in respect to the scenarios described at paragraphs 11.10 and 11.11 above:

(a) the NNN/IO shall have a Security Agreement with NATO and be certified by the NATO Office of Security (NOS) that they can appropriately protect released NATO classified information;

(b) each NNN/IO shall be treated on a case-by-case basis; and the basis of any acceptance / agreement shall be set out in the security arrangements supporting the Security Agreement between NATO and the NNN/IO;

(c) the terms of any such acceptance / agreement shall be approved by the NAMILCOM on the basis of an objective assessment carried out by the NOS, working in conjunction with the NAMILCOM Communications and Information Systems Security and Evaluation Agency (SECAN), the C3B Information Assurance and Cyber Defence Capability Panel and the NATO HQ C3 Staff, of the capability of the NNN/IO to perform cryptographic evaluations that meet requirements equivalent to those used within NATO for the cryptographic protection of NS information; and

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2010)0003-ADD1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

(d) the NOS, in conjunction with SECAN and the NATO HQ C3 Staff, shall satisfy themselves, through verification and periodic re-verification, that the NNN/IO has in place appropriate structures, rules and procedures for the evaluation, selection, approval and control of cryptographic products and mechanisms, and that those structures, rules and procedures are being effectively and securely applied in practice.

11.13. Where acceptance / agreement is reached in accordance with the conditions set out in paragraph 11.12 above, the confidentiality of information classified NS may be protected by either cryptographic products or mechanisms approved by the NATO Military Committee (NAMILCOM) or cryptographic products or mechanisms approved by the NCSA (or equivalent authority) of the NNN/IO for the protection of the equivalent classification level.

11.14. During transmission between NATO and NNN/IO CIS and within NNN/IO CIS, the confidentiality of information classified NC or NR shall be protected by cryptographic products or mechanisms evaluated and approved by an appropriate authority. The appropriate authority may be the NAMILCOM, the NCSA of a NATO member nation or the equivalent authority of the NNN/IO, provided that the NNN/IO has appropriate structures, rules and procedures in place for the evaluation, selection, approval and control of such products or mechanisms, and that those structures, rules and procedures are being effectively and securely applied in practice. The structures, rules and procedures shall be agreed between the NAMILCOM and the NNN/IO.

11.15. The sensitive nature of the cryptomaterial used to protect NATO classified information necessitates the application of special security precautions beyond those required for the protection of other NATO classified information.

11.16. The protection which shall be afforded to cryptomaterial shall be commensurate with the damage that may be caused should that protection fail. There shall be positive means to assess and verify the protection and proper functioning of the cryptographic products and mechanisms, and the protection and control of cryptographic information (e.g. implementation details and associated documentation).

11.17. In recognition of the particular sensitivity of cryptographic information, special regulations and bodies shall exist within NATO and within each member nation to govern the receipt, control and dissemination of NATO cryptographic information to specially certified persons.

11.18. Special procedures shall also be followed which regulate the sharing of technical information, and which regulate the selection, production and procurement of cryptographic products and mechanisms.

12. EMISSION SECURITY

12.1. Security measures shall be implemented to protect against the compromise of information classified NC and above through unintentional electromagnetic emissions. The measures shall be commensurate with the risk of exploitation and the sensitivity of the information.

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2010)0003-ADD1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

13. SPECIFIC CIS SECURITY RESPONSIBILITIES

13.1. NATO Military Committee (NAMILCOM)

13.1.1. The NAMILCOM's responsibilities on CIS Security include the security approval and release of cryptographic equipment and participating in the evaluation and selection of cryptographic products and mechanisms for standard NATO use. The four nationally manned agencies of the Military Committee (SECAN, DACAN, EUSEC and EUDAC) provide advice and support on CIS Security to the NAMILCOM, to the SC, to the C3B and, as appropriate, to their sub-structures, to member nations and to other NATO organisations.

13.2. C3 Board (C3B)

13.2.1. As the senior Consultation, Command and Control (C3) policy committee within the Alliance, the C3B supports the NAMILCOM and the NATO political authorities in their validation process for C3 capabilities and projects by reviewing operational C3 requirements. The C3B is responsible for the provision of secure and interoperable NATO-wide C3 systems. Staff support to the C3B is provided by the NATO HQ C3 Staff (NHQC3S).

13.3. NATO Cyber Defence Management Board (CDMB)

13.3.1 The CDMB is the cyber defence coordination body providing strategic planning and direction for the implementation of the Cyber Defence Policy and facilitating cooperation with Allies. The CDMB reports to and receive political guidance from the NAC through the Defence Policy and Planning Committee in reinforced format (DPPC(R)). The CDMB is supervised by Allies through the C3B on C3 policy and implementation aspects of cyber defence. CDMB consults on specific subject matters through the appropriate NATO committees.

13.4. National CIS Security Authority (NCSA)

13.4.1. Each NATO and non-NATO nation, where applicable to the latter, shall identify an NCSA, which may be established as an agency in the national security infrastructure. The NCSA is responsible for :

(a) controlling cryptographic technical information related to the protection of NATO information within their nation;

(b) ensuring that cryptographic systems, products and mechanisms for protecting NATO information are appropriately selected, operated and maintained;

(c) ensuring that CIS security products for protecting NATO information are appropriately selected, operated and maintained within their nation;

(d) communicating on NATO communications security and technical matters on CIS Security, both civil and military, with appropriate NATO and national bodies; and

(e) identifying a National TEMPEST Authority, as appropriate.

13.4.2. NCSAs work in co-ordination with their NSA(s).

DECLASSIFIED - PUBLICLY DISCLOSED - PDN(2010)0003-ADD1 - DECLASSIFIE - MISE EN LECTURE PUBLIQUE

13.5. **National Distribution Authority (NDA)**

13.5.1. Each NATO and non-NATO nation, where applicable to the latter, shall identify an NDA, which may be established as an agency in the national security infrastructure, which is responsible for the management of NATO cryptomaterial within their nation and shall ensure that appropriate procedures are enforced and channels established for the comprehensive accounting, secure handling, storage, distribution and destruction of all cryptomaterial.

13.5.2. NDAs work in co-ordination with their NSA(s).

13.6. **Security Accreditation Authority(s)**

13.6.1. Each NATO and non-NATO nation, where applicable to the latter, shall identify a security accreditation authority(s) which is responsible for the security accreditation of the following :

(a) national CIS handling NATO classified information; and

(b) NATO CIS operating within national bodies / organisations, as appropriate for non-NATO Nations.

13.6.2. Where a NATO civil or military body is established within a NATO nation, the NATO CIS shall be subject to security accreditation by a NATO SAA. In this case, the security accreditation may be co-ordinated with the appropriate national security accreditation authority.

13.7. **NATO Security Accreditation Authority (SAA)**

13.7.1. There are three NATO SAAs which are responsible for the security accreditation of NATO CIS handling NATO classified information. The SAA shall be the Director, NATO Office of Security and the Strategic Commanders, or their delegated / nominated representative(s), dependent upon the CIS to be accredited.

13.7.2. The NATO CIS Security Accreditation Board, composed of the NATO SAAs as identified in the paragraph above, shall have security accreditation oversight for all NATO CIS handling NATO classified information to ensure a corporate and consistent approach to security of NATO CIS. The NSAB Terms of Reference shall be subject to approval by the Security Committee.

13.8. **Security Authority for NNN**

13.8.1. The NNN shall appoint a security authority to be responsible for the security provisions of the present Enclosure and the oversight of the NNN Authorities with specific CIS Security responsibilities for national CIS handling NATO classified information (including NCSA, NDA and SAAs).

ENCLOSURE "G"

CLASSIFIED PROJECT AND INDUSTRIAL SECURITY

DECLASSIFIED - PUBLIC DISCLOSURE / DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

INTRODUCTION

1. This Enclosure deals with security aspects of industrial operations that are unique to the negotiation and letting of contracts involving NATO classified information and their performance by industry, including the release of NATO classified information during pre-contract negotiations and contract performance. This Enclosure sets out the security policy for:

(a) the security requirements for tendering, negotiation and letting of contracts involving NATO classified information;

(b) contracts involving NATO classified information with contractors in non-NATO nations

(c) the industrial security clearances for contracts involving NATO classified information (Facility Security Clearances (FSCs) and Personnel Security Clearances (PSC));

(d) the release of NATO classified information in contracting;

(e) the handling of NATO classified information in Communication and Information Systems (CIS);

(f) International Visit Control Procedures (IVCP); and

(g) the international transmission and transportation of NATO classified material;

2. This Enclosure is supported by the Directive on Classified Project and Industrial Security which sets out the detailed requirements and procedures.

TENDERING, NEGOTIATION AND LETTING OF CONTRACTS INVOLVING NATO CLASSIFIED INFORMATION

3. The prime contract for a NATO programme/project shall be negotiated and awarded by a NATO Programme/Project Agency/Office (NPA/NPO). An FSC shall be required for all Contractors involved in contracts that require the Contractor's facility to manage, generate or have access to classified information NATO CONFIDENTIAL (NC) and above. For contracts classified NATO RESTRICTED (NR), an FSC is not required.

4. The NPA/NPO or other contracting authority which initiates the contract shall ensure that Contractor's facilities hold an appropriate FSC for the specific phase of the contract. The contracting authority shall verify that Contractor's personnel accessing classified information NC or above at the premises of the contracting authority hold the appropriate PSC.

DECLASSIFIED - PUBLIC DISCLOSURE / DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

5. After the prime contract has been let, a prime Contractor may negotiate sub-contracts with other Contractors, i.e., Sub-contractors. These Sub-contractors may also negotiate sub-contracts with other Sub-contractors. If these sub-contracts require access to information classified NC and above, the facility and personnel security requirements identified in the "Industrial Security Clearances For NATO Contracts" section of this Enclosure and in the Directive on Classified Project and Industrial Security shall apply. If a potential Sub-contractor is under the jurisdiction[1] of a non-NATO nation *prior* permission to negotiate a sub-contract shall be obtained from the NPA/NPO or other contracting authority respectively. If the NPA/NPO has placed restrictions on the award of contracts to NATO-nations that are not participants in a programme/project, the NPA/NPO shall be requested to consider and give permission prior to contract discussion with contractors from those nations.

6. Upon letting the contract, the NPA/NPO or other contracting authority shall notify the NSA/DSA of the Contractor, and ensure that the Security Aspect Letter (SAL) and/or the Project Security Instruction (PSI), as applicable, is provided to the prime Contractor, with the contract.

SECURITY REQUIREMENTS FOR CONTRACTS INVOLVING NATO CLASSIFIED INFORMATION

7. The prime Contractor and Sub-contractors shall be contractually required, under penalty of termination of their contract, to take all measures prescribed by the NSAs/DSAs for protecting all NATO classified information generated by or entrusted to the Contractor, or embodied in articles manufactured by the Contractor.

(a) Contracts for major programme/projects involving NATO classified information shall contain a PSI as an annex; a "Project Security Classification Guide" shall be a part of the PSI. All other contracts involving NATO classified information shall include, as a minimum, a SAL, which may be a PSI that is reduced in scope. In the latter case, the Programme/Project Security Classification Guide may be referred to as a "Security Classification Checklist".

The PSI supplements the NATO security policies and requirements, establishes specific security procedures associated with the NATO programme/project concerned and assigns responsibilities for the implementation of security measures concerning classified information.

(b) For contracts involving only NR information specific regulations have been established in the Directive on Classified Project and Industrial Security, in particular in its Appendix 4 "Contract Security Clause for Tenders and Contracts involving NATO RESTRICTED Information".

8. The classification for programme/project elements of information associated with possible sub-contracts shall be based on the Programme/Project Security Classification Guide.

---

1 Power to exercise authority over a subject matter or a territory/geographic area

DECLASSIFIED - PUBLIC DISCLOSURE / DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

CONTRACTS INVOLVING NATO CLASSIFIED INFORMATION *WITH CONTRACTORS* IN NON-NATO NATIONS

9. The letting of contracts involving NATO classified information with Contractors in non-NATO nations constitutes release of information and has to be in accordance with Enclosure "E" to C-M(2002)49, the Directive on Security of Information and the Directive on Classified Project and Industrial Security. The release shall always be with the consent of the relevant originator(s).

10. Contracts involving NATO classified information with Contractors in non-NATO nations require the existence of a bilateral Security Agreement/Arrangement between NATO or a contracting/sponsoring NATO nation and the non-NATO nation where the Contractor is under the jurisdiction of a NSA/DSA or other competent authority with the authority to commit the Contractor to provide the required protection. If the contract is governed by a bilateral Security Agreement/Arrangement between a contracting/sponsoring NATO nation and a non-NATO nation, the NATO nation shall provide a written security assurance to NATO confirming that the NATO classified information provided is governed under the scope of that Security Agreement/Arrangement. A copy of the assurance shall be provided to the NOS and the relevant NPO/NPA.

11. The undertaking of placing a contract to a Contractor of a non-NATO nation shall follow the procedures as established in the Directive on Classified Project and Industrial Security.

12. For non-NATO nations, an appropriate security authority(s) shall be identified that fulfils the equivalent functions of the NSA/DSA in a NATO nation.

INDUSTRIAL SECURITY CLEARANCES FOR NATO CONTRACTS

General

13. The policy described in subsequent paragraphs for facilities and individuals apply to contracts and sub-contracts.

Facility Security Clearances (FSC)

14. The NSA/DSA of each NATO nation is responsible for ensuring that any facility under its jurisdiction which will require access to information classified NC and above has adopted the protective security measures necessary to qualify for an FSC. In granting an FSC, the NSA/DSA shall ensure that they have the means to be advised of any circumstances that could have a bearing upon the viability of the clearance granted.

15. The assessment to be made prior to issuing an FSC shall be in accordance with the requirements and criteria set out in the supporting Directive on Classified Project and Industrial Security in addition to any applicable national laws and regulations.

16. A bidder, not holding an appropriate FSC as required by the potential contract/subcontract shall not be automatically excluded from the competition. The contracting authority should make all efforts in restricting the classification level of the information required to be provided to bidders to the lowest possible level still permitting an informed and qualified response to the invitation to tender. However, the tender document shall advise on the requirement for an appropriate FSC prior to the award of the contract/subcontract.

17. Scenarios identifying FSC requirements are provided in the supporting Directive on Classified Project and Industrial Security.

18. An FSC or PSC is not required for contracts or access to information classified NR. A nation which, under its National security laws and regulations, requires an FSC for a contract or sub-contract classified NR shall not discriminate against a Contractor from a nation not requiring an FSC , but shall ensure that the contractor has been informed of its responsibilities in respect to the protection of the information, and obtains an acknowledgement of those responsibilities.

Personnel Security Clearances for Facility Employees

19. The facility's employees who require access to NATO classified information NC and above shall hold an appropriate PSC. The issuing of PSCs shall be in accordance with Enclosure "C" to C-M(2002)49, the Directive on Personnel Security and the Directive on Classified Project and Industrial Security.

20. Applications for the security clearance for employees of Contractor facilities shall be made to the NSA/DSA which is responsible for the facility. In submitting the request for verification or initiation of a PSC, the facility shall include the level of NATO classified information to which the employee will have access.

21. If a facility wishes to employ a citizen of a non-NATO nation in a position that requires access to NATO classified information, it is the responsibility of the NSA/DSA of the nation which has jurisdiction over the hiring facility, to carry out the security clearance procedure prescribed herein, and determine that the individual can be granted access in accordance with the requirements of Enclosure "C", the Directive on Personnel Security and the Directive on Classified Project and Industrial Security.

RELEASE OF NATO CLASSIFIED INFORMATION IN CONTRACTING

22. The release of NATO classified information in contracting can constitute either release to non-NATO Nations and International Organisations or release to non-Programme/Project participants from NATO Nations. The release shall be with the consent of the relevant NPA/NPO and/or originator, as applicable, and in accordance with other relevant enclosures to the NATO Security Policy, the Directive on Security of Information as well as the Directive on Classified Project and Industrial Security.

DECLASSIFIED - PUBLIC DISCLOSURE / DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

DECLASSIFIED - PUBLIC DISCLOSURE / DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

THE HANDLING OF CLASSIFIED INFORMATION IN COMMUNICATION AND INFORMATION SYSTEMS (CIS)

23. Only appropriately security accredited CIS shall be used for the storing, processing or transmitting (called hereafter "handling") of NATO classified information. Enclosure "F" to C-M(2002)49, the "Primary Directive on CIS Security" (AC/35-D/2004), the "INFOSEC Management Directive for CIS" (AC/35-D/2005) and all relevant Technical and Implementation Directives on CIS Security (AC/322 documents) provide further policy and directions for the conformant implementation of CIS handling NATO classified information.

24. The security accreditation of CIS handling NR information may be delegated to Contractors according to national security laws and regulations. Where this delegation is exercised, the relevant NSAs/DSAs/SAAs shall retain the responsibility for the protection of NR information handled by the Contractor and the right to inspect the security measures taken by the Contractors. In addition, the Contractor shall provide the Contracting Authority and, where appropriate, the security authority as established in the Directive on Classified Projects and Industrial Security with a statement of compliance certifying that the CIS handling NR information has been accredited in compliance with the policy on Security within NATO and its supporting directives on CIS Security.

INTERNATIONAL VISIT CONTROL PROCEDURES (IVCP)

25. IVCP apply to international visits by representatives of NATO Nations, NATO Civil and Military Bodies, Contractors and Sub-Contractors involving NATO classified information. They also apply to representatives of a Non NATO Nation including Contractors/Sub-Contractors of such Nation if the Nation has adopted the IVCP.

26. Visits involving access to NATO information classified NC and above or unescorted access to security areas shall be approved by the NSA/DSA. Visits involving access to NU[2] or NR information may be arranged directly between the sending and receiving facility without formal requirements.

27. Detailed arrangements for the conduct of International Visits are laid down in the Directive on Classified Project and Industrial Security.

PERSONNEL ON LOAN WITHIN A NATO PROJECT/ PROGRAMME

28. When an individual who has been cleared for access to NATO classified information is to be loaned from one facility to another in the same NATO programme/project, but in a different NATO nation, the individual's parent facility shall request its NSA/DSA to provide a NATO Personnel Security Clearance Certificate for the individual to the NSA/DSA of the facility to which he is to be loaned. The individual on loan shall be assigned using the international visit request procedures set out in the Directive on Classified Project and Industrial Security, and in accordance with National security laws and regulations.

---

2 NU is not a NATO security classification

DECLASSIFIED - PUBLIC DISCLOSURE / DÉCLASSIFIÉ - MIS EN LECTURE PUBLIQUE

INTERNATIONAL TRANSMISSION AND TRANSPORTATION OF NATO CLASSIFIED MATERIAL

Security Principles Applicable to all Forms of Transportation

29. The following principles shall be enforced when examining proposed security arrangements for the international transportation of consignments of classified material:

(a) security shall be assured at all stages during the transportation and under all circumstances, from the point of origin to the ultimate destination;

(b) the degree of protection accorded to a consignment shall be determined by the highest classification level of material contained within it;

(c) an FSC shall be obtained, where required, for companies providing transportation. In such cases, personnel handling the consignment shall be issued an PSC in compliance with the provisions of this Enclosure;

(d) journeys shall be point-to-point to the extent possible, and shall be completed as quickly as circumstances permit; and

(e) care shall be exercised to arrange routes only through NATO nations. Routes through non-NATO nations should only be undertaken when authorised by the NSA/DSA having jurisdiction over the consignor and in accordance with the supporting Directive on Security of Information.

30. Arrangements for consignments of classified material shall be stipulated for each programme/project. However, such arrangements shall ensure that there is no likelihood of unauthorized access to classified material.

31. The security standards for the international transportation of NATO classified material can be found in the supporting Directive on Security of Information. However, the detailed requirements for the hand carriage of NATO classified material, carriage of classified material by commercial courier companies, security guards and escorts, and the transportation of explosives, propellants or other dangerous substances are set out in the supporting Directive on Classified Project and Industrial Security.

DECLASSIFIED-PUBLICLY DISCLOSED - PDN(2010)0003-ADD1 - DÉCLASSIFIÉ-MIS EN LECTURE PUBLIQUE

GLOSSARY

Accountable Information	All information classified CTS and NS and all Special Category Information (such as ATOMAL).
Authentication	Authentication is the act of verifying the claimed identity of an entity.
Availability	The property of information and material being accessible and usable upon demand by an authorised individual or entity.
Breach of security	An act or omission, deliberate or accidental, contrary to NATO Security Policy and supporting directives, that results in the actual or possible compromise of NATO classified information or supporting services and resources (including, for example, classified information lost while being transported; classified information left in an unsecured area where uncleared persons have unescorted access; an accountable document cannot be found; classified information has been subjected to unauthorised modification; destroyed in an unauthorised manner or, for CIS, there is a denial of service).
Classified Information	Any information (namely, knowledge that can be communicated in any form) or material determined to require protection against unauthorised disclosure and which has been so designated by a security classification.
Communication and Information System Security (CIS Security)	The application of security measures for the protection of communication, information and other electronic systems, and the information that is stored, processed or transmitted in these systems with respect to confidentiality, integrity, availability, authentication and non-repudiation.
Competent Authority	An authority identified by the NSA of a NATO nation which is authorised to carry out personnel security clearances in order to give their nationals access to NATO classified information.
Compromise	Compromise denotes a situation when - due to a breach of security or adverse activity (such as espionage, acts of terrorism, sabotage or theft) - NATO classified information has lost its confidentiality, integrity or availability, or supporting services and resources have lost their integrity or availability. This includes loss, disclosure to unauthorised individuals (e.g. through espionage or to the media) unauthorised modification, destruction in an unauthorised manner, or denial of service.
Confidentiality	The property that information is not made available or disclosed to unauthorised individuals or entities.
Consignee	The contractor, facility or other organisation receiving material from the consignor.
Consignor	The contractor, facility or other organisation responsible for organising and dispatching material.
Contract	A legally enforceable agreement to provide goods or services.

DECLASSIFIED-PUBLICLY DISCLOSED - PDN(2010)0003-ADD1 - DÉCLASSIFIÉ-MIS EN LECTURE PUBLIQUE

Contractor	An industrial, commercial or other entity that agrees to provide goods or services.
Courier	A person officially assigned to hand-carry material.
Cryptomaterial	Includes cryptographic algorithms and cryptographic hardware - and software-modules and products including implementation details and associated documentation and keying material (for both, symmetric and asymmetric cryptographic mechanisms).
Designated Security Authority (DSA)	An authority responsible to the National Security Authority (NSA) of a NATO nation which is responsible for communicating to industry the national policy in all matters of NATO industrial security policy and for providing direction and assistance in its implementation. In some countries, the function of a DSA may be carried out by the NSA.
Document	Any recorded information regardless of its physical form or characteristics, including, without limitation, written or printed matter, data processing cards and tapes, maps, charts, photographs, paintings, drawings, engravings, sketches, working notes and papers, carbon copies or ink ribbons, or reproductions by any means or process, and sound, voice, magnetic or electronic or optical or video recordings in any form, and portable IT equipment with resident computer storage media, and removable computer storage media.
Dynamic risk management	The ability to perform risk management in a way that the risk of using a CIS is continuously assessed, any change in the context in which the CIS operates is reflected in the risk signature dynamically and the security countermeasures, most appropriate to the situation, are applied timely.
Escorts	Armed or unarmed national police, military, or other government personnel. Their function is to facilitate the secure movement of the material, but they do not have direct responsibility in matters of the protection of the material itself.
Facility	An installation, plant, factory, laboratory, office, university or other educational Institution, or commercial undertaking, including any associated warehouses, storage areas, utilities and components which, when related by function and location, form an operating entity.
Facility Security Clearance (FSC)	An administrative determination by a NSA/DSA that, from a security viewpoint, a facility can afford adequate security protection to NATO classified information of a specified classification or below, and its personnel who require access to NATO classified information have been properly cleared and briefed on NATO security requirements necessary to perform on the NATO classified contracts.
Guards	Civilian (Government or participating contractor employees) or military personnel who may be armed or unarmed. They may be assigned for security guard duties only or may combine security guard duties with other duties.

DECLASSIFIED-PUBLICLY DISCLOSED - PDN(2010)0003-ADD1 - DÉCLASSIFIÉ-MIS EN LECTURE PUBLIQUE

Host Nation	General : the nation in which a NATO civil or military body is located. Industrial security : the nation designated by an official body of NATO to act as the governmental agency to contract for the performance of a NATO prime contract. Nations in which sub-contracts are performed are not referred to as host nations.
Information	Knowledge that can be communicated in any form.
Information Assurance	Information shall be protected by applying the principle of Information Assurance, which is described as the set of measures to achieve a given level of confidence in the protection of communication, information and other electronic systems, non-electronic systems, and the information that is stored, processed or transmitted in these systems with respect to confidentiality, integrity, availability, non-repudiation and authentication.
Infraction	A security infraction is an act or omission, deliberate or accidental, contrary to NATO Security Policy and supporting directives that does not result in the actual or possible compromise of NATO classified information. (e.g. classified information left unsecured inside a secure facility where all persons are appropriately cleared, failure to double wrap classified information, etc.).
Integrity	The property that information (including data, such as cipher text) has not been altered or destroyed in an unauthorised manner.
International Visits	Visits made by individuals subject to one NSA/DSA or belonging to a NATO body, to facilities or bodies subject to another NSA/DSA or to NATO, which will require, or may give rise to access to NATO classified information or where, regardless of the level of classification involved, national legislation governing the establishment or body to be visited in support of NATO approved related activities requires that such visits shall be approved by the relevant NSA/DSA. All NATO civil and military bodies fall within the security jurisdiction of NATO.
Life-cycle	Life cycle of information encompasses the stages of planning, collection, creation or generation of information; its organisation, retrieval, use, accessibility and transmission; its storage and protection; and, finally, its disposition through transfer to archives or destruction.
Major Programme/Project	A programme or project of major significance, normally involving more than two nations and security measures that extend beyond the normal basic requirements described in NATO Security Policy.
Material	Material includes documents and also any items of machinery, equipment/components, weapons or tools, either manufactured or in the process of manufacture.
Nationals	Nationals includes “nationals of a Kingdom”, “citizens of a State”, and ”landed immigrants in Canada”. “Landed immigrants in Canada” are individuals who have gone through a national screening process including residency checks, criminal records and security checks, and who are going to obtain lawful permission to establish permanent residence in the nation.

DECLASSIFIED-PUBLICLY DISCLOSED - PDN(2010)0003-ADD1 - DÉCLASSIFIÉ-MIS EN LECTURE PUBLIQUE

National Security Authority (NSA)	An authority of a NATO nation which is responsible for the maintenance of security of NATO classified information in national agencies and elements, military or civil, at home or abroad.
NATO	"NATO" denotes the North Atlantic Treaty Organisation and the bodies governed either by the Agreement on the status of the North Atlantic Treaty Organisation, National Representatives and International Staff, signed in Ottawa on 20th September, 1951 or by the Protocol on the status of International Military Headquarters set up pursuant to the North Atlantic Treaty, signed in Paris on 28th August, 1952.
NATO Classified Contract	Any contract issued by a NATO civil or military body or a NATO member nation in support of a NATO funded or administered programme/project that will require access to or generate NATO classified information.
NATO Classified Information	(a) information means knowledge that can be communicated in any form (b) classified information means information or material determined to require protection against unauthorised disclosure which has been so designated by a security classification (c) the word "material" includes documents and also any items of machinery or equipment or weapons either manufactured or in the process of manufacture (d) the word "document" means any recorded information regardless of its physical form or characteristics, including, without limitation, written or printed matter, data processing cards and tapes, maps, charts, photographs, paintings, drawings, engravings, sketches, working notes and papers, carbon copies or ink ribbons, or reproductions by any means or process, and sound, voice, magnetic or electronic or optical or video recordings in any form, and portable IT equipment with resident computer storage media, and removable computer storage media.
NATO Military Committee (NAMILCOM)	The highest military authority in NATO; the NAMILCOM is responsible for the overall conduct of military affairs. The NAMILCOM is responsible for endorsing and prioritising from an operational point of view the users' requirements submitted by Strategic Commanders.
NATO Personnel Security Clearance	A determination that an individual is eligible to have access to NATO classified information.
NATO Production and Logistics Organisation (NPLO)	A subsidiary body, created within the framework of NATO for the implementation of tasks arising from that Treaty, to which North Atlantic Council grants clearly defined organisational, administrative and financial independence. It shall be comprised of a board of directors; and an executive body, composed of a General Manager and staff.
NATO Programme	A Council approved programme that is administered by a NATO management /office under NATO regulations.
NATO Project	A Council approved project that is administered by a NATO management agency/office under NATO regulations.

DECLASSIFIED-PUBLICLY DISCLOSED - PDN(2010)0003-ADD1 - DÉCLASSIFIÉ-MIS EN LECTURE PUBLIQUE

NATO Project Management Agency	The executive body of a NPLO.
Need-to-know	See under “Principle of Need-to-know”.
Negotiations	The term encompasses all aspects of awarding a contract or sub-contract from the initial “notification of intention to call for bids” to the final decision to let a contract or sub-contract.
Non-repudiation	The measure of assurance to the recipient that shows that information was sent by a particular person or organisation and to the sender that shows that information has been received by the intended recipients
Open Storage Area	An area, constructed in accordance with security requirements and authorized by the head of the civil or military body for open storage of classified information.
Originator	The nation or international organisation under whose authority information has been produced or introduced into NATO.
Parent Nation	The Kingdom of which an individual is a national, or the state of which an individual is a citizen.
Parent National Security Authority (NSA)	The NSA of the Kingdom of which an individual is a national, or the state of which an individual is a citizen.
Personnel Security Clearance (PSC)	A determination that an individual is eligible to have access to classified information.
Prime Contract	The initial contract led by a NATO Project Management / Agency / Office for a Programme/project.
Prime Contractor	An industrial, commercial or other entity of a member nation which has contracted with a NATO Project Management Agency/Office to perform a service, or manufacture a product, in the framework of a NATO project, and which, in turn, may subcontract with potential sub-contractors as approved.
Principle of Need-to-know	The principle according to which a positive determination is made that a prospective recipient has a requirement for access to, knowledge of, or possession of information in order to perform official tasks or services.
Programme/Project Security Classification Guide	Part of the program (project) security instructions (PSI) which identifies the elements of the program that are classified, specifying the security classification levels. The security classification guide may be expanded throughout the program life cycle, and the elements of information may be re-classified or downgraded.
Programme/Project Security Instruction (PSI)	A compilation of security regulations/procedures, based upon NATO Security Policy and supporting directives, which are applied to a specific project/programme in order to standardise security procedures. The PSI also constitutes an Annex to the main contract, and may be revised throughout the program lifecycle. For sub-contracts let within the program, the PSI constitutes the basis for the SAL.

DECLASSIFIED-PUBLICLY DISCLOSED - PDN(2010)0003-ADD1 - DÉCLASSIFIÉ-MIS EN LECTURE PUBLIQUE

Risk	The likelihood of a vulnerability being successfully exploited by a threat, leading to a compromise of confidentiality, integrity and/or availability and damage being sustained.
Risk management	A systematic approach to determining which security counter-measures are required to protect information and supporting services and resources, based upon an assessment of the threats and vulnerabilities. Risk management involves planning, organising, directing and controlling resources to ensure that the risk remains within acceptable bounds.
Security Aspects Letter (SAL)	A document, issued by the appropriate authority, as part of any NATO classified contract or sub-contract, other than Major Programmes/Projects, identifying the security requirements or those elements thereof requiring security protection.
Security Assurance	A guarantee provided to NATO either directly or through a NATO nation or NATO civil or military body sponsoring release, that a non-NATO recipient of NATO classified information will provide the same degree of protection to it as required by NATO Security Policy.
Security Classification Check List	Part of a security aspect letter (SAL) which describes the elements of a contract that are classified, specifying the security classification levels. In case of contracts let within a program/project, such elements of information derive from the programme (project) security instructions issued for that programme.
Special Category Information	Information such as ATOMAL or Single Integrated Operational Plan (SIOP) to which additional handling/protection procedures are applied.
Sub-contract	A contract entered into by a prime contractor with another contractor (i.e., the sub-contractor) for the furnishing of goods or services.
Sub-contractor	A contractor to whom a prime contractor lets a sub-contract.
Threat	The potential for compromise, loss or theft of NATO classified information or supporting services and resources. A threat may be defined by its source, motivation or result, it may be deliberate or accidental, violent or surreptitious, external or internal.
Vulnerability	A weakness, an attribute, or lack of control that would allow or facilitate a threat actuation against NATO classified information or supporting services and resources.

DÉCISION (UE, Euratom) 2015/444 DE LA COMMISSION

du 13 mars 2015

concernant les règles de sécurité aux fins de la protection des informations classifiées de l'Union européenne

LA COMMISSION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 249,

vu le traité instituant la Communauté européenne de l'énergie atomique, et notamment son article 106,

vu le protocole n° 7 sur les privilèges et immunités de l'Union européenne annexé aux traités, et notamment son article 18,

considérant ce qui suit:

(1) Les dispositions de la Commission en matière de sécurité concernant la protection des informations classifiées de l'Union européenne (ICUE) doivent être révisées et actualisées, en tenant compte des évolutions institutionnelles, organisationnelles, opérationnelles et technologiques.

(2) La Commission européenne a signé des accords en matière de sécurité pour ses principaux sites avec les gouvernements belge, luxembourgeois et italien ([1]).

(3) La Commission, le Conseil et le Service européen pour l'action extérieure sont résolus à appliquer des normes équivalentes de sécurité pour protéger les ICUE.

(4) Il importe d'associer, le cas échéant, le Parlement européen et d'autres institutions, agences, organes ou organismes de l'Union aux principes, aux normes et à la réglementation relatifs à la protection des informations classifiées qui sont nécessaires pour protéger les intérêts de l'Union et de ses États membres.

(5) Les risques pesant sur les ICUE sont gérés dans le cadre d'une procédure. Cette dernière vise à déterminer les risques connus pesant sur la sécurité, à définir des mesures de sécurité permettant de ramener ces risques à un niveau acceptable conformément aux principes de base et aux normes minimales énoncés dans la présente décision et à appliquer ces mesures selon la notion de défense en profondeur. L'efficacité de telles mesures fait l'objet d'une évaluation constante.

(6) Au sein de la Commission, la sécurité physique visant à protéger les informations classifiées correspond à l'application de mesures physiques et techniques de protection pour empêcher l'accès non autorisé aux ICUE.

(7) La gestion des ICUE correspond à l'application de mesures administratives pour contrôler les ICUE tout au long de leur cycle de vie afin de compléter les mesures prévues aux chapitres 2, 3 et 5 de la présente décision et de contribuer ainsi à la dissuasion, à la détection et au retour aux conditions opérationnelles dans le cadre de la compromission ou de la perte délibérée ou accidentelle de telles informations. Ces mesures concernent en particulier la création, la conservation, l'enregistrement, la duplication, la traduction, le déclassement, la déclassification, le transport et la destruction des ICUE et elles complètent les règles générales de la Commission relatives à la gestion des documents [décisions 2002/47/CE, CECA, Euratom ([2]) et 2004/563/CE, Euratom ([3])].

([1]) Voir Arrangement entre le Gouvernement belge et le Parlement européen, le Conseil, la Commission, le Comité économique et social européen, le Comité des régions, la Banque européenne d'investissement en matière de sécurité du 31 décembre 2004, Accord de sécurité signé entre la Commission et le Gouvernement luxembourgeois du 20 janvier 2007, et Accordo tra il Governo italiano e la Commissione europea dell'energia atomica (Euratom) per l'istituzione di un Centro comune di ricerche nucleari di competenza generale du 22 juillet 1959.

([2]) Décision 2002/47/CE, CECA, Euratom de la Commission du 23 janvier 2002 modifiant son règlement intérieur (JO L 21 du 24.1.2002, p. 23).

([3]) Décision 2004/563/CE, Euratom de la Commission du 7 juillet 2004 modifiant son règlement intérieur (JO L 251 du 27.7.2004, p. 9).

(8) La présente décision est arrêtée sans préjudice des règlements suivants:

a) règlement (Euratom) n° 3 ([1]);

b) règlement (CE) n° 1049/2001 du Parlement européen et du Conseil ([2]);

c) règlement (CE) n° 45/2001 du Parlement européen et du Conseil ([3]);

d) règlement (CEE, Euratom) n° 354/83 du Conseil ([4]),

A ADOPTÉ LA PRÉSENTE DÉCISION:

CHAPITRE PREMIER

PRINCIPES DE BASE ET NORMES MINIMALES

Article premier

Définitions

Aux fins de la présente décision, on entend par:

1) «service de la Commission», l'une des directions générales ou l'un des services de la Commission ou l'un des cabinets des membres de la Commission;

2) «matériel cryptographique», les algorithmes cryptographiques, les modules matériels et logiciels cryptographiques, et les produits comprenant les modalités de mise en œuvre et la documentation y relative, ainsi que les éléments de mise à la clé;

3) «déclassification», la suppression de toute classification de sécurité;

4) «défense en profondeur», l'application d'un éventail de mesures de sécurité organisées en plusieurs niveaux de défense;

5) «document», toute information enregistrée quelles que soient sa forme ou ses caractéristiques physiques;

6) «déclassement», le passage à un niveau de classification de sécurité inférieur;

7) «traitement» d'ICUE, l'ensemble des actions dont les ICUE sont susceptibles de faire l'objet tout au long de leur cycle de vie. Sont ainsi visés leur création, leur enregistrement, leur traitement, leur transport, leur déclassement, leur déclassification et leur destruction. En ce qui concerne les systèmes d'information et de communication (SIC), sont en outre compris leur collecte, leur affichage, leur transmission et leur stockage;

8) «détenteur», une personne dûment autorisée qui, sur la base d'un besoin d'en connaître avéré, est en possession d'un élément d'ICUE et à laquelle il incombe par conséquent d'en assurer la protection;

9) «modalités d'application», tout ensemble de dispositions ou notes de sécurité adoptées conformément au chapitre 5 de la décision de la Commission (UE, Euratom) 2015/443 ([5]);

10) «matériel», tout média, support de données ou élément de machine ou d'équipement, déjà fabriqué ou en cours de fabrication;

11) «autorité d'origine», l'institution, l'organe ou l'agence de l'Union, l'État membre, l'État tiers ou l'organisation internationale sous l'autorité duquel/de laquelle les informations classifiées ont été créées et/ou introduites dans les structures de l'Union;

12) «locaux», tous les biens et possessions immeubles et assimilés de la Commission;

([1]) Règlement (Euratom) n° 3 du 31 juillet 1958 portant application de l'article 24 du traité instituant la Communauté européenne de l'énergie atomique (JO 17 du 6.10.1958, p. 406/58).

([2]) Règlement (CE) n° 1049/2001 du Parlement européen et du Conseil du 30 mai 2001 relatif à l'accès du public aux documents du Parlement européen, du Conseil et de la Commission (JO L 145 du 31.5.2001, p. 43).

([3]) Règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données (JO L 8 du 12.1.2001, p. 1).

([4]) Règlement (CEE, Euratom) n° 354/83 du Conseil du 1er février 1983 concernant l'ouverture au public des archives historiques de la Communauté économique européenne et de la Communauté européenne de l'énergie atomique (JO L 43 du 15.2.1983, p. 1).

([5]) Décision de la Commission (UE, Euratom) 2015/443 du 13 mars 2015 relative à la sécurité au sein de la Commission (voir page 41 du présent Journal officiel).

13) «procédure de gestion des risques de sécurité», l'ensemble de la procédure consistant à identifier, contrôler et limiter les événements aléatoires susceptibles d'avoir des répercussions sur la sécurité d'une organisation ou de tout système qu'elle utilise. La procédure couvre l'ensemble des activités liées aux risques, y compris l'évaluation, le traitement, l'acceptation et la communication;

14) «statut», le statut des fonctionnaires de l'Union européenne et le régime applicable aux autres agents de l'Union européenne, énoncés dans le règlement (CEE, Euratom, CECA) n° 259/68 du Conseil ([1]);

15) «menace», la cause potentielle d'un incident non souhaité susceptible de porter atteinte à une organisation ou à tout système qu'elle utilise. Les menaces peuvent être accidentelles ou délibérées (malveillantes); elles sont caractérisées par des éléments menaçants, des cibles potentielles et des méthodes d'attaque;

16) «vulnérabilité», toute faiblesse de quelque nature que ce soit dont une ou plusieurs menaces est susceptible de tirer parti pour se concrétiser. La vulnérabilité peut résulter d'une omission ou être liée à un contrôle défaillant en termes de rigueur, d'exhaustivité ou d'homogénéité; elle peut être de nature technique, procédurale, physique, organisationnelle ou opérationnelle.

Article 2

Objet et champ d'application

1. La présente décision définit les principes de base et les normes de sécurité minimales pour la protection des ICUE.

2. La présente décision s'applique à tous les services de la Commission et dans l'ensemble des locaux de la Commission.

3. Nonobstant toute indication spécifique concernant des groupes particuliers de personnel, la présente décision s'applique aux membres de la Commission, au personnel de la Commission couvert par le statut et par le régime applicable aux autres agents de l'Union européenne, aux experts nationaux détachés auprès de la Commission (END), aux prestataires de services et à leur personnel, aux stagiaires et à toute personne ayant accès aux bâtiments et autres propriétés de la Commission, ou à des informations gérées par la Commission.

4. Les dispositions de la présente décision s'appliquent sans préjudice de la décision 2002/47/CE, CECA, Euratom et de la décision 2004/563/CE, Euratom.

Article 3

Définition des ICUE, classifications et marquages de sécurité

1. Par «informations classifiées de l'Union européenne» (ICUE), on entend toute information ou tout matériel identifié comme tel par la classification de sécurité de l'Union européenne, dont la divulgation non autorisée pourrait porter atteinte à des degrés divers aux intérêts de l'Union européenne, ou à ceux d'un ou de plusieurs de ses États membres.

2. Les ICUE relèvent de l'un des niveaux de classification suivants:

a) TRÈS SECRET UE/EU TOP SECRET: informations et matériels dont la divulgation non autorisée pourrait causer un préjudice exceptionnellement grave aux intérêts essentiels de l'Union européenne ou d'un ou de plusieurs de ses États membres;

b) SECRET UE/EU SECRET: informations et matériels dont la divulgation non autorisée pourrait nuire gravement aux intérêts essentiels de l'Union européenne ou d'un ou de plusieurs de ses États membres;

c) CONFIDENTIEL UE/EU CONFIDENTIAL: informations et matériels dont la divulgation non autorisée pourrait nuire aux intérêts essentiels de l'Union européenne ou d'un ou de plusieurs de ses États membres;

d) RESTREINT UE/EU RESTRICTED: informations et matériels dont la divulgation non autorisée pourrait être défavorable aux intérêts de l'Union européenne ou d'un ou de plusieurs de ses États membres.

3. Les ICUE portent un marquage de classification de sécurité conformément au paragraphe 2. Elles peuvent porter des marquages supplémentaires, qui ne sont pas des marquages de classification mais sont destinés à désigner le domaine d'activité auquel elles sont liées, identifier l'autorité d'origine, limiter la diffusion, restreindre l'utilisation ou indiquer la communicabilité.

([1]) Règlement (CEE, Euratom, CECA) n° 259/68 du Conseil, du 29 février 1968, fixant le statut des fonctionnaires des Communautés européennes ainsi que le régime applicable aux autres agents de ces Communautés, et instituant des mesures particulières temporairement applicables aux fonctionnaires de la Commission (régime applicable aux autres agents) (JO L 56 du 4.3.1968, p. 1).

Article 4

Gestion de la classification

1. Chaque membre de la Commission ou service de la Commission veille à ce que les ICUE qu'il crée soient classifiées de manière appropriée, clairement identifiées en tant qu'ICUE, et qu'elles ne conservent leur niveau de classification qu'aussi longtemps que nécessaire.

2. Sans préjudice de l'article 26 ci-après, les ICUE ne sont pas déclassées ni déclassifiées, et aucun des marquages de classification de sécurité visés à l'article 3, paragraphe 2, n'est modifié ni supprimé sans le consentement écrit préalable de l'autorité d'origine.

3. Le cas échéant, des modalités d'application sur le traitement des ICUE, comprenant un guide pratique de la classification, sont adoptées conformément à l'article 60 ci-après.

Article 5

Protection des informations classifiées

1. Les ICUE sont protégées conformément à la présente décision et à ses modalités d'application.

2. Il incombe au détenteur de tout élément d'ICUE de le protéger conformément à la présente décision et à ses modalités d'application, conformément aux dispositions prévues au chapitre 4 ci-après.

3. Lorsque les États membres introduisent des informations classifiées portant un marquage national de classification de sécurité dans les structures ou réseaux de la Commission, cette dernière protège ces informations conformément aux règles applicables aux ICUE de niveau équivalent tel que prévu dans le tableau d'équivalence des classifications de sécurité figurant à l'annexe I.

4. Un ensemble d'ICUE peut justifier un niveau de protection correspondant à une classification plus élevée que celle appliquée à ses différentes composantes.

Article 6

Gestion des risques de sécurité

1. Les mesures de sécurité pour la protection des ICUE tout au long de leur cycle de vie sont proportionnées en particulier à leur classification de sécurité, à la forme sous laquelle se présentent les informations ou les matériels ainsi qu'à leur volume, au lieu et à la construction des établissements où se trouvent des ICUE et à la menace évaluée à l'échelle locale que représentent les activités malveillantes et/ou criminelles, y compris l'espionnage, le sabotage et le terrorisme.

2. Les plans d'urgence tiennent compte de la nécessité de protéger les ICUE en cas d'urgence afin de prévenir l'accès et la divulgation non autorisés ainsi que la perte d'intégrité ou de disponibilité.

3. Les mesures de prévention et de retour aux conditions opérationnelles visant à limiter l'impact de défaillances ou d'incidents graves sur le traitement et le stockage des ICUE sont prévues dans les plans de continuité de l'activité de tous les services.

Article 7

Mise en œuvre de la présente décision

1. Le cas échéant, les modalités d'application en complément ou à l'appui de la présente décision sont adoptées conformément à l'article 60 ci-après.

2. Les services de la Commission prennent toutes les mesures nécessaires dans le cadre leur responsabilité pour veiller à ce que, lors du traitement ou de la conservation des ICUE ou de toute autre information classifiée, la présente décision et les modalités d'application correspondantes soient appliquées.

3. Les mesures de sécurité prises en application de la présente décision sont conformes aux principes en matière de sécurité au sein de la Commission énoncés à l'article 3 de la décision (UE, Euratom) 2015/443.

4. Le directeur général des ressources humaines et de la sécurité met en place l'autorité de sécurité de la Commission au sein de la direction générale des ressources humaines et de la sécurité. L'autorité de sécurité de la Commission assume les responsabilités qui lui sont assignées par la présente décision et ses modalités d'application.

5. Au sein de chaque service de la Commission, le responsable local de la sécurité (LSO), visé à l'article 20 de la décision (UE, Euratom) 2015/443, assume les responsabilités générales suivantes aux fins de la protection des ICUE, conformément à la présente décision, en coopération étroite avec la direction générale des ressources humaines et de la sécurité:

a) gestion des demandes d'autorisations de sécurité pour le personnel;

b) contribution aux réunions de formation et de sensibilisation sur la sécurité;

c) supervision de l'agent contrôleur (RCO) du service;

d) dénonciation des infractions à la sécurité et de la compromission des ICUE;

e) conservation des clés de rechange et du relevé de chaque combinaison;

f) exécution d'autres tâches en relation avec la protection des ICUE ou définies par les modalités d'application.

Article 8

Infractions à la sécurité et compromission des ICUE

1. Une infraction à la sécurité est un acte ou une omission commis par une personne qui est contraire aux règles de sécurité énoncées dans la présente décision et ses modalités d'application.

2. Il y a compromission lorsque, à la suite d'une infraction à la sécurité, des ICUE ont été divulguées en totalité ou en partie à des personnes non autorisées.

3. Toute infraction à la sécurité, réelle ou présumée, est immédiatement signalée à l'autorité de sécurité de la Commission.

4. Lorsqu'il est avéré ou qu'il existe des motifs raisonnables de supposer que des ICUE ont été compromises ou perdues, une enquête de sécurité est menée conformément à l'article 13 de la décision (UE, Euratom) 2015/443.

5. Toutes les mesures appropriées sont prises pour:

a) en informer l'autorité d'origine;

b) faire en sorte qu'une enquête soit menée par des membres du personnel n'étant pas directement concernés par l'infraction afin d'établir les faits;

c) évaluer le préjudice éventuel causé aux intérêts de l'Union ou des États membres;

d) éviter que les faits ne se reproduisent; et

e) informer les autorités compétentes des mesures prises.

6. Toute personne responsable d'une violation des règles de sécurité énoncées dans la présente décision est passible d'une sanction disciplinaire conformément au statut. Toute personne responsable de la compromission ou de la perte d'ICUE est passible de sanctions disciplinaires et/ou peut faire l'objet d'une action en justice conformément aux dispositions législatives et réglementaires applicables.

CHAPITRE 2

MESURES DE SÉCURITÉ CONCERNANT LE PERSONNEL

Article 9

Définitions

Aux fins du présent chapitre, les définitions suivantes sont applicables:

1) Par «autorisation d'accès aux ICUE», on entend une décision de l'autorité de sécurité de la Commission prise en fonction d'une assurance donnée par une autorité compétente d'un État membre attestant qu'un fonctionnaire de la Commission, un autre agent ou un expert national détaché peut, pour autant que son besoin d'en connaître ait été établi et qu'il ait été correctement informé des responsabilités qui lui incombent en la matière, être autorisé à avoir accès aux ICUE jusqu'à un niveau de classification donné (CONFIDENTIEL UE/EU CONFIDENTIAL ou supérieur) jusqu'à une date donnée; l'individu en question est alors «autorisé sécurité».

2) Par «autorisation de sécurité du personnel», on entend l'application de mesures visant à faire en sorte que l'accès aux ICUE ne soit accordé qu'aux personnes qui ont:

a) un besoin d'en connaître,

b) fait l'objet d'une autorisation de sécurité du niveau correspondant, lorsqu'il y a lieu, et

c) été informées de leurs responsabilités.

3) Par «habilitation de sécurité du personnel» (HSP), on entend une déclaration émanant d'une autorité compétente d'un État membre établie à la suite d'une enquête de sécurité menée par les autorités compétentes d'un État membre et attestant qu'une personne peut, pour autant que son besoin d'en connaître ait été établi et qu'elle ait été correctement informée des responsabilités qui lui incombent en la matière, être autorisée à avoir accès aux ICUE jusqu'à un niveau de classification donné (CONFIDENTIEL UE/EU CONFIDENTIAL ou supérieur) jusqu'à une date donnée.

4) Par «certificat d'habilitation de sécurité du personnel» (CHSP), on entend un certificat délivré par une autorité compétente attestant qu'une personne détient une habilitation de sécurité valable ou une autorisation de sécurité délivrée par l'autorité de sécurité de la Commission, indiquant le niveau de classification des ICUE auxquelles la personne peut être autorisée à avoir accès (CONFIDENTIEL UE/EU CONFIDENTIAL ou supérieur), la durée de validité de l'habilitation ou autorisation de sécurité correspondante et la date d'expiration du certificat.

5) Par «enquête de sécurité», on entend les procédures d'enquête menées par l'autorité compétente d'un État membre, dans le respect de ses dispositions législatives et réglementaires nationales, en vue d'obtenir l'assurance qu'il n'existe pas de renseignements défavorables de nature à empêcher une personne d'obtenir une habilitation de sécurité jusqu'à un niveau déterminé (CONFIDENTIEL UE/EU CONFIDENTIAL ou supérieur).

Article 10

Principes de base

1. Une personne ne peut se voir accorder l'accès à des ICUE qu'après:

(1) que son besoin d'en connaître a été établi;

(2) avoir été informée des règles de sécurité applicables à la protection des ICUE ainsi que des normes et lignes directrices correspondantes en matière de sécurité, et avoir reconnu les responsabilités qui lui incombent en matière de protection de ces informations; et

(3) pour les informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur, s'être vu accorder une autorisation de sécurité du niveau correspondant ou avoir été dûment autorisée en vertu de ses fonctions conformément aux dispositions législatives et réglementaires nationales.

2. Toutes les personnes qui, en raison de leurs attributions, peuvent avoir besoin d'accéder à des ICUE CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur font l'objet d'une autorisation de sécurité du niveau correspondant avant que l'accès à de telles ICUE ne leur soit accordé. La personne concernée consent par écrit à se soumettre à la procédure d'habilitation de sécurité concernant le personnel. Dans le cas contraire, cette personne ne peut être affectée à un poste, une fonction ou une tâche requérant l'accès des informations classifiées de niveau CONFIDENTIEL UE/EU CONFIDENTIAL ou supérieur.

3. Les procédures d'habilitation de sécurité concernant le personnel ont pour but de déterminer si une personne, compte tenu de sa loyauté, de son intégrité et de sa fiabilité, peut être autorisée à avoir accès à des ICUE.

4. Il convient d'établir, au moyen d'une enquête de sécurité, la loyauté, l'intégrité et la fiabilité d'une personne aux fins de l'octroi d'une habilitation de sécurité lui permettant d'accéder à des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur; cette enquête est menée par les autorités compétentes d'un État membre conformément aux dispositions législatives et réglementaires nationales.

5. L'autorité de sécurité de la Commission assume seule la responsabilité de se mettre en relation avec les autorités nationales de sécurité (ANS) ou d'autres autorités nationales compétentes pour toutes les questions relevant de l'habilitation de sécurité. Tous les contacts entre les services de la Commission et leur personnel d'une part et les ANS ou autres autorités compétentes d'autre part doivent passer par l'autorité de sécurité de la Commission.

Article 11

Procédure d'autorisation de sécurité

1. Il appartient à chaque directeur général ou chef de service au sein de la Commission de répertorier, au sein de son service, les postes nécessitant l'accès à des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur pour s'acquitter de leurs tâches et exigeant par conséquent une autorisation de sécurité.

2. Dès lors qu'il a connaissance de la nomination d'une personne à un poste nécessitant l'accès à des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur, le responsable local de la sécurité (LSO) du service de la Commission concerné informe l'autorité de sécurité de la Commission, qui transmet à cette personne le questionnaire d'habilitation de sécurité délivré par l'ANS de l'État membre dont est ressortissant l'intéressé nommé en tant que membre du personnel des institutions européennes. La personne concernée consent par écrit à se soumettre à la procédure d'habilitation de sécurité et renvoie le questionnaire rempli dans les plus brefs délais à l'autorité de sécurité de la Commission.

3. L'autorité de sécurité de la Commission transmet le questionnaire d'habilitation de sécurité rempli à l'ANS de l'État membre dont est ressortissant l'intéressé nommé en tant que membre du personnel des institutions européennes et demande qu'il soit procédé à une enquête de sécurité pour le niveau de classification des ICUE auxquelles cette personne devra avoir accès.

4. Si des informations utiles à une enquête de sécurité sont portées à la connaissance de l'autorité de sécurité de la Commission concernant une personne ayant demandé une habilitation de sécurité, l'autorité de sécurité de la Commission, agissant conformément à la réglementation applicable, en avertit l'ANS compétente.

5. À l'issue de l'enquête de sécurité, et dès que possible après avoir été informée par l'ANS compétente de son évaluation générale des conclusions de l'enquête en question, l'autorité de sécurité de la Commission:

a) peut accorder à l'intéressé l'autorisation d'accéder à des ICUE jusqu'au niveau de classification correspondant jusqu'à une date qu'elle détermine elle-même, mais n'excédant pas une durée de 5 ans, lorsque les résultats de l'enquête de sécurité permettent d'obtenir l'assurance qu'il n'existe pas de renseignements défavorables de nature à mettre en doute la loyauté, l'intégrité et la fiabilité de l'intéressé;

b) lorsque le résultat de l'enquête de sécurité ne permet pas d'obtenir cette assurance, conformément à la règlementation applicable, informe l'intéressé, qui peut demander à être entendu par l'autorité de sécurité de la Commission; celle-ci peut à son tour demander à l'ANS compétente tout éclaircissement complémentaire qu'elle est en mesure de donner conformément à ses dispositions législatives et réglementaires nationales. En cas de confirmation des résultats de l'enquête, il n'est pas accordé d'autorisation aux fins de l'accès à des ICUE.

6. L'enquête de sécurité et ses résultats obéissent aux dispositions législatives et réglementaires en vigueur dans l'État membre concerné, y compris celles relatives aux recours. Les décisions de l'autorité de sécurité de la Commission sont susceptibles de recours conformément au statut.

7. La Commission acceptera l'autorisation d'accès à des ICUE octroyée par toute autre institution, organe ou agence de l'Union, pour autant qu'elle reste valable. Les autorisations couvriront toute fonction exercée par l'intéressé au sein de la Commission. L'institution, l'organe ou l'agence de l'Union dans lequel la personne prend ses fonctions signalera le changement d'employeur à l'ANS concernée.

8. Si l'intéressé n'entame pas sa période de service dans un délai de douze mois à compter de la notification des conclusions de l'enquête de sécurité à l'autorité de sécurité de la Commission ou si cette période de service connaît une interruption de douze mois au cours de laquelle l'intéressé n'occupe pas de poste au sein de la Commission, d'une autre institution, organe ou agence de l'Union ou d'une administration nationale d'un État membre, l'autorité de sécurité de la Commission en réfère à l'ANS compétente afin que celle-ci confirme que l'habilitation de sécurité reste valable et pertinente.

9. Si des informations sont portées à la connaissance de l'autorité de sécurité de la Commission concernant un risque de sécurité que représente une personne titulaire d'une autorisation de sécurité valide, l'autorité de sécurité, agissant conformément à la réglementation applicable, en avertit l'ANS compétente.

10. Lorsqu'une ANS notifie à l'autorité de sécurité de la Commission que l'assurance visée au paragraphe 5, point a), n'est plus fournie concernant une personne titulaire d'une autorisation valide d'accès à des ICUE, l'autorité de sécurité de la Commission peut demander à l'ANS concernée tout éclaircissement qu'elle est en mesure de donner dans le respect de ses dispositions législatives et réglementaires nationales. Si les informations défavorables sont confirmées par l'ANS compétente, l'autorisation de sécurité est retirée et la personne concernée n'est plus autorisée à avoir accès aux ICUE, ni à des postes où un tel accès est possible et où elle pourrait nuire à la sécurité.

11. Toute décision de retirer ou suspendre une autorisation d'accès à des ICUE à une personne entrant dans le champ d'application de la présente décision et, s'il y a lieu, les raisons la justifiant sont communiquées à la personne concernée, qui peut demander à être entendue par l'autorité de sécurité de la Commission. Les informations communiquées par une ANS sont soumises aux dispositions législatives et réglementaires en vigueur dans l'État membre concerné. Les décisions prises dans ce contexte par l'autorité de sécurité de la Commission sont susceptibles de recours conformément au statut.

12. Les services de la Commission veillent à ce que les experts nationaux détachés auprès d'eux pour occuper un poste nécessitant une autorisation de sécurité pour accéder à des ICUE présentent, avant de prendre leurs fonctions, une HSP ou un certificat d'habilitation de sécurité du personnel (CHSP) valable, conformément aux dispositions législatives et réglementaires nationales, à l'autorité de sécurité de la Commission qui, sur cette base, délivre une autorisation de sécurité pour l'accès aux ICUE jusqu'au niveau équivalent à celui indiqué dans l'habilitation de sécurité nationale, avec une validité maximale couvrant la durée de leur mission.

Accès à des ICUE pour les personnes dûment autorisées en vertu de leurs fonctions

13. Les membres de la Commission, qui ont accès aux ICUE en vertu de leurs fonctions conformément au traité, sont informés de leurs obligations en matière de sécurité en ce qui concerne la protection des ICUE.

Registres des habilitations de sécurité et des autorisations de sécurité

14. L'autorité de sécurité de la Commission tient des registres des habilitations de sécurité et des autorisations accordées aux fins de l'accès à des ICUE, conformément à la présente décision. Ces registres contiennent au minimum le niveau de classification des ICUE auxquelles l'intéressé peut se voir accorder l'accès, la date à laquelle l'habilitation de sécurité a été délivrée et sa durée de validité.

15. L'autorité de sécurité de la Commission peut délivrer un CHSP précisant le niveau de classification des ICUE auxquelles l'intéressé peut se voir accorder l'accès (CONFIDENTIEL UE/EU CONFIDENTIAL ou un niveau supérieur), la durée de validité de l'autorisation d'accès à des ICUE correspondante et la date d'expiration du certificat proprement dit.

Renouvellement des autorisations de sécurité

16. Après la première délivrance d'une autorisation de sécurité et pour autant que l'intéressé ait accompli une période de service ininterrompue auprès de la Commission européenne ou d'une autre institution, organe ou agence de l'Union et qu'il ait toujours besoin d'avoir accès aux ICUE, l'autorisation de sécurité pour l'accès aux ICUE est réexaminée en vue de son renouvellement, généralement tous les cinq ans à compter de la date de notification des conclusions de la dernière enquête de sécurité sur laquelle elle était fondée.

17. L'autorité de sécurité de la Commission peut prolonger la validité de l'autorisation de sécurité existante pour une période de douze mois au maximum, pour autant que l'ANS compétente ou une autre autorité nationale compétente n'ait reçu aucun renseignement défavorable dans un délai de deux mois à compter de la date de transmission de la demande de renouvellement et du questionnaire d'habilitation de sécurité correspondant. Si, à la fin de cette période de douze mois, l'ANS compétente ou une autre autorité nationale compétente n'a pas notifié son avis à l'autorité de sécurité de la Commission, l'intéressé est affecté à des fonctions qui ne nécessitent pas d'autorisation de sécurité.

Article 12

Réunions d'information sur les autorisations de sécurité

1. Après avoir participé à la réunion d'information sur les autorisations de sécurité organisée par l'autorité de sécurité de la Commission, toutes les personnes auxquelles a été délivrée une autorisation de sécurité reconnaissent par écrit qu'elles sont conscientes de leurs obligations en matière de protection des ICUE et des conséquences qui pourraient résulter si des ICUE devaient être compromises. L'autorité de sécurité de la Commission tient un registre de ces déclarations écrites.

2. Toutes les personnes autorisées à avoir accès aux ICUE ou tenues de les traiter sont averties dans un premier temps et périodiquement informées par la suite des menaces pesant sur la sécurité, et elles doivent rendre compte immédiatement à l'autorité de sécurité de la Commission de toute démarche ou activité qu'elles jugent suspecte ou inhabituelle.

3. Toutes les personnes qui cessent d'exercer des fonctions nécessitant un accès aux ICUE sont informées, et le cas échéant reconnaissent par écrit, qu'elles ont l'obligation de continuer à protéger les ICUE.

Article 13

Autorisations de sécurité temporaires

1. Dans des circonstances exceptionnelles, lorsque cela est dûment justifié dans l'intérêt du service et en attendant l'achèvement de l'enquête de sécurité complète, l'autorité de sécurité de la Commission peut, après avoir consulté l'ANS de l'État membre dont l'intéressé est ressortissant et sous réserve des résultats des vérifications préliminaires effectuées pour s'assurer de l'absence d'informations défavorables pertinentes, accorder à titre temporaire l'autorisation d'accéder à des ICUE pour une fonction déterminée, sans préjudice des dispositions concernant le renouvellement des habilitations de sécurité. Ces autorisations temporaires d'accès aux ICUE sont valables pour une période non renouvelable ne dépassant pas six mois et ne donnent pas accès aux informations classifiées TRÈS SECRET UE/EU TOP SECRET.

2. Après avoir été informées conformément à l'article 12, paragraphe 1, toutes les personnes auxquelles a été délivrée une autorisation temporaire reconnaissent par écrit qu'elles sont conscientes de leurs obligations en matière de protection des ICUE et des conséquences qui pourraient résulter si des ICUE devaient être compromises. L'autorité de sécurité de la Commission tient un registre de ces déclarations écrites.

Article 14

Participation à des réunions classifiées organisées par la Commission

1. Les services de la Commission chargés d'organisation des réunions lors desquelles des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur sont traitées informent, par l'intermédiaire de leur responsable local de la sécurité ou de l'organisateur de la réunion, l'autorité de sécurité de la Commission suffisamment à l'avance des dates, heures, lieux et participants à ces réunions.

2. Sous réserve des dispositions de l'article 11, paragraphe 13, les personnes désignées pour participer à des réunions organisées par la Commission lors desquelles des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur sont traitées, ne peuvent le faire qu'après confirmation de leur situation au regard de l'habilitation ou de l'autorisation de sécurité. L'accès à ces réunions classifiées est refusé aux personnes pour lesquelles l'autorité de sécurité de la Commission n'a vu aucun CHSP ni autre preuve d'habilitation de sécurité, ainsi qu'aux participants de la Commission qui ne détiennent pas d'autorisation de sécurité.

3. Avant d'organiser une réunion classifiée, l'organisateur responsable de la réunion ou le responsable local de la sécurité du service de la Commission organisateur de la réunion demande aux participants extérieurs de fournir à l'autorité de sécurité de la Commission un CHSP ou une autre preuve d'habilitation de sécurité. L'autorité de sécurité de la Commission informe le responsable local de la sécurité ou l'organisateur de la réunion de tout CHSP ou autre preuve de HSP qu'elle reçoit. Le cas échéant, il peut être fait usage d'une liste de noms récapitulative mentionnant les preuves d'habilitation de sécurité voulues.

4. Lorsque l'autorité de sécurité de la Commission est informée par les autorités compétentes qu'une HSP a été retirée à une personne dont les fonctions requièrent la participation à des réunions organisées par la Commission, l'autorité de sécurité de la Commission en informe le responsable local de la sécurité du service de la Commission chargé d'organiser la réunion.

Article 15

Accès potentiel aux ICUE

Les courriers, les gardes et les escortes doivent disposer d'une autorisation de sécurité du niveau correspondant ou faire l'objet d'une enquête appropriée conformément aux dispositions législatives et réglementaires nationales, et être informés des procédures de sécurité applicables à la protection des ICUE ainsi que des obligations qui leur incombent en matière de protection des informations de cette nature qui leur sont confiées.

CHAPITRE 3

MESURES DE SÉCURITÉ PHYSIQUE VISANT À PROTÉGER LES INFORMATIONS CLASSIFIÉES

Article 16

Principes de base

1. Les mesures de sécurité physique sont destinées à faire obstacle à toute intrusion par la ruse ou par la force, à avoir un effet dissuasif, à empêcher et détecter les actes non autorisés et permettre d'établir une distinction entre les membres du personnel au regard de l'accès aux ICUE conformément au principe du besoin d'en connaître. Ces mesures sont déterminées sur la base d'une procédure de gestion des risques, conformément à la présente décision et à ses modalités d'application.

2. Plus précisément, les mesures de sécurité physique sont destinées à prévenir l'accès non autorisé aux ICUE en:

a) garantissant que les ICUE sont correctement traitées et stockées;

b) permettant d'établir une distinction entre les membres du personnel au regard de l'accès aux ICUE sur la base de leur besoin d'en connaître et, le cas échéant, de leur autorisation de sécurité;

c) ayant un effet dissuasif, en empêchant et en détectant les actes non autorisés; et

d) en empêchant ou en retardant toute intrusion par la ruse ou par la force.

3. Les mesures physiques de sécurité sont mises en place pour tous les locaux, bâtiments, bureaux, salles et autres zones dans lesquels des ICUE sont traitées ou stockées, y compris les zones où se trouvent les systèmes d'information et de communication visés au chapitre 5.

4. Des zones où sont stockées des ICUE CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur sont créées en tant que zones sécurisées conformément au présent chapitre et agréées par l'autorité d'homologation de sécurité de la Commission.

5. Seuls des équipements ou des dispositifs agréés par l'autorité de sécurité de la Commission sont utilisés pour protéger les ICUE CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur.

Article 17

Règles et mesures en matière de sécurité physique

1. Les mesures de sécurité physique sont choisies en fonction d'une évaluation de la menace réalisée par l'autorité de sécurité de la Commission, le cas échéant en concertation avec d'autres services de la Commission, d'autres institutions, agences ou organes de l'Union et/ou les autorités compétentes des États membres. La Commission applique une procédure de gestion du risque pour protéger les ICUE dans ses locaux afin de garantir un niveau de protection physique qui soit proportionné au risque évalué. La procédure de gestion des risques tient compte de tous les facteurs pertinents, et notamment:

a) du niveau de classification des ICUE;

b) de la forme et du volume des ICUE, sachant que l'application de mesures de protection plus strictes pourrait être requise pour des volumes importants ou en cas de compilation d'ICUE;

c) de l'environnement et de la structure des bâtiments ou des zones où se trouvent des ICUE; et

d) de l'évaluation de la menace que constituent les services de renseignement prenant pour cible l'Union, ses institutions, organes ou agences ou les États membres, ainsi que les actes de sabotage, le terrorisme et les activités subversives ou les autres activités criminelles.

2. En appliquant la notion de défense en profondeur, l'autorité de sécurité de la Commission détermine la bonne combinaison de mesures de sécurité physique qu'il convient de mettre en œuvre. À cet effet, l'autorité de sécurité de la Commission élabore des normes et des critères minimaux établis dans les modalités d'application.

3. L'autorité de sécurité de la Commission est autorisée à mener des fouilles aux entrées et aux sorties afin d'avoir un effet dissuasif quant à l'introduction non autorisée de matériel dans des locaux ou des bâtiments ou au retrait non autorisé de toute ICUE des lieux précités.

4. Lorsque des ICUE risquent d'être vues, même accidentellement, les services de la Commission concernés prennent les mesures appropriées, définies par l'autorité de sécurité de la Commission, pour parer à ce risque.

5. Pour les nouveaux établissements, les règles en matière de sécurité physique et leurs spécifications fonctionnelles doivent être définies avec le consentement de l'autorité de sécurité de la Commission lors de la planification et de la conception des établissements. Pour les établissements existants, les règles en matière de sécurité physique doivent être appliquées conformément aux normes et critères minimaux définis dans les modalités d'application.

Article 18

Équipement destiné à la protection physique des ICUE

1. Deux types de zones physiquement protégées sont créés en vue de la protection physique des ICUE:

a) les zones administratives; et

b) les zones sécurisées (dont les zones sécurisées du point de vue technique).

2. Il appartient à l'autorité d'homologation de sécurité de la Commission d'établir qu'une zone répond aux conditions requises pour être désignée comme zone administrative, zone sécurisée ou zone sécurisée du point de vue technique.

3. Pour les zones administratives:

a) un périmètre défini est établi de façon visible afin de permettre le contrôle des personnes et, dans la mesure du possible, des véhicules;

b) ne peuvent y pénétrer sans escorte que les personnes dûment autorisées par l'autorité de sécurité de la Commission ou toute autre autorité compétente; et

c) toutes les autres personnes sont escortées en permanence ou font l'objet de contrôles équivalents.

4. Pour les zones sécurisées:

a) un périmètre défini et protégé est établi de façon visible et toutes les entrées et sorties sont contrôlées par un système de laissez-passer ou d'identification individuelle;

b) ne peuvent y pénétrer sans escorte que les personnes habilitées et expressément autorisées à y entrer sur la base de leur besoin d'en connaître; et

c) toutes les autres personnes sont escortées en permanence ou font l'objet de contrôles équivalents.

5. Lorsque le fait de pénétrer dans une zone sécurisée équivaut en pratique à un accès direct aux informations classifiées qu'elle renferme, les règles supplémentaires suivantes sont d'application:

a) le niveau de classification le plus élevé qui s'applique aux informations conservées habituellement dans la zone doit être clairement indiqué;

b) tous les visiteurs doivent disposer d'une autorisation spécifique pour pénétrer dans la zone, sont escortés en permanence et disposent de l'habilitation de sécurité correspondante, sauf si des mesures sont prises pour empêcher l'accès aux ICUE.

6. Les zones sécurisées qui sont protégées contre les écoutes sont qualifiées de zones sécurisées du point de vue technique. Les règles supplémentaires suivantes sont applicables:

a) ces zones sont équipées d'un système de détection des intrusions (SDI), verrouillées lorsqu'elles ne sont pas occupées et gardées lorsqu'elles sont occupées. Toutes les clés sont gérées conformément à l'article 20;

b) toutes les personnes et tous les matériels entrant dans ces zones sont contrôlés;

c) ces zones doivent faire l'objet, à intervalles réguliers, d'inspections physiques et/ou techniques par l'autorité de sécurité de la Commission. Ces inspections doivent également être effectuées après une entrée non autorisée, réelle ou présumée; et

d) ces zones ne sont pas équipées de lignes de communication, de téléphones ou d'autres dispositifs de communication ou matériels électriques ou électroniques qui ne sont pas autorisés.

7. Nonobstant le paragraphe 6, point d), avant d'être utilisé dans des zones dans lesquelles sont organisées des réunions ou sont exécutées des tâches mettant en jeu des informations classifiées SECRET UE/EU SECRET et d'un niveau de classification supérieur, et lorsque la menace pesant sur des ICUE est jugée élevée, tout dispositif de communication et tout matériel électrique ou électronique est d'abord examiné par l'autorité de sécurité de la Commission pour vérifier qu'aucune information intelligible ne peut être transmise par inadvertance ou de manière illicite par ces équipements en dehors du périmètre de la zone sécurisée.

8. Les zones sécurisées qui ne sont pas occupées vingt-quatre heures sur vingt-quatre par le personnel de service sont, au besoin, inspectées après les heures normales de travail et à intervalles aléatoires en dehors de ces heures, sauf si un SDI a été installé.

9. Des zones sécurisées et des zones sécurisées du point de vue technique peuvent être temporairement établies dans une zone administrative en vue de la tenue d'une réunion classifiée ou à toute autre fin similaire.

10. Le responsable local de la sécurité du service de la Commission concerné établit des procédures d'exploitation de sécurité (SecOP) pour chaque zone sécurisée dont il a la charge, qui précisent, conformément aux dispositions de la présente décision et de ses modalités d'application:

a) le niveau de classification des ICUE traitées ou stockées dans la zone;

b) les mesures de surveillance et de protection qu'il convient de mettre en place;

c) les personnes autorisées à pénétrer dans la zone sans escorte en raison de leur besoin d'en connaître et en fonction de leur autorisation de sécurité;

d) le cas échéant, les procédures applicables aux escortes ou à la protection des ICUE lorsque d'autres personnes sont autorisées à pénétrer dans la zone;

e) les autres mesures et procédures applicables.

11. Les chambres fortes sont installées dans des zones sécurisées. Les murs, les planchers, les plafonds, les fenêtres et les portes verrouillables sont approuvés par l'autorité de sécurité de la Commission et offrent une protection équivalente à celle d'un meuble de sécurité approuvé pour le stockage d'ICUE du même niveau de classification.

Article 19

Mesures de protection physiques applicables au traitement et au stockage des ICUE

1. Les ICUE RESTREINT UE/EU RESTRICTED peuvent être traitées:

a) dans une zone sécurisée;

b) dans une zone administrative à condition que les personnes non autorisées ne puissent avoir accès aux ICUE; ou

c) en dehors d'une zone sécurisée ou d'une zone administrative à condition que le détenteur les transporte conformément à l'article 31 et se soit engagé à se conformer aux mesures compensatoires prévues dans les modalités d'application pour empêcher que des personnes non autorisées aient accès aux ICUE.

2. Les ICUE RESTREINT UE/EU RESTRICTED sont stockées dans un meuble de bureau adapté et fermé dans une zone administrative ou dans une zone sécurisée. Ces informations peuvent être temporairement stockées en dehors d'une zone administrative ou d'une zone sécurisée à condition que le détenteur se soit engagé à se conformer aux mesures compensatoires prévues dans les modalités d'application.

3. Les ICUE CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET peuvent être traitées:

a) dans une zone sécurisée;

b) dans une zone administrative à condition que les personnes non autorisées ne puissent avoir accès aux ICUE; ou

c) en dehors d'une zone sécurisée ou d'une zone administrative à condition que le détenteur:

i) se soit engagé à se conformer aux mesures compensatoires prévues dans les modalités d'application pour empêcher que des personnes non autorisées aient accès aux ICUE;

ii) exerce en personne un contrôle permanent sur les ICUE; et

iii) si les documents sont sous forme papier, qu'il en ait informé le bureau d'ordre compétent.

4. Les ICUE classifiées CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET sont stockées dans une zone sécurisée, dans un meuble de sécurité ou une chambre forte.

5. Les ICUE classifiées TRÈS SECRET UE/EU TOP SECRET sont traitées dans une zone sécurisée, mise en place et entretenue par l'autorité de sécurité de la Commission, et agréée à ce niveau de classification par l'autorité d'homologation de sécurité de la Commission.

6. Les ICUE classifiées TRÈS SECRET UE/EU TOP SECRET sont stockées dans une zone sécurisée, agréée à ce niveau de classification par l'autorité d'homologation de sécurité de la Commission, selon l'une des modalités suivantes:

a) dans un meuble de sécurité conformément aux dispositions de l'article 18, moyennant un ou plusieurs des contrôles supplémentaires suivants:

(1) protection ou vérification en permanence par un membre habilité du personnel de sécurité ou du personnel de service;

(2) un système de détection des intrusions approuvé auquel on associe du personnel de sécurité prêt à intervenir en cas d'incident;

ou

b) dans une chambre forte équipée d'un système de détection des intrusions à laquelle on associe du personnel de sécurité prêt à intervenir en cas d'incident.

Article 20

Contrôle des clés et combinaisons utilisées pour la protection des ICUE

1. Des procédures de gestion des clés et des combinaisons pour les bureaux, les salles, les chambres fortes et les meubles de sécurité sont définies dans les modalités d'application conformément à l'article 60 ci-après. Ces procédures sont destinées à empêcher un accès non autorisé.

2. Les combinaisons doivent être mémorisées par le plus petit nombre possible de personnes qui ont besoin de les connaître. Les combinaisons des meubles de sécurité et des chambres fortes servant au stockage d'ICUE doivent être changées:

a) à la réception d'un nouveau meuble;

b) lors de tout changement du personnel connaissant la combinaison;

c) en cas de compromission, réelle ou présumée;

d) lorsqu'une serrure a fait l'objet d'un entretien ou d'une réparation; et

e) au moins tous les douze mois.

CHAPITRE 4

GESTION DES INFORMATIONS CLASSIFIÉES DE L'UNION EUROPÉENNE

Article 21

Principes de base

1. Tous les documents d'ICUE doivent être gérés conformément à la politique de la Commission en matière de gestion des documents et doivent donc être répertoriés, enregistrés, conservés puis éliminés, soumis à un échantillonnage ou transférés aux archives historiques conformément à la liste commune de conservation des dossiers au niveau de la Commission européenne.

2. Les informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur sont enregistrées à des fins de sécurité avant leur diffusion et lors de leur réception. Les informations classifiées TRÈS SECRET UE/EU TOP SECRET sont enregistrées dans des bureaux d'ordre désignés.

3. Un système de bureaux d'ordre pour les ICUE est mis en place au sein de la Commission conformément aux dispositions de l'article 27.

4. Les services et les locaux de la Commission dans lesquels les ICUE sont traitées ou stockées font l'objet d'une inspection régulière par l'autorité de sécurité de la Commission.

5. En dehors des zones physiquement protégées, les ICUE sont transmises entre les services et les locaux selon les modalités suivantes:

a) en règle générale, les ICUE sont transmises par voie électronique protégée par des produits cryptographiques agréés conformément au chapitre 5;

b) si la voie visée au point a) n'est pas utilisée, les ICUE sont transportées:

   i) soit sur des supports électroniques (par exemple clé USB, CD, disque dur) protégés par des produits cryptographiques agréés conformément au chapitre 5;

   ii) soit, dans tous les autres cas, de la manière prescrite dans les modalités d'application.

Article 22

Classifications et marquages

1. Les informations sont classifiées dans les cas où elles doivent être protégées compte tenu de leur confidentialité, conformément à l'article 3, paragraphe 1.

2. L'autorité d'origine des ICUE est chargée de déterminer le niveau de classification de sécurité, conformément aux modalités d'application, normes et lignes directrices applicables en matière de classification, et de la diffusion initiale des informations.

3. Le niveau de classification des ICUE est fixé conformément à l'article 3, paragraphe 2, et aux modalités d'application correspondantes.

4. La classification de sécurité est clairement et correctement indiquée, indépendamment de la forme sous laquelle se présentent les ICUE: format papier, forme orale, électronique ou autre.

5. Les différentes parties d'un document donné (pages, paragraphes, sections, annexes, appendices et pièces jointes) peuvent nécessiter une classification différente et doivent alors porter le marquage afférent, y compris lorsqu'elles sont stockées sous forme électronique.

6. Le niveau général de classification d'un document ou d'un dossier est au moins aussi élevé que celui de sa partie portant la classification la plus élevée. Lorsqu'il rassemble des informations provenant de plusieurs sources, le document final est examiné pour en fixer le niveau général de classification de sécurité car il peut requérir un niveau de classification supérieur à celui de chacune des parties qui le composent.

7. Dans la mesure du possible, les documents dont toutes les parties n'ont pas le même niveau de classification sont structurés de manière que les parties ayant des niveaux de classification différents puissent au besoin être aisément identifiées et séparées des autres.

8. Les lettres ou notes d'envoi accompagnant des pièces jointes portent le plus haut niveau de classification attribué à ces dernières. L'autorité d'origine indique clairement leur niveau de classification lorsqu'elles sont séparées de leurs pièces jointes, au moyen d'un marquage approprié, par exemple:

CONFIDENTIEL UE/EU CONFIDENTIAL

Sans pièce(s) jointe(s) RESTREINT UE/EU RESTRICTED

Article 23

Marquages

Outre l'un des marquages de classification de sécurité prévus à l'article 3, paragraphe 2, les ICUE peuvent porter des marquages complémentaires, tels que:

a) un identifiant désignant l'autorité d'origine;

b) des marquages restrictifs, des mots-codes ou des acronymes utilisés pour préciser le domaine d'activité sur lequel porte le document ou pour indiquer une diffusion particulière en fonction du besoin d'en connaître ou des restrictions d'utilisation;

c) des marquages relatifs à la communicabilité;

d) le cas échéant, la date ou l'événement particulier à partir desquels elles peuvent être déclassées ou déclassifiées.

Article 24

Abréviations indiquant la classification

1. Des abréviations uniformisées indiquant la classification peuvent être utilisées pour préciser le niveau de classification des différents paragraphes d'un texte. Les abréviations ne remplacent pas la mention de la classification en toutes lettres.

2. Les abréviations uniformisées ci-après peuvent être utilisées dans les documents classifiés de l'Union européenne pour indiquer le niveau de classification de sections ou blocs de texte de moins d'une page:

TRÈS SECRET UE/EU TOP SECRET	TS-UE/EU-TS
SECRET UE/EU SECRET	S-UE/EU-S
CONFIDENTIEL UE/EU CONFIDENTIAL	C-UE/EU-C
RESTREINT UE/EU RESTRICTED	R-UE/EU-R

Article 25

Création d'ICUE

1. Lors de la création de documents classifiés de l'Union européenne:

a) sur chaque page figure un marquage indiquant clairement le niveau de classification;

b) chaque page est numérotée;

c) le document porte un numéro d'enregistrement et un sujet qui n'est pas lui-même une information classifiée, sauf s'il s'est vu apposer un marquage à ce titre;

d) le document est daté;

e) les documents classifiés SECRET UE/EU SECRET ou d'un niveau de classification supérieur portent un numéro d'exemplaire sur chaque page dès lors qu'ils doivent être diffusés en plusieurs exemplaires.

2. Lorsqu'il n'est pas possible d'appliquer le paragraphe 1 à des ICUE, d'autres mesures appropriées sont prises conformément aux modalités d'application.

Article 26

Déclassement et déclassification des ICUE

1. Au moment de la création du document classifié, l'autorité d'origine indique, si possible, si les ICUE qui y figurent peuvent ou non être déclassées ou déclassifiées à une date donnée ou après un événement spécifique.

2. Chaque service de la Commission réexamine régulièrement les ICUE dont il est l'autorité d'origine pour déterminer si leur niveau de classification est toujours d'application. Un système pour réexaminer au moins une fois tous les cinq ans le niveau de classification des ICUE enregistrées dont la Commission est l'auteur est instauré conformément aux modalités d'application. Un tel réexamen n'est pas nécessaire lorsque l'autorité d'origine a indiqué dès le départ que les informations seraient automatiquement déclassées ou déclassifiées et que celles-ci se sont vu apposer les marquages correspondants.

3. Les informations classifiées RESTREINT UE/EU RESTRICTED dont la Commission est l'auteur sont considérées comme étant automatiquement déclassifiées à l'issue d'une période de trente ans, conformément au règlement (CEE, Euratom) nº 354/83 du Conseil modifié par le règlement (CE, Euratom) nº 1700/2003 du Conseil ([1]).

Article 27

Bureaux d'ordre pour les ICUE au sein de la Commission

1. Sans préjudice de l'article 52, paragraphe 5 ci-après, dans chaque service de la Commission où des ICUE de niveau CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET sont traitées ou stockées, on détermine un bureau d'ordre local compétent chargé de veiller à ce que les ICUE soient traitées conformément à la présente décision.

2. Le bureau d'ordre géré par le secrétariat général représente le bureau d'ordre central pour les ICUE. Il constitue:

— le bureau d'ordre local pour le secrétariat général de la Commission;

— le bureau d'ordre pour les cabinets privés des membres de la Commission, sauf s'ils disposent d'un bureau d'ordre local désigné pour les ICUE;

— le bureau d'ordre pour les directions générales ou les services qui n'ont pas de bureau d'ordre local pour les ICUE;

— le principal point d'entrée et de sortie pour toutes les informations classifiées RESTREINT UE/EU RESTRICTED et d'un niveau de classification supérieur jusqu'à SECRET UE/EU SECRET inclus, échangées entre la Commission et ses services et des pays tiers et organisations internationales, ainsi que, si des dispositions spécifiques le prévoient, pour d'autres institutions, agences et organes de l'Union européenne.

3. Au sein de la Commission, un bureau d'ordre est désigné par l'autorité de sécurité de la Commission pour faire fonction d'autorité centrale de réception et de diffusion des informations classifiées TRÈS SECRET UE/EU TOP SECRET. S'il y a lieu, les bureaux d'ordre subordonnés peuvent être désignés pour traiter ces informations à des fins d'enregistrement.

4. Ces bureaux d'ordre subordonnés ne peuvent transmettre de documents TRÈS SECRET UE/EU TOP SECRET directement à d'autres bureaux d'ordre subordonnés rattachés au même bureau d'ordre TRÈS SECRET UE/EU TOP SECRET central sans l'autorisation expresse et écrite de ce dernier, ni à des bureaux d'ordre extérieurs.

5. Les bureaux d'ordre pour les ICUE sont conçus comme des zones sécurisées telles que définies au chapitre 3 et agréées par l'autorité d'homologation de sécurité de la Commission (AHS).

Article 28

Agent contrôleur

1. Chaque bureau d'ordre pour les ICUE est géré par un agent contrôleur (RCO).

2. L'agent contrôleur dispose d'une habilitation de sécurité appropriée.

3. L'agent contrôleur est placé sous la supervision du responsable local de la sécurité au sein du service de la Commission pour ce qui concerne l'application des dispositions relatives à la manipulation des ICUE et la mise en œuvre des règles, normes et lignes directrices correspondantes en matière de sécurité.

4. Dans le cadre de ses responsabilités de gestion du bureau d'ordre pour les ICUE auquel il est affecté, l'agent contrôleur exécute les tâches générales suivantes conformément à la présente décision et aux modalités d'application, normes et lignes directrices correspondantes:

— gestion des opérations relatives à l'enregistrement, la conservation, la reproduction, la traduction, la transmission, l'expédition et la destruction des ICUE ou leur transfert au service des archives historiques;

— vérification périodique de la nécessité de maintenir la classification de ces informations;

— exécution de toute autre tâche en relation avec la protection des ICUE définie dans les modalités d'application.

Article 29

Enregistrement des ICUE à des fins de sécurité

1. Aux fins de la présente décision, on entend par enregistrement à des fins de sécurité (ci-après dénommé «enregistrement») l'application de procédures permettant de garder la trace du cycle de vie des ICUE, y compris de leur diffusion.

([1]) Règlement (CE, Euratom) nº 1700/2003 du Conseil du 22 septembre 2003 modifiant le règlement (CEE, Euratom) nº 354/83 concernant l'ouverture au public des archives historiques de la Communauté économique européenne et de la Communauté européenne de l'énergie atomique (JO L 243 du 27.9.2003, p. 1).

2. Tout élément d'information ou matériel classifié CONFIDENTIEL UE/EU CONFIDENTIAL et d'un niveau de classification supérieur est enregistré par un bureau d'ordre déterminé à chaque fois qu'il est réceptionné ou expédié par une entité structurée.

3. Lorsque les ICUE sont traitées ou stockées à l'aide d'un système d'information et de communication (SIC), les procédures d'enregistrement peuvent être mises en œuvre au moyen de processus intervenant au sein du SIC même.

4. Les modalités d'application contiennent des dispositions plus détaillées concernant l'enregistrement des ICUE à des fins de sécurité.

Article 30

Duplication et traduction des documents classifiés de l'Union européenne

1. Les documents classifiés TRÈS SECRET UE/EU TOP SECRET ne doivent pas être dupliqués ou traduits sans le consentement écrit préalable de l'autorité d'origine.

2. Lorsque l'autorité d'origine de documents classifiés SECRET UE/EU SECRET et d'un niveau de classification inférieur n'a pas imposé de restrictions à leur duplication ou à leur traduction, lesdits documents peuvent être dupliqués ou traduits sur instruction du détenteur.

3. Les mesures de sécurité applicables au document original le sont aussi à ses copies et à ses traductions.

Article 31

Transport des ICUE

1. Les ICUE sont transportées de manière à les protéger contre toute divulgation non autorisée durant le transport.

2. Le transport des ICUE est soumis à des mesures de protection:

— en adéquation avec le niveau de classification des ICUE transportées;

— adaptées aux conditions spécifiques de leur transport, notamment selon que les ICUE sont transportées:

  — à l'intérieur d'un même bâtiment de la Commission ou d'un groupe autonome de bâtiments de la Commission,

  — entre des bâtiments de la Commission situés dans un même État membre,

  — à l'intérieur de l'Union,

  — de l'Union vers le territoire d'un État tiers; et

  — adaptées à la nature et la forme des ICUE concernées.

3. Ces mesures de protection sont indiquées en détail dans les modalités d'application ou, dans le cas de projets et programmes visés à l'article 42, en tant que partie intégrante des instructions de sécurité relatives à un programme ou un projet (ISP).

4. Les modalités d'application ou les ISP incluent des dispositions en rapport avec le niveau de classification des ICUE concernant:

— le mode de transport, à savoir transport par porteur, courrier diplomatique ou militaire, services postaux ou services de courrier commercial;

— l'emballage des ICUE;

— les contre-mesures techniques pour les ICUE transportées sur support électronique;

— toute autre mesure de nature procédurale, physique ou électronique;

— les procédures d'enregistrement;

— l'emploi de personnel disposant d'autorisations de sécurité.

5. Lorsque les ICUE sont transportées par des supports électroniques, et nonobstant l'article 21, paragraphe 5, les mesures de protection énoncées dans les modalités d'application correspondantes peuvent être complétées par des contre-mesures techniques appropriées approuvées par l'autorité de sécurité de la Commission, de façon à réduire au minimum le risque de perte ou de compromission.

Article 32

Destruction des ICUE

1. Les documents classifiés de l'Union européenne qui ne sont plus nécessaires peuvent être détruits, compte tenu des règlements relatifs aux archives et des règles et règlements de la Commission relatifs à la gestion et à l'archivage des documents, en particulier la liste commune de conservation des dossiers au niveau de la Commission européenne.

2. Les ICUE de niveau CONFIDENTIEL UE/EU CONFIDENTIAL et d'un niveau de classification supérieur sont détruites par l'agent contrôleur du bureau d'ordre compétent sur instruction du détenteur ou d'une autorité compétente. L'agent contrôleur actualise en conséquence les cahiers d'enregistrement et les autres informations relatives aux enregistrements.

3. La destruction de documents classifiés SECRET UE/EU SECRET ou TRÈS SECRET UE/EU TOP SECRET est effectuée par l'agent contrôleur en présence d'un témoin justifiant de l'habilitation de sécurité correspondant au moins au niveau de classification du document à détruire.

4. L'agent du bureau d'ordre et le témoin, lorsque la présence de ce dernier est requise, signent un procès-verbal de destruction qui est rempli dans le bureau d'ordre. L'agent contrôleur du bureau d'ordre compétent conserve les procès-verbaux de destruction des documents TRÈS SECRET UE/EU TOP SECRET pendant dix ans au minimum, et ceux des documents CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET pendant cinq ans au minimum.

5. Les documents classifiés, y compris ceux dont la classification est RESTREINT UE/EU RESTRICTED, sont détruits par des méthodes définies dans les modalités d'application et répondant aux normes UE applicables ou à des normes équivalentes.

6. La destruction des supports de données informatiques utilisés pour les ICUE s'effectue conformément aux procédures définies dans les modalités d'application.

Article 33

Destruction des ICUE en cas d'urgence

1. Les services de la Commission qui détiennent des ICUE établissent des plans tenant compte des conditions locales pour assurer la sauvegarde en temps de crise des matériels classifiés de l'Union européenne, y compris si nécessaire des plans de destruction et d'évacuation en cas d'urgence. Ils émettent les consignes qu'ils jugent appropriées pour éviter que des ICUE ne tombent entre les mains de personnes non autorisées.

2. Les dispositions prises pour la sauvegarde et/ou la destruction en temps de crise des matériels CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET ne doivent en aucun cas nuire à la sauvegarde ni à la destruction des matériels TRÈS SECRET UE/EU TOP SECRET, et notamment des matériels de chiffrement, dont la prise en charge doit avoir la priorité sur toutes les autres tâches.

3. En cas d'urgence, s'il existe un risque imminent de divulgation non autorisée, les ICUE sont détruites par le détenteur de manière à ce qu'elles ne puissent pas être reconstituées en tout ou en partie. L'autorité d'origine et le bureau d'ordre d'origine sont informés de la destruction en urgence d'ICUE enregistrées.

4. Les modalités d'application contiennent des dispositions plus détaillées concernant la destruction des ICUE.

CHAPITRE 5

PROTECTION DES INFORMATIONS CLASSIFIÉES DE L'UNION EUROPÉENNE DANS LES SYSTÈMES D'INFORMATION ET DE COMMUNICATION (SIC)

Article 34

Principes d'assurance de l'information

1. Par «assurance de l'information (AI) dans le domaine des systèmes d'information et de communication», on entend la certitude que ces systèmes protégeront les informations qu'ils traitent et fonctionneront comme ils le doivent, quand ils le doivent, sous le contrôle d'utilisateurs légitimes.

2. Une assurance de l'information efficace garantit des niveaux appropriés de:

Authenticité: garantie que l'information est véridique et émane de sources dignes de foi;

Disponibilité: caractéristique de l'information selon laquelle elle est accessible et utilisable, à la demande d'une entité autorisée;

Confidentialité: propriété selon laquelle les informations ne sont pas divulguées à des personnes ou à des entités non autorisées et l'accès à ces informations n'est pas accordé à des processus non autorisés;

Intégrité: propriété consistant à préserver l'exactitude et le caractère complet des informations et éléments;

Non-répudiation: la possibilité de prouver qu'une action ou un événement a eu lieu, de sorte qu'il ne peut être contesté par la suite.

3. L'AI est fondée sur un processus de gestion des risques.

Article 35

Définitions

Aux fins du présent chapitre, les définitions suivantes sont applicables:

a) par «homologation», on entend l'agrément formel d'un système d'information et de communication par l'autorité d'homologation de sécurité (AHS) autorisant son emploi pour traiter des ICUE dans son environnement opérationnel, après la validation formelle du plan de sécurité et la mise en œuvre adéquate de celui-ci;

b) par «processus d'homologation», on entend les étapes et tâches requises avant d'obtenir l'agrément de l'autorité d'homologation de sécurité. Ces étapes et tâches sont définies dans une norme de processus d'homologation;

c) on entend par «système d'information et de communication» (SIC) tout système permettant le traitement d'informations sous forme électronique. Un système d'information et de communication comprend l'ensemble des moyens nécessaires pour le faire fonctionner, y compris l'infrastructure, l'organisation, le personnel et les ressources d'information;

d) on entend par «risque résiduel» le risque qui subsiste après que des mesures de sécurité ont été mises en œuvre, étant entendu qu'il est impossible de contrer toutes les menaces et d'éliminer toutes les vulnérabilités;

e) on entend par «risque» la possibilité qu'une menace donnée se concrétise en tirant parti des vulnérabilités internes et externes d'une organisation ou d'un des systèmes qu'elle utilise et cause ainsi un préjudice à l'organisation ou à ses ressources matérielles ou immatérielles. Il se mesure en tenant compte à la fois de la probabilité de voir se concrétiser des menaces et de l'impact de celles-ci;

f) l'«acceptation des risques» consiste à décider d'accepter qu'un risque résiduel subsiste au terme du traitement des risques;

g) l'«évaluation des risques» consiste à déterminer les menaces et les vulnérabilités et à procéder à l'analyse des risques correspondants, c'est-à-dire à examiner leur probabilité et leur impact;

h) la «communication des risques» consiste à sensibiliser la communauté des utilisateurs du SIC aux risques, à informer les autorités d'homologation de ces risques et à faire rapport à leur sujet aux autorités responsables de l'exploitation;

i) le «traitement des risques» consiste à atténuer, à éliminer, à réduire (par un ensemble approprié de mesures sur le plan technique, physique ou au niveau de l'organisation ou des procédures), à transférer ou à surveiller les risques.

Article 36

SIC traitant des ICUE

1. Les SIC traitent des ICUE dans le respect de la notion d'AI.

2. Pour les SIC traitant des ICUE, le respect de la politique de sécurité des systèmes d'information de la Commission, telle qu'énoncée dans la décision C(2006)3602 ([1]) de la Commission, implique:

a) l'application de la méthode «planifier-déployer-contrôler-agir» pour la mise en œuvre de la politique de sécurité des systèmes d'information tout au long du cycle de vie du système d'information;

b) la détermination des besoins de sécurité au moyen d'une évaluation d'impact sur l'activité;

c) la réalisation d'une classification formelle des éléments pour le système d'information et les données qu'il contient;

([1]) C(2006) 3602 du 16 août 2006 relative à la sécurité des systèmes d'information utilisés par les services de la Commission.

d) la mise en œuvre de toutes les mesures de sécurité obligatoires définies par la politique de sécurité des systèmes d'information;

e) l'application d'un processus de gestion des risques, composé des étapes suivantes: identification des menaces et des vulnérabilités, évaluation des risques, traitement des risques, acceptation des risques et communication des risques;

f) la définition d'un plan de sécurité, incluant la politique de sécurité et les procédures d'exploitation de sécurité, ainsi que sa mise en œuvre, sa vérification et sa révision.

3. L'ensemble du personnel participant à l'élaboration, au développement, aux essais, au fonctionnement, à la gestion ou à l'utilisation des SIC traitant des ICUE notifie à l'AHS toutes les faiblesses en matière de sécurité, les incidents, les infractions à la sécurité ou les compromissions potentiels susceptibles d'avoir un impact sur la protection du SIC et/ou des ICUE qu'il contient.

4. Lorsque la protection des ICUE est assurée par des produits cryptographiques, ces produits doivent être approuvés comme suit:

a) la préférence est donnée aux produits agréés par le Conseil ou par le secrétaire général du Conseil en sa qualité d'autorité d'agrément cryptographique du Conseil, sur recommandation du groupe d'experts sécurité de la Commission;

b) lorsque des motifs opérationnels particuliers le justifient, l'autorité d'agrément cryptographique de la Commission (AAC) peut, sur recommandation du groupe d'experts sécurité de la Commission, ne pas respecter les exigences prévues au point a) et délivrer un agrément à titre provisoire pour une période spécifique.

5. Lors de la transmission, du traitement et du stockage des ICUE par voie électronique, des produits cryptographiques qui ont fait l'objet d'un agrément sont utilisés. Nonobstant cette exigence, des procédures spécifiques peuvent être appliquées en cas d'urgence ou dans le cadre de configurations techniques spécifiques après agrément de l'AAC.

6. Des mesures de sécurité sont mises en œuvre afin de protéger les SIC traitant des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur contre la compromission de ces informations par des émissions électromagnétiques non intentionnelles («mesures de sécurité TEMPEST»). Ces mesures de sécurité sont proportionnées au risque d'exploitation et au niveau de classification des informations.

7. L'autorité de sécurité de la Commission exerce les fonctions suivantes:

— autorité chargée de l'AI (AAI);

— autorité d'homologation de sécurité (AHS);

— autorité TEMPEST (AT);

— autorité d'agrément cryptographique (AAC);

— autorité chargée de la distribution cryptographique (ADC).

8. Pour chaque système, l'autorité de sécurité de la Commission désigne une autorité opérationnelle chargée de l'AI.

9. Les responsabilités des fonctions décrites aux paragraphes 7 et 8 seront définies dans les modalités d'application.

Article 37

Homologation des SIC traitant des ICUE

1. Tous les SIC traitant des ICUE font l'objet d'un processus d'homologation basé sur les principes d'AI, dont le niveau de détail doit être proportionné au niveau de protection requis.

2. Le processus d'homologation inclut la validation formelle par l'AHS de la Commission du plan de sécurité pour le SIC concerné, afin d'obtenir l'assurance que:

a) le processus de gestion des risques visé à l'article 36, paragraphe 2, a été correctement mis en œuvre;

b) le détenteur du système a accepté le risque résiduel en connaissance de cause; et

c) un niveau suffisant de protection du SIC et des ICUE qu'il traite a été atteint conformément à la présente décision.

3. L'AHS de la Commission délivre une déclaration d'homologation qui détermine le niveau maximal de classification des ICUE qui peuvent être traitées dans un SIC ainsi que les modalités et les conditions de fonctionnement correspondantes. Cette disposition s'applique sans préjudice des missions du conseil d'homologation de sécurité défini à l'article 11 du règlement (UE) nº 512/2014 du Parlement européen et du Conseil ([1]).

4. Un comité conjoint d'homologation de sécurité (CHS) est chargé de l'homologation des SIC de la Commission qui impliquent plusieurs parties. Ce comité est composé d'un représentant de l'AHS de chaque partie concernée et présidé par un représentant de l'AHS de la Commission.

5. Le processus d'homologation consiste en une série de tâches exécutées par les parties concernées. La responsabilité de la préparation des dossiers d'homologation et de la documentation incombe entièrement au détenteur du SIC.

6. L'homologation relève de la responsabilité de l'AHS de la Commission qui, à tout moment au cours du cycle de vie du SIC, est habilitée à:

a) exiger qu'un processus d'homologation soit appliqué;

b) procéder à un audit ou une inspection du SIC;

c) si les conditions de fonctionnement ne sont plus satisfaites, exiger l'élaboration et la mise en œuvre effective d'un plan d'amélioration de la sécurité selon un calendrier bien défini, en retirant éventuellement l'autorisation d'utiliser le SIC jusqu'à ce que les conditions de son fonctionnement soient à nouveau satisfaites.

7. Le processus d'homologation est établi dans une norme sur le processus d'homologation applicable aux SIC traitant des ICUE, adoptée conformément à l'article 10, paragraphe 3, de la décision C(2006) 3602.

Article 38

Situations d'urgence

1. Nonobstant les dispositions du présent chapitre, les procédures spécifiques décrites ci-après peuvent être appliquées dans les situations d'urgence, telles que les crises, les conflits ou les guerres, imminentes ou effectives, ou dans des circonstances opérationnelles exceptionnelles.

2. Sous réserve du consentement de l'autorité compétente, les ICUE peuvent être transmises au moyen de produits cryptographiques agréés pour un niveau de classification inférieur ou sans faire l'objet d'un chiffrement dans le cas où tout retard causerait un préjudice indéniablement plus important que celui qui découlerait de la divulgation du matériel classifié et dans les conditions suivantes:

a) l'expéditeur et le destinataire ne possèdent pas le dispositif de chiffrement nécessaire; et

b) le matériel classifié ne peut être communiqué en temps voulu par aucun autre moyen.

3. Les informations classifiées transmises dans les conditions visées au paragraphe 1 ne portent aucun marquage ni indication qui les distinguerait d'informations non classifiées ou pouvant être protégées à l'aide d'un produit cryptographique disponible. Leur destinataire est informé, sans délai et par d'autres moyens, du niveau de classification.

4. Un rapport est adressé par la suite à l'autorité compétente et au groupe d'experts sécurité de la Commission.

CHAPITRE 6

SÉCURITÉ INDUSTRIELLE

Article 39

Principes de base

1. Par «sécurité industrielle», on entend l'application de mesures visant à assurer la protection des ICUE

a) dans le cadre de contrats classifiés, par:

   i) des candidats ou des soumissionnaires tout au long de la durée de la procédure d'appel d'offres et de passation de marché,

   ii) des contractants ou des sous-traitants tout au long du cycle de vie des contrats classifiés;

([1]) Règlement (CE) nº 512/2014 du Parlement européen et du Conseil du 16 avril 2014 modifiant le règlement (UE) nº 912/2010 établissant l'Agence du GNSS européen (JO L 150 du 20.5.2014, p. 72).

b) dans le cadre de conventions de subvention classifiées, par:

i) des candidats durant les procédures d'octroi de subventions;

ii) des bénéficiaires tout au long du cycle de vie des conventions de subvention classifiées.

2. De tels contrats ou conventions de subvention ne doivent pas concerner des informations classifiées TRÈS SECRET UE/EU TOP SECRET.

3. Sauf mention contraire, les dispositions du présent chapitre visant des contrats classifiés ou des contractants s'appliquent également aux contrats de sous-traitance classifiés et aux sous-traitants.

Article 40

Définitions

Aux fins du présent chapitre, on entend par:

a) «contrat classifié», un contrat-cadre ou un contrat, tel que défini dans le règlement (CE, Euratom) n° 1605/2002 ([1]), conclu par la Commission ou l'un de ses services avec un contractant en vue de la fourniture de biens meubles ou immeubles, de la réalisation de travaux ou de la prestation de services, dont l'exécution requiert ou implique la création, le traitement ou le stockage d'ICUE;

b) «contrat de sous-traitance classifié», un contrat conclu par un contractant de la Commission ou de l'un de ses services avec un autre contractant (c'est-à-dire le sous-traitant) en vue de la fourniture de biens meubles ou immeubles, de la réalisation de travaux ou de la prestation de services, dont l'exécution nécessite ou implique la création, le traitement ou le stockage d'ICUE;

c) «convention de subvention classifiée», une convention aux termes de laquelle la Commission octroie une subvention, telle que définie dans la première partie, titre VI, du règlement (CE, Euratom) n° 1605/2002, et dont l'exécution nécessite ou implique la création, le traitement ou le stockage d'ICUE;

d) «autorité de sécurité désignée (ASD)», l'autorité responsable devant l'autorité nationale de sécurité (ANS) d'un État membre qui est chargée de communiquer à des entités industrielles ou autres la politique nationale dans tous les domaines relevant de la sécurité industrielle et de fournir des orientations et une aide pour sa mise en œuvre. Les fonctions de l'ASD peuvent être exercées par l'ANS ou par toute autre autorité compétente.

Article 41

Procédure applicable aux contrats et conventions de subvention classifiés

1. En tant qu'autorité contractante, chaque service de la Commission veille à ce que les normes minimales de sécurité industrielle prévues dans le présent chapitre soient mentionnées ou intégrées dans le contrat et respectées lors de l'octroi de contrats ou conventions de subvention classifiés.

2. Aux fins du paragraphe 1, les services compétents au sein de la Commission demandent l'avis de la direction générale des ressources humaines et de la sécurité, en particulier la direction de la sécurité, et veillent à ce que les contrats et contrats de sous-traitance types et les conventions de subvention types incluent des dispositions reflétant les principes de base et les normes minimales de protection des ICUE que doivent respecter les contractants et les sous-traitants, de même que les bénéficiaires des conventions de subvention.

3. La Commission collabore étroitement avec l'ANS, l'ASD ou toute autre autorité compétente des États membres concernés.

4. Lorsqu'une autorité contractante envisage de lancer une procédure visant à conclure un contrat classifié ou une convention de subvention classifiée, elle demande l'avis de l'autorité de sécurité de la Commission sur les questions concernant la classification et les éléments de la procédure à tous les stades de celle-ci.

5. Les modèles pour les contrats et contrats de sous-traitance classifiés, les conventions de subvention classifiées, les avis de marché, les documents d'orientation concernant les conditions dans lesquelles des habilitations de sécurité d'établissement (HSE) sont requises, les instructions de sécurité relatives à un programme/un projet (ISP), les annexes de sécurité (AS), les visites, la transmission et le transport d'ICUE dans le cadre de contrats ou de conventions de subvention classifiés, sont établis dans les modalités d'application sur la sécurité industrielle, après consultation du groupe d'experts sécurité de la Commission.

([1]) Règlement (CE, Euratom) n° 1605/2002 du Conseil du 25 juin 2002 portant règlement financier applicable au budget général des Communautés européennes (JO L 248 du 16.9.2002, p. 1).

6. La Commission peut conclure des contrats ou des conventions de subvention classifiés destinés à confier à des opérateurs économiques immatriculés dans un État membre ou dans un État tiers ayant conclu un accord ou un arrangement administratif en vertu du chapitre 7 de la présente décision, des tâches qui impliquent ou nécessitent l'accès, le traitement ou le stockage d'ICUE.

Article 42

Aspects liés à la sécurité dans un contrat classifié ou une convention de subvention classifiée

1. Les contrats classifiés ou les conventions de subvention classifiées incluent les aspects suivants liés à la sécurité:

Instructions de sécurité relatives à un programme/un projet

a) Par «instructions de sécurité relatives à un programme/un projet» (ISP), on entend une liste des procédures de sécurité appliquées à un programme ou à un projet spécifique en vue d'uniformiser ces procédures. Elles peuvent être revues tout au long de la durée du programme ou du projet.

b) La direction générale des ressources humaines et de la sécurité élabore des ISP génériques; les services de la Commission chargés des programmes ou des projets impliquant le traitement ou le stockage d'ICUE peuvent élaborer, le cas échéant, des ISP spécifiques basées sur les ISP génériques.

c) Des ISP spécifiques sont élaborées en particulier pour les programmes et les projets caractérisés par l'importance de leur portée, leur échelle ou leur complexité, ou par la multitude et/ou la diversité des contractants, bénéficiaires et autres partenaires et acteurs impliqués, par exemple en ce qui concerne leur statut juridique. Les ISP spécifiques sont élaborées par le ou les services de la Commission gérant le programme ou le projet, en coopération étroite avec la direction générale des ressources humaines et de la sécurité.

d) La direction générale des ressources humaines et de la sécurité soumet les ISP génériques et spécifiques pour avis au groupe d'experts sécurité de la Commission.

Annexe de sécurité

a) Par «annexe de sécurité» (AS), on entend un ensemble de conditions contractuelles spéciales, établi par l'autorité contractante, qui fait partie intégrante de tout contrat classifié impliquant l'accès à des ICUE ou la création de telles informations, dans lequel sont définis les conditions de sécurité ou les éléments du contrat qui doivent être protégés pour des raisons de sécurité.

b) Les impératifs de sécurité propres à un contrat sont exposés dans une AS. Le cas échéant, l'AS contient le guide de la classification de sécurité (GCS) et fait partie intégrante du contrat ou du contrat de sous-traitance classifié ou de la convention de subvention classifiée.

c) L'AS contient les dispositions imposant au contractant ou au bénéficiaire de respecter les normes minimales énoncées dans la présente décision. L'autorité contractante s'assure que l'AS indique que le non-respect de ces normes minimales peut constituer un motif suffisant de résiliation du contrat ou de la convention de subvention.

2. Les ISP et les AS incluent un GCS en tant qu'élément de sécurité obligatoire:

a) par «guide de la classification de sécurité» (GCS), on entend un document qui décrit les éléments d'un programme, projet, contrat ou convention de subvention qui sont classifiés, et précise les niveaux de classification de sécurité applicables. Le GCS peut être étoffé tout au long de la durée du programme, projet, contrat ou convention de subvention et les éléments d'information peuvent être reclassifiés ou déclassés; lorsqu'il existe, le GCS fait partie de l'AS.

b) Avant de lancer un appel d'offres en vue de l'attribution d'un contrat classifié ou d'attribuer un tel contrat, le service de la Commission, en sa qualité d'autorité contractante, détermine la classification de sécurité de toute information devant être fournie aux candidats, soumissionnaires ou contractants, ainsi que la classification de sécurité de toute information devant être créée par le contractant. Dans cette perspective, il élabore un GCS qui sera utilisé aux fins de l'exécution du contrat, conformément à la présente décision et à ses modalités d'application, après consultation de l'autorité de sécurité de la Commission.

c) Les principes ci-après sont appliqués pour déterminer le niveau de classification de sécurité des différents éléments d'un contrat classifié:

i) dans le cadre de l'élaboration d'un GCS, le service de la Commission, en tant qu'autorité contractante, tient compte de tous les aspects pertinents en matière de sécurité, y compris de la classification de sécurité attribuée aux informations fournies et dont l'utilisation aux fins du contrat a été approuvée par l'autorité d'origine desdites informations;

ii) le niveau général de classification du contrat ne peut pas être inférieur à la classification la plus élevée de l'un de ses éléments; et

iii) le cas échéant, l'autorité contractante se met en rapport, par l'intermédiaire de l'autorité de sécurité de la Commission, avec les ANS, les ASD ou toute autre autorité de sécurité compétente des États membres dans l'éventualité d'une modification touchant au niveau de classification des informations créées par les contractants ou fournies à ceux-ci dans le cadre de l'exécution d'un contrat et lors de toute modification ultérieure du GCS.

Article 43

Accès aux ICUE pour le personnel des contractants et des bénéficiaires

L'autorité contractante ou qui octroie la subvention veille à ce que le contrat classifié ou la convention de subvention classifiée renferme des dispositions indiquant que le personnel d'un contractant, sous-traitant ou bénéficiaire qui, aux fins de l'exécution du contrat, contrat de sous-traitance ou convention de subvention classifié(e), requiert l'accès à des ICUE, peut se voir accorder un tel accès uniquement si les conditions suivantes sont remplies:

a) s'être vu accorder une autorisation de sécurité du niveau correspondant ou avoir été dûment autorisé en fonction de son besoin d'en connaître;

b) avoir été informé des règles de sécurité applicables à la protection des ICUE et avoir reconnu les responsabilités qui lui incombent en matière de protection de ces informations;

c) avoir reçu une habilitation de sécurité du niveau correspondant pour les informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET par l'ANS, l'ASD ou toute autre autorité compétente respective.

Article 44

Habilitation de sécurité d'établissement

1. Par «habilitation de sécurité d'établissement» (HSE), on entend une décision administrative prise par une ANS, une ASD ou toute autre autorité de sécurité compétente selon laquelle, du point de vue de la sécurité, un établissement peut assurer un niveau suffisant de protection pour les ICUE d'un niveau de classification de sécurité déterminé.

2. Une HSE est délivrée par l'ANS, l'ASD ou toute autre autorité de sécurité compétente d'un État membre afin d'indiquer, conformément aux dispositions législatives et réglementaires nationales, qu'un opérateur économique est en mesure, au sein de ses établissements, de garantir aux ICUE la protection adaptée au niveau de classification approprié (CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET). Cette HSE est présentée à l'autorité de sécurité de la Commission qui la transmet au service de la Commission agissant en qualité d'autorité contractante ou octroyant la subvention, avant qu'un candidat, soumissionnaire ou contractant, ou demandeur ou bénéficiaire d'une subvention, puisse recevoir des ICUE ou avoir accès à des ICUE.

3. S'il y a lieu, l'autorité contractante avertit, par l'intermédiaire de l'autorité de sécurité de la Commission, l'ANS, l'ASD ou toute autre autorité de sécurité compétente concernée qu'une HSE est nécessaire pour l'exécution du contrat. Une HSE ou une HSP est requise lorsque des ICUE classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET doivent être fournies dans le cadre de la procédure de passation de marché ou d'octroi de subvention.

4. L'autorité contractante ou qui octroie la subvention n'attribue pas de contrat classifié ou de convention de subvention classifiée au soumissionnaire ou participant sélectionné tant que l'ANS, l'ASD ou toute autre autorité de sécurité compétente de l'État membre dans lequel le contractant ou le soumissionnaire concerné est immatriculé, ne lui a pas confirmé qu'une HSE appropriée a été délivrée.

5. Lorsque l'autorité de sécurité de la Commission a été avertie par l'ANS, l'ASD ou toute autre autorité de sécurité compétente ayant délivré une HSE, de modifications apportées à ladite HSE, elle informe le service de la Commission agissant en qualité d'autorité contractante ou qui octroie la subvention. Dans le cadre d'un contrat de sous-traitance, l'ANS, l'ASD ou toute autre autorité de sécurité compétente en est informée.

6. Pour l'autorité contractante ou qui octroie la subvention, le retrait d'une HSE par l'ANS, l'ASD ou toute autre autorité de sécurité compétente concernée constitue un motif suffisant pour résilier un contrat classifié ou exclure un candidat, soumissionnaire ou demandeur de la procédure d'appel d'offres. Une disposition est incluse à cet effet dans les contrats types et les conventions de subvention types à élaborer.

Article 45

Dispositions applicables aux contrats et conventions de subvention classifiés

1. Lorsque des ICUE sont communiquées à un candidat, soumissionnaire ou demandeur durant la procédure de passation de marché, l'appel d'offres ou l'appel de propositions contient une disposition obligeant le candidat, le soumissionnaire ou le demandeur qui ne présente pas d'offre ou de proposition ou qui n'est pas sélectionné à restituer tous les documents classifiés dans un délai spécifié.

2. L'autorité contractante ou qui octroie la subvention informe, par l'intermédiaire de l'autorité de sécurité de la Commission, l'ANS, l'ASD ou toute autre autorité de sécurité compétente qu'un contrat classifié ou une convention de subvention classifiée a été attribué, et lui communique les données correspondantes, notamment le nom du ou des contractants ou bénéficiaires, la durée du contrat et le niveau maximal de classification.

3. Lorsqu'il est mis fin à un tel contrat ou convention de subvention, l'autorité contractante ou qui octroie la subvention avertit rapidement, par l'intermédiaire de l'autorité de sécurité de la Commission, l'ANS, l'ASD ou toute autre autorité de sécurité compétente de l'État membre dans lequel le contractant ou le bénéficiaire de la subvention est immatriculé.

4. En principe, le contractant ou le bénéficiaire de la subvention est tenu de restituer à l'autorité contractante ou qui octroie la subvention les ICUE en sa possession, dès que le contrat classifié ou la convention de subvention classifiée arrive à expiration ou que la participation d'un bénéficiaire de la subvention arrive à son terme.

5. Des dispositions spéciales concernant l'élimination d'ICUE durant l'exécution du contrat classifié ou de la convention de subvention classifiée ou à son expiration figurent dans l'AS.

6. Lorsque le contractant ou le bénéficiaire de la subvention est autorisé à conserver des ICUE après l'expiration d'un contrat classifié ou d'une convention de subvention classifiée, les normes minimales figurant dans la présente décision demeurent d'application et la confidentialité des ICUE est protégée par le contractant ou le bénéficiaire de la subvention.

Article 46

Dispositions spécifiques applicables aux contrats classifiés

1. Les conditions pertinentes pour la protection des ICUE dans lesquelles le contractant peut sous-traiter des activités sont définies dans l'appel d'offres et le contrat classifié.

2. Un contractant doit obtenir l'autorisation de l'autorité contractante avant de pouvoir sous-traiter des éléments d'un contrat classifié. Aucun contrat de sous-traitance impliquant l'accès à des ICUE ne peut être attribué à des sous-traitants immatriculés dans un pays tiers, sauf s'il existe un cadre règlementaire en matière de sécurité des informations tel qu'il est prévu au chapitre 7.

3. Il incombe au contractant de veiller à ce que toutes les activités de sous-traitance soient réalisées en conformité avec les normes minimales définies dans la présente décision et de s'abstenir de fournir des ICUE à un sous-traitant sans l'autorisation écrite préalable de l'autorité contractante.

4. En ce qui concerne les ICUE créées ou traitées par le contractant, la Commission est considérée comme l'autorité d'origine et les droits qui incombent à l'autorité d'origine sont exercés par l'autorité contractante.

Article 47

Visites liées à des contrats classifiés

1. Lorsque des membres du personnel de la Commission, des contractants ou des bénéficiaires de subvention doivent avoir accès à des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET dans leurs locaux respectifs aux fins de l'exécution d'un contrat classifié ou d'une convention de subvention classifiée, les visites sont organisées en liaison avec les ANS, les ASD ou toute autre autorité de sécurité compétente concernée. L'autorité de sécurité de la Commission est informée de ces visites. Toutefois, dans le cadre de programmes ou projets spécifiques, les ANS, les ASD ou toute autre autorité de sécurité compétente peuvent également convenir d'une procédure selon laquelle ces visites peuvent être organisées directement.

2. Tous les visiteurs sont en possession d'une habilitation de sécurité adéquate et jouissent d'un accès aux ICUE liées au contrat classifié sur la base du principe du besoin d'en connaître.

3. Les visiteurs se voient uniquement accorder l'accès aux ICUE liées à l'objectif de la visite.

4. Les modalités d'application contiennent des dispositions plus détaillées.

5. Le respect des dispositions concernant les visites liées à des contrats classifiés définies dans la présente décision et dans les modalités d'application visées au paragraphe 4 est obligatoire.

Article 48

Transmission et transport d'ICUE en relation avec des contrats classifiés ou des conventions de subvention classifiées

1. En ce qui concerne la transmission des ICUE par voie électronique, les dispositions pertinentes du chapitre 5 de la présente décision s'appliquent.

2. En ce qui concerne le transport d'ICUE, les dispositions pertinentes du chapitre 4 de la présente décision et de ses modalités d'application s'appliquent, conformément aux dispositions législatives et réglementaires nationales.

3. En ce qui concerne le transport de matériel classifié en tant que fret, les principes ci-après s'appliquent pour déterminer les mesures de sécurité à mettre en œuvre:

a) la sécurité est assurée à tous les stades pendant le transport, du point d'origine jusqu'à la destination finale;

b) le degré de protection accordé à un envoi est déterminé en fonction du niveau de classification le plus élevé du matériel qu'il contient;

c) avant tout transfert transfrontalier de matériel classifié CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET, un plan de transport est établi par l'expéditeur et approuvé par l'ANS, l'ASD ou toute autre autorité de sécurité compétente concernée;

d) les trajets sont directs dans la mesure du possible, et aussi rapides que les circonstances le permettent;

e) chaque fois que cela est possible, les itinéraires ne devraient passer que par des États membres. Les itinéraires passant par des États autres que les États membres ne devraient être suivis qu'à condition d'avoir été autorisés par l'ANS, l'ASD ou toute autre autorité de sécurité compétente des États de l'expéditeur et du destinataire.

Article 49

Transfert d'ICUE aux contractants ou bénéficiaires de subvention établis dans des États tiers

Les ICUE sont transférées aux contractants ou bénéficiaires de subvention établis dans des États tiers conformément aux mesures de sécurité convenues entre l'autorité de sécurité de la Commission, le service de la Commission, en sa qualité d'autorité contractante ou octroyant la subvention, et l'ANS, l'ASD ou toute autre autorité de sécurité compétente de l'État tiers concerné dans lequel le contractant ou le bénéficiaire de la subvention est immatriculé.

Article 50

Traitement d'informations classifiées RESTREINT UE/EU RESTRICTED dans le cadre de contrats classifiés ou de conventions de subvention classifiées

1. La protection des informations classifiées RESTREINT UE/EU RESTRICTED traitées ou stockées dans le cadre de contrats classifiés ou de conventions de subvention classifiées est fondée sur les principes de proportionnalité et de rentabilité.

2. Aucune HSE ni HSP n'est requise dans le cadre de contrats classifiés ou de conventions de subvention classifiées impliquant le traitement d'informations classifiées au niveau RESTREINT UE/EU RESTRICTED.

3. Lorsqu'un contrat ou une convention de subvention prévoit le traitement d'informations classifiées RESTREINT UE/EU RESTRICTED dans un SIC exploité par un contractant ou un bénéficiaire de subvention, l'autorité contractante ou octroyant la subvention veille, après avoir consulté l'autorité de sécurité de la Commission, à ce que les exigences techniques et administratives à remplir concernant l'homologation du SIC soient précisées dans le contrat ou la convention de subvention; ces exigences sont proportionnées au risque évalué, compte tenu de tous les facteurs pertinents. La portée de l'homologation dudit SIC est décidée d'un commun accord par l'autorité de sécurité de la Commission et l'ANS ou ASD compétente.

CHAPITRE 7

ÉCHANGE D'INFORMATIONS CLASSIFIÉES AVEC D'AUTRES INSTITUTIONS, AGENCES, ORGANES ET ORGANISMES DE L'UNION, AVEC DES ÉTATS MEMBRES ET AVEC DES ÉTATS TIERS ET DES ORGANISATIONS INTERNATIONALES

Article 51

Principes de base

1. Dans le cas où la Commission ou l'un de ses services établit qu'il est nécessaire d'échanger des ICUE avec une autre institution, agence, organe ou organisme de l'Union, ou avec un État tiers ou une organisation internationale, les mesures nécessaires sont prises afin d'instituer un cadre juridique ou administratif approprié à cette fin, pouvant comprendre des accords sur la sécurité des informations ou des arrangements administratifs conclus conformément aux dispositions réglementaires applicables.

2. Sans préjudice de l'article 57, les ICUE sont échangées avec une autre institution, agence, organe ou organisme de l'Union, ou avec un État tiers ou une organisation internationale, uniquement si un tel cadre juridique ou administratif approprié est mis en place et qu'il existe des garanties suffisantes indiquant que l'institution, agence, organe ou organisme de l'Union ou l'État tiers ou l'organisation internationale en question applique des principes de base et des normes minimales équivalents pour la protection des informations classifiées.

Article 52

Échange d'ICUE avec d'autres institutions, agences, organes et organismes de l'Union

1. Avant de conclure un arrangement administratif pour l'échange d'ICUE avec une autre institution, agence, organe ou organisme de l'Union, la Commission s'assure que celle-ci ou celui-ci:

a) dispose d'un cadre réglementaire pour la protection des ICUE établissant des principes de base et des normes minimales équivalents à ceux énoncés dans la présente décision et ses modalités d'application;

b) applique des normes de sécurité et des lignes directrices concernant la sécurité du personnel, la sécurité physique, la gestion des ICUE et la sécurité des systèmes d'information et de communication (SIC) garantissant un niveau de protection des ICUE équivalent à celui appliqué au sein de la Commission;

c) marque les informations classifiées qu'il ou elle crée comme ICUE.

2. En étroite coopération avec les autres services compétents de la Commission, la direction générale des ressources humaines et de la sécurité est le service chef de file au sein de la Commission pour la conclusion d'arrangements administratifs pour l'échange d'ICUE avec d'autres institutions, agences, organes ou organismes de l'Union.

3. Les arrangements administratifs prennent, en règle générale, la forme d'un échange de lettres, signées par le directeur général des ressources humaines et de la sécurité au nom de la Commission.

4. Avant de conclure un arrangement administratif sur l'échange d'ICUE, l'autorité de sécurité de la Commission effectue une visite d'évaluation visant à évaluer le cadre réglementaire pour la protection des ICUE et s'assurer de l'efficacité des mesures mises en œuvre pour protéger les ICUE. L'arrangement administratif prend effet et les ICUE sont échangées uniquement si le résultat de cette visite d'évaluation est satisfaisant et que les recommandations émises à la suite de la visite sont respectées. Des visites de suivi régulières sont effectuées afin de vérifier que l'arrangement administratif est respecté et que les mesures de sécurité mises en place continuent de répondre aux principes de base et normes minimales convenus.

5. Au sein de la Commission, le bureau d'ordre géré par le secrétariat général représente, en règle générale, le principal point d'entrée et de sortie des échanges d'informations classifiées avec d'autres institutions, agences, organes et organismes de l'Union. Toutefois, si pour des raisons de sécurité, d'organisation ou de fonctionnement, cela s'avère plus approprié pour protéger les ICUE, des bureaux d'ordre locaux sont établis au sein des services de la Commission conformément à la présente décision et à ses modalités d'application; ces bureaux servent de point d'entrée et de sortie pour les informations classifiées concernant des sujets relevant de la compétence des services de la Commission concernés.

6. Le groupe d'experts sécurité de la Commission est informé du processus de conclusion d'arrangements administratifs conformément au paragraphe 2.

Article 53

Échange d'ICUE avec les États membres

1. Des ICUE peuvent être échangées avec les États membres et leur être communiquées à condition qu'ils protègent ces informations classifiées conformément aux exigences applicables aux informations classifiées portant un marquage national de classification de sécurité de niveau équivalent, tel que prévu dans le tableau d'équivalence des classifications de sécurité figurant à l'annexe I.

2. Lorsque les États membres introduisent des informations classifiées portant un marquage national de classification de sécurité dans les structures ou réseaux de l'Union européenne, la Commission protège ces informations conformément aux règles applicables aux ICUE de niveau équivalent tel que prévu dans le tableau d'équivalence des classifications de sécurité figurant à l'annexe I.

Article 54

Échange d'ICUE avec des États tiers et des organisations internationales

1. Lorsque la Commission établit qu'il existe un besoin durable d'échanger des informations classifiées avec des États tiers ou des organisations internationales, les mesures nécessaires sont prises pour instituer un cadre juridique ou administratif approprié à cette fin, pouvant comprendre de accords sur la sécurité des informations ou des arrangements administratifs conclus conformément aux dispositions réglementaires applicables.

2. Les accords sur la sécurité des informations ou les arrangements administratifs visés au paragraphe 1 contiennent des dispositions pour garantir que, lorsque des États tiers ou des organisations internationales reçoivent des ICUE, ces informations bénéficient d'une protection conforme à leur niveau de classification et à des normes minimales équivalentes à celles prévues dans la présente décision.

3. La Commission peut conclure des arrangements administratifs, conformément à l'article 56, lorsque le niveau de classification des ICUE n'est en règle générale pas supérieur à RESTREINT UE/EU RESTRICTED.

4. Les arrangements administratifs pour l'échange d'informations classifiées visés au paragraphe 3 contiennent des dispositions pour garantir que, lorsque des États tiers ou des organisations internationales reçoivent des ICUE, ces informations bénéficient d'une protection conforme à leur niveau de classification et à des normes minimales équivalentes à celles prévues dans la présente décision. Le groupe d'experts sécurité de la Commission est consulté sur la conclusion d'accords sur la sécurité des informations ou d'arrangements administratifs.

5. La décision de communiquer des ICUE émanant de la Commission à un État tiers ou à une organisation internationale est prise par le service de la Commission, en tant qu'autorité d'origine des ICUE concernées au sein de la Commission, au cas par cas, en fonction de la nature et du contenu de ces informations, du besoin d'en connaître du destinataire et d'une appréciation des avantages que l'Union peut en retirer. Si l'autorité d'origine des informations classifiées à communiquer, ou des sources qu'elles peuvent contenir, n'est pas la Commission, le service de la Commission qui détient ces informations classifiées demande au préalable le consentement écrit de l'autorité d'origine. Au cas où l'autorité d'origine ne peut être identifiée, le service de la Commission qui détient ces informations classifiées assume cette responsabilité en lieu et place de l'autorité d'origine après avoir consulté le groupe d'experts sécurité de la Commission.

Article 55

Accords sur la sécurité des informations

1. Les accords sur la sécurité des informations avec des États tiers ou des organisations internationales sont conclus conformément à l'article 218 du TFUE.

2. Les accords sur la sécurité des informations:

a) fixent les principes de base et les normes minimales régissant l'échange d'informations classifiées entre l'Union et un État tiers ou une organisation internationale;

b) prévoient des modalités techniques d'application qui doivent être arrêtées d'un commun accord entre les autorités de sécurité compétentes des institutions et organes de l'Union concernés et l'autorité de sécurité compétente de l'État tiers ou de l'organisation internationale concerné(e). Ces modalités tiennent compte du niveau de protection offert par les règlements, les structures et les procédures de sécurité en vigueur au sein de l'État tiers ou de l'organisation internationale concerné(e);

c) prévoient que, préalablement à l'échange d'informations classifiées au titre de l'accord, il a été vérifié que la partie destinataire est apte à protéger et sauvegarder de manière appropriée les informations classifiées qui lui sont transmises.

3. Lorsque la nécessité d'échanger des informations classifiées est établie conformément à l'article 51, paragraphe 1, la Commission consulte le Service européen pour l'action extérieure, le secrétariat général du Conseil et d'autres institutions et organes de l'Union, le cas échéant, afin de déterminer s'il y a lieu de soumettre une recommandation conformément à l'article 218, paragraphe 3, du TFUE.

4. Les ICUE ne font l'objet d'aucun échange par voie électronique, sauf disposition expresse de l'accord sur la sécurité des informations ou des modalités techniques d'application.

5. Au sein de la Commission, le bureau d'ordre géré par le secrétariat général représente, en règle générale, le principal point d'entrée et de sortie des échanges d'informations classifiées avec des États tiers et des organisations internationales. Toutefois, si pour des raisons de sécurité, d'organisation ou de fonctionnement, cela s'avère plus approprié pour protéger les ICUE, des bureaux d'ordre locaux sont établis au sein des services de la Commission conformément à la présente décision et à ses modalités d'application; ces bureaux servent de point d'entrée et de sortie pour les informations classifiées concernant des sujets relevant de la compétence des services de la Commission concernés.

6. Afin d'évaluer l'efficacité des règlements, structures et procédures de sécurité en vigueur dans l'État tiers ou l'organisation internationale concerné(e), la Commission participe à des visites d'évaluation en collaboration avec d'autres institutions, agences ou organes de l'Union, d'un commun accord avec l'État tiers ou l'organisation internationale concerné(e). Ces visites d'évaluation ont pour finalité d'évaluer:

a) le cadre réglementaire applicable à la protection des informations classifiées;

b) tous les aspects spécifiques de la politique de sécurité et du mode d'organisation de la sécurité dans l'État tiers ou l'organisation internationale susceptibles d'avoir une incidence sur le niveau des informations classifiées qui peuvent être échangées;

c) les mesures et les procédures de sécurité effectivement en place; et

d) les procédures d'habilitation de sécurité pour le niveau de classification des ICUE à communiquer.

Article 56

Arrangements administratifs

1. Lorsqu'il existe un besoin durable, dans le contexte d'un cadre politique ou juridique de l'Union, d'échanger avec un État tiers ou une organisation internationale des informations dont le niveau de classification n'est en principe pas supérieur à RESTREINT UE/EU RESTRICTED, et que l'autorité de sécurité de la Commission, après avoir consulté le groupe d'experts sécurité de la Commission, a établi, notamment, que la partie en question ne dispose pas d'un système de sécurité suffisamment développé lui permettant de conclure un accord sur la sécurité des informations, la Commission peut décider de conclure un arrangement administratif avec les autorités compétentes de l'État tiers ou de l'organisation internationale concerné(e).

2. Ces arrangements administratifs prennent, en règle générale, la forme d'un échange de lettres.

3. Une visite d'évaluation est réalisée préalablement à la conclusion de l'arrangement. Le groupe d'experts sécurité de la Commission est informé du résultat de la visite d'évaluation. Si des raisons exceptionnelles justifient l'échange urgent d'informations classifiées, les ICUE peuvent être communiquées à condition que tout soit mis en œuvre pour effectuer dès que possible une visite d'évaluation.

4. Les ICUE ne font l'objet d'aucun échange par voie électronique, sauf disposition expresse de l'arrangement administratif.

Article 57

Communication ad hoc exceptionnelle d'ICUE

1. S'il n'existe aucun accord sur la sécurité des informations ni arrangement administratif, et si la Commission ou l'un de ses services décide qu'il est nécessaire, à titre exceptionnel dans le contexte d'un cadre politique ou juridique de l'Union, de communiquer des ICUE à un État tiers ou à une organisation internationale, l'autorité de sécurité de la Commission vérifie, dans la mesure du possible, auprès des autorités de sécurité de l'État tiers ou de l'organisation internationale concerné(e) que son règlement, ses structures et ses procédures de sécurité permettent de garantir que les ICUE qui lui seront communiquées bénéficieront d'une protection conforme à des normes qui ne sont pas moins strictes que celles prévues dans la présente décision.

2. La décision de communiquer des ICUE à l'État tiers ou à l'organisation internationale concerné(e) est prise, après consultation du groupe d'experts sécurité de la Commission, par la Commission sur la base d'une proposition du membre de la Commission chargé des questions de sécurité.

3. Lorsqu'une décision de communiquer des ICUE a été prise par la Commission et sous réserve du consentement de l'autorité d'origine, y compris des auteurs des sources qu'elles peuvent contenir, le service de la Commission compétent transmet les informations concernées, qui portent un marquage relatif à la communicabilité indiquant l'État tiers ou l'organisation internationale auquel elles ont été communiquées. Avant la communication effective ou au moment de celle-ci, la tierce partie concernée s'engage par écrit à protéger les ICUE qui lui sont transmises conformément aux principes de base et aux normes minimales prévus dans la présente décision.

CHAPITRE 8

DISPOSITIONS FINALES

Article 58

Remplacement de la décision précédente

La présente décision abroge et remplace la décision 2001/844/CE, CECA, Euratom de la Commission ([1]).

Article 59

Informations classifiées créées avant l'entrée en vigueur de la présente décision

1. Toutes les ICUE portant un marquage en application de la décision 2001/844/CE, CECA, Euratom continuent d'être protégées conformément aux dispositions pertinentes de la présente décision.

2. Toutes les informations classifiées détenues par la Commission à la date d'entrée en vigueur de la décision 2001/844/CE, CECA, Euratom, à l'exception des informations classifiées Euratom:

a) lorsqu'elles ont été créées par la Commission, restent considérées comme reclassifiées par défaut dans la catégorie RESTREINT UE, à moins que leur auteur n'ait décidé de leur attribuer une autre classification au plus tard le 31 janvier 2002 et n'en ait informé tous les destinataires du document concerné;

b) lorsqu'elles ont été créées par des personnes extérieures à la Commission, sont maintenues dans leur classification originelle et donc traitées comme des ICUE du même niveau, à moins que l'auteur n'accepte de les déclassifier ou de les déclasser.

Article 60

Modalités d'application et notes de sécurité

1. Au besoin, l'adoption des modalités d'application de la présente décision feront l'objet d'une décision d'habilitation distincte de la Commission en faveur du membre de la Commission chargé des questions de sécurité, conformément au règlement intérieur.

2. Après avoir été habilité à la suite de la décision de la Commission susvisée, le membre de la Commission chargé des questions de sécurité peut rédiger des notes de sécurité définissant des lignes directrices et des bonnes pratiques en matière de sécurité dans le cadre du champ d'application de la présente décision et de ses modalités d'application.

3. La Commission peut déléguer les tâches mentionnées dans les premier et deuxième paragraphes du présent article au directeur général des ressources humaines et de la sécurité au moyen d'une décision de délégation distincte, conformément au règlement intérieur.

Article 61

Entrée en vigueur

La présente décision entre en vigueur le jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Fait à Bruxelles, le 13 mars 2015.

Par la Commission

Le président

Jean-Claude JUNCKER

([1]) Décision 2001/844/CE, CECA, Euratom de la Commission du 29 novembre 2001 modifiant son règlement intérieur (JO L 317 du 3.12.2001, p. 1).

ANNEXE I

ÉQUIVALENCE DES CLASSIFICATIONS DE SÉCURITÉ

UE	TRÈS SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Euratom	EURA TOP SECRET	EURA SECRET	EURA CONFIDENTIAL	EURA RESTRICTED
Belgique	Très Secret (Loi 11.12.1998) Zeer Geheim (Wet 11.12.1998)	Secret (Loi 11.12.1998) Geheim (Wet 11.12.1998)	Confidentiel (Loi 11.12.1998) Vertrouwelijk (Wet 11.12.1998)	Note (1) ci-dessous
Bulgarie	Строго секретно	Секретно	Поверително	За служебно ползване
République tchèque	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Danemark	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Allemagne	Streng geheim	Geheim	VS (2) — Vertraulich	VS — Nur für den Dienst-gebrauch
Estonie	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Irlande	Top Secret	Secret	Confidential	Restricted
Grèce	Άκρως Απόρρητο Abr: ΑΑΠ	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Espagne	Secreto	Reservado	Confidencial	Difusión Limitada
France	Très Secret Défense	Secret Défense	Confidentiel Défense	Note (3) ci-dessous
Croatie	VRLO TAJNO	TAJNO	POVJERLJIVO	OGRANIČENO
Italie	Segretissimo	Segreto	Riservatissimo	Riservato
Chypre	Άκρως Απόρρητο Abr: (ΑΑΠ)	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Lettonie	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Lituanie	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Luxembourg	Très Secret Lux	Secret Lux	Confidentiel Lux	Restreint Lux
Hongrie	«Szigorúan titkos!»	«Titkos!»	«Bizalmas!»	«Korlátozott terjesztésű!»
Malte	L-Oġhla Segretezza	Sigriet	Kunfidenzjali	Ristrett
Pays-Bas	Stg. ZEER GEHEIM	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep. VERTROUWELIJK
Autriche	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Pologne	Ściśle Tajne	Tajne	Poufne	Zastrzeżone
Portugal	Muito Secreto	Secreto	Confidencial	Reservado

UE	TRÈS SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Roumanie	Strict secret de importanță deosebită	Strict secret	Secret	Secret de serviciu
Slovénie	Strogo tajno	Tajno	Zaupno	Interno
Slovaquie	Prísne tajné	Tajné	Dôverné	Vyhradené
Finlande	ERITTÄIN SALAINEN YTTERST HEMLIG	SALAINEN HEMLIG	LUOTTAMUKSELLINEN KONFIDENTIELL	KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG
Suède (4)	HEMLIG/TOP SECRET HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET	HEMLIG/SECRET HEMLIG	HEMLIG/CONFIDENTIAL HEMLIG	HEMLIG/RESTRICTED HEMLIG
Royaume-Uni	UK TOP SECRET	UK SECRET	Pas d'équivalence (5)	UK OFFICIAL — SENSITIVE

(1) La classification «Diffusion restreinte/Beperkte Verspreiding» n'est pas une classification de sécurité en Belgique. La Belgique traite et protège les informations RESTREINT UE/EU RESTRICTED d'une manière qui n'est pas moins stricte que les normes et procédures décrites dans le règlement de sécurité du Conseil de l'Union européenne.

(2) Allemagne: VS = Verschlusssache.

(3) La France n'utilise pas la catégorie de classification «RESTREINT» dans son système national. Elle traite et protège les informations RESTREINT UE/EU RESTRICTED d'une manière qui n'est pas moins stricte que les normes et procédures décrites dans le règlement de sécurité du Conseil de l'Union européenne.

(4) Suède: les marquages de classification de sécurité de la première ligne sont utilisés par les autorités chargées de la défense et les marquages de la deuxième ligne par les autres autorités.

(5) Le Royaume-Uni traite et protège les ICUE marquées CONFIDENTIEL UE/EU CONFIDENTIAL conformément aux exigences de sécurité relatives à la protection des informations classifiées UK SECRET.

ANNEXE II

LISTE DES ABRÉVIATIONS

Acronyme	Signification
AC	Autorité Crypto
AAC	Autorité d'agrément cryptographique
CCTV	Closed Circuit Television — système de télévision en circuit fermé (vidéosurveillance)
ADC	Autorité de distribution cryptographique
SIC	Systèmes d'information et de communication traitant des ICUE
ASD	Autorité de sécurité désignée
ICUE	Informations classifiées de l'Union européenne
HSE	Habilitation de sécurité d'établissement
AI	Assurance de l'information
AAI	Autorité chargée de l'assurance de l'information
SDI	Système de détection des intrusions
TI	Technologies de l'information
LSO	Responsable local de la sécurité
ANS	Autorité nationale de sécurité
HSP	Habilitation de sécurité du personnel
CHSP	Certificat d'habilitation de sécurité du personnel
ISP	Instructions de sécurité relatives à un programme/un projet
RCO	Agent contrôleur
AHS	Autorité d'homologation de sécurité
AS	Annexe de sécurité
GCS	Guide de la classification de sécurité
SecOP	Procédures d'exploitation de sécurité
AT	Autorité TEMPEST
TFUE	Traité sur le fonctionnement de l'Union européenne

ANNEXE III

LISTE DES AUTORITÉS NATIONALES DE SÉCURITÉ

BELGIQUE

Autorité nationale de Sécurité
SPF Affaires étrangères, Commerce extérieur et Coopération au Développement
15, rue des Petits Carmes
1000 Bruxelles
Téléphone secrétariat: +32 25014542
Fax +32 25014596
E-mail: nvo-ans@diplobel.fed.be

BULGARIE

State Commission on Information Security
90 Cherkovna Str.
1505 Sofia
Téléphone +359 29333600
Fax +359 29873750
E-mail: dksi@government.bg
Site web: www.dksi.bg

RÉPUBLIQUE TCHÈQUE

Národní bezpečnostní úřad
(National Security Authority)
Na Popelce 2/16
150 06 Praha 56
Téléphone +420 257283335
Fax +420 257283110
E-mail: czech.nsa@nbu.cz
Site web: www.nbu.cz

DANEMARK

Politiets Efterretningstjeneste
(Danish Security Intelligence Service)
Klausdalsbrovej 1
2860 Søborg
Téléphone +45 33148888
Fax +45 33430190

Forsvarets Efterretningstjeneste
(Danish Defence Intelligence Service)
Kastellet 30
2100 Copenhagen Ø
Téléphone +45 33325566
Fax +45 33931320

ALLEMAGNE

Bundesministerium des Innern
Referat ÖS III 3
Alt-Moabit 101 D
D-11014 Berlin
Téléphone +49 30186810
Fax +49 30186811441
E-mail: oesIII3@bmi.bund.de

ESTONIE

National Security Authority Department
Estonian Ministry of Defence
Sakala 1
15094 Tallinn
Téléphone +372 717 0019, +372 7170117
Fax +372 7170213
E-mail: nsa@mod.gov.ee

GRÈCE

Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ)
Διακλαδική Διεύθυνση Στρατιωτικών Πληροφοριών (ΔΔΣΠ)
Διεύθυνση Ασφαλείας και Αντιπληροφοριών
ΣΤΓ 1020 -Χολαργός (Αθήνα)
Ελλάδα
Τηλ.: +30 2106572045 (ώρες γραφείου)
+ 30 2106572009 (ώρες γραφείου)
Φαξ: +30 2106536279; + 30 2106577612

Hellenic National Defence General Staff (HNDGS)
Military Intelligence Sectoral Directorate
Security Counterintelligence Directorate
GR-STG 1020 Holargos — Athens
Téléphone +30 2106572045
+ 30 2106572009
Fax +30 2106536279, +30 2106577612

ESPAGNE

Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Avenida Padre Huidobro s/n
28023 Madrid
Téléphone +34 913725000
Fax +34 913725808
E-mail: nsa-sp@areatec.com

FRANCE

Secrétariat général de la défense et de la sécurité nationale
Sous-direction Protection du secret (SGDSN/PSD)
51 Boulevard de la Tour-Maubourg
75700 Paris 07 SP
Téléphone +33 171758177
Fax + 33 171758200

CROATIE

Office of the National Security Council
Croatian NSA
Jurjevska 34
10000 Zagreb
Croatia
Téléphone +385 14681222
Fax + 385 14686049
Site web: www.uvns.hr

IRLANDE

National Security Authority
Department of Foreign Affairs
76 — 78 Harcourt Street
Dublin 2
Téléphone +353 14780822
Fax +353 14082959

ITALIE

Presidenza del Consiglio dei Ministri
D.I.S. — U.C.Se.
Via di Santa Susanna, 15
00187 Roma
Téléphone +39 0661174266
Fax +39 064885273

CHYPRE

ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ
ΣΤΡΑΤΙΩΤΙΚΟ ΕΠΙΤΕΛΕΙΟ ΤΟΥ ΥΠΟΥΡΓΟΥ
Εθνική Αρχή Ασφάλειας (ΕΑΑ)
Υπουργείο Άμυνας
Λεωφόρος Εμμανουήλ Ροΐδη 4
1432 Λευκωσία, Κύπρος
Τηλέφωνα: +357 22807569, +357 22807643,
+357 22807764
Τηλεομοιότυπο: +357 22302351

Ministry of Defence
Minister's Military Staff
National Security Authority (NSA)
4 Emanuel Roidi street
1432 Nicosia
Téléphone +357 22807569, +357 22807643,
+357 22807764
Fax +357 22302351
E-mail: cynsa@mod.gov.cy

LETTONIE

National Security Authority
Constitution Protection Bureau of the Republic of Latvia
P.O.Box 286
LV-1001 Riga
Téléphone +371 67025418
Fax +371 67025454
E-mail: ndi@sab.gov.lv

LITUANIE

Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija
(The Commission for Secrets Protection Coordination of the Republic of Lituania National Security Authority)
Gedimino 40/1
LT-01110 Vilnius
Téléphone +370 706 66701, +370 706 66702
Fax +370 706 66700
E-mail: nsa@vsd.lt

LUXEMBOURG

Autorité nationale de Sécurité
Boîte postale 2379
1023 Luxembourg
Téléphone +352 24782210 central
+ 352 24782253 direct
Fax +352 24782243

HONGRIE

Nemzeti Biztonsági Felügyelet
(National Security Authority of Hungary)
H-1024 Budapest, Szilágyi Erzsébet fasor 11/B
Téléphone +36 (1) 7952303
Fax +36 (1) 7950344

Adresse postale:
H-1357 Budapest, PO Box 2
E-mail: nbf@nbf.hu
Site web: www.nbf.hu

MALTE

Ministry for Home Affairs and National Security
P.O. Box 146
MT-Valletta
Téléphone +356 21249844
Fax +356 25695321

PAYS-BAS

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Postbus 20010
2500 EA Den Haag
Téléphone +31 703204400
Fax +31 703200733

Ministerie van Defensie
Beveiligingsautoriteit
Postbus 20701
2500 ES Den Haag
Téléphone +31 703187060
Fax +31 703187522

AUTRICHE

Informationssicherheitskommission
Bundeskanzleramt
Ballhausplatz 2
1014 Wien
Téléphone +43 1531152594
Fax +43 1531152615
E-mail: ISK@bka.gv.at

POLOGNE

Agencja Bezpieczeństwa Wewnętrznego — ABW
(Internal Security Agency)
2A Rakowiecka St.
00-993 Warszawa
Téléphone +48 22 58 57 944
Fax +48 22 58 57 443
E-mail: nsa@abw.gov.pl
Site web: www.abw.gov.pl

PORTUGAL

Presidência do Conselho de Ministros
Autoridade Nacional de Segurança
Rua da Junqueira, 69
1300-342 Lisboa
Téléphone +351 213031710
Fax +351 213031711

ROUMANIE

Oficiul Registrului Național al Informațiilor Secrete de Stat
(Romanian NSA — ORNISS National Registry Office for Classified Information)
4 Mures Street
012275 Bucharest
Téléphone +40 212245830
Fax +40 212240714
E-mail: nsa.romania@nsa.ro
Site web: www.orniss.ro

SLOVÉNIE

Urad Vlade RS za varovanje tajnih podatkov
Gregorčičeva 27
1000 Ljubljana
Téléphone +386 14781390
Fax +386 14781399
E-mail: gp.uvtp@gov.si

SLOVAQUIE

Národný bezpečnostný úrad
(National Security Authority)
Budatínska 30
P.O. Box 16
850 07 Bratislava
Téléphone +421 268692314
Fax +421 263824005
Site web: www.nbusr.sk

FINLANDE

National Security Authority
Ministry for Foreign Affairs
P.O. Box 453
FI-00023 Government
Téléphone 16055890
Fax +358 916055140
E-mail: NSA@formin.fi

SUÈDE

Utrikesdepartementet
(Ministry for Foreign Affairs)
SSSB
S-103 39 Stockholm
Téléphone +46 84051000
Fax +46 87231176
E-mail: ud-nsa@foreign.ministry.se

ROYAUME-UNI

UK National Security Authority
Room 335, 3rd Floor
70 Whitehall
London
SW1A 2AS
Téléphone 1: +44 2072765649
Téléphone 2: +44 2072765497
Fax +44 2072765651
E-mail: UK-NSA@cabinet-office.x.gsi.gov.uk

II

(Actes non législatifs)

DÉCISIONS

DÉCISION DU CONSEIL

du 23 septembre 2013

concernant les règles de sécurité aux fins de la protection des informations classifiées de l'Union européenne

(2013/488/UE)

LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 240, paragraphe 3,

vu la décision 2009/937/UE du Conseil du 1er décembre 2009 portant adoption de son règlement intérieur [1], et notamment son article 24,

considérant ce qui suit:

(1) Afin de développer les activités du Conseil dans tous les domaines qui requièrent le traitement d'informations classifiées, il convient de mettre en place un système de sécurité global aux fins de la protection des informations classifiées couvrant le Conseil, son secrétariat général et les États membres.

(2) La présente décision devrait s'appliquer lorsque le Conseil, ses instances préparatoires et son secrétariat général (SGC) traitent des informations classifiées de l'Union européenne (ICUE).

(3) Conformément aux dispositions législatives et réglementaires nationales et dans la mesure requise pour le fonctionnement du Conseil, les États membres devraient respecter la présente décision lorsque leurs autorités compétentes, leur personnel ou leurs contractants traitent des ICUE, afin que chacun puisse avoir la certitude qu'un niveau équivalent de protection est assuré pour les ICUE.

(4) Le Conseil, la Commission et le Service européen pour l'action extérieure (SEAE) sont résolus à appliquer des normes équivalentes de sécurité pour protéger les ICUE.

(5) Le Conseil souligne qu'il importe d'associer, le cas échéant, le Parlement européen et d'autres institutions, organes, organismes ou agences de l'Union aux principes, aux normes et à la réglementation relatifs à la protection des informations classifiées qui sont nécessaires pour protéger les intérêts de l'Union et de ses États membres.

(6) Le Conseil devrait déterminer le cadre approprié pour l'échange des ICUE détenues par le Conseil avec d'autres institutions, organes, organismes ou agences, de l'Union, le cas échéant, conformément à la présente décision et aux arrangements interinstitutionnels en vigueur;

(7) Les organes et les agences de l'Union créés en vertu du titre V, chapitre 2, du traité sur l'Union européenne (TUE), Europol et Eurojust devraient appliquer, dans le cadre de leur organisation interne, les principes de base et les normes minimales énoncés dans la présente décision aux fins de la protection des ICUE, lorsque le prévoit l'acte qui les établit.

(8) Les règles de sécurité adoptées par le Conseil aux fins de la protection des ICUE devraient être appliquées dans le cadre des opérations de gestion de crise mises en place en vertu du titre V, chapitre 2, du traité sur l'Union européenne et par leur personnel, comme le prévoit l'acte du Conseil établissant ces opérations.

(9) Les représentants spéciaux de l'Union et les membres de leurs équipes devraient appliquer les règles de sécurité adoptées par le Conseil aux fins de la protection des ICUE, comme le prévoit l'acte du Conseil correspondant.

(10) La présente décision est arrêtée sans préjudice des articles 15 et 16 du traité sur le fonctionnement de l'Union européenne (TFUE), ni des instruments les mettant en œuvre.

(11) La présente décision est arrêtée sans préjudice des pratiques en vigueur au sein des États membres en matière d'information de leurs parlements nationaux sur les activités de l'Union.

[1] JO L 325 du 11.12.2009, p. 35.

(12) Afin que les règles de sécurité aux fins de la protection des ICUE soient appliquées en temps utile eu égard à l'adhésion de la République de Croatie à l'Union européenne, il convient que la présente décision entre en vigueur à la date de sa publication,

A ADOPTÉ LA PRÉSENTE DÉCISION:

Article premier

Objectif, champ d'application et définitions

1. La présente décision définit les principes de base et les normes de sécurité minimales pour la protection ICUE.

2. Ces principes de base et normes minimales s'appliquent au Conseil et au SGC et sont respectés par les États membres, conformément à leurs dispositions législatives et réglementaires nationales, afin que chacun puisse avoir la certitude qu'un niveau équivalent de protection est assuré pour les ICUE.

3. Aux fins de la présente décision, les définitions figurant à l'appendice A s'appliquent.

Article 2

Définition des ICUE, classifications et marquages de sécurité

1. Par «informations classifiées de l'Union européenne» (ICUE), on entend toute information ou tout matériel identifié comme tel par la classification de sécurité de l'Union européenne, dont la divulgation non autorisée pourrait porter atteinte à des degrés divers aux intérêts de l'Union européenne, ou à ceux d'un ou de plusieurs de ses États membres.

2. Les ICUE relèvent de l'un des niveaux de classification suivants:

a) TRÈS SECRET UE/EU TOP SECRET: informations et matériels dont la divulgation non autorisée pourrait causer un préjudice exceptionnellement grave aux intérêts essentiels de l'Union européenne ou d'un ou de plusieurs de ses États membres;

b) SECRET UE/EU SECRET: informations et matériels dont la divulgation non autorisée pourrait nuire gravement aux intérêts essentiels de l'Union européenne ou d'un ou de plusieurs de ses États membres;

c) CONFIDENTIEL UE/EU CONFIDENTIAL: informations et matériels dont la divulgation non autorisée pourrait nuire aux intérêts essentiels de l'Union européenne ou d'un ou de plusieurs de ses États membres;

d) RESTREINT UE/EU RESTRICTED: informations et matériels dont la divulgation non autorisée pourrait être défavorable aux intérêts de l'Union européenne ou d'un ou de plusieurs de ses États membres.

3. Les ICUE portent un marquage de classification de sécurité conformément au paragraphe 2. Elles peuvent porter des marquages supplémentaires pour désigner le domaine d'activité auquel elles sont liées, identifier l'autorité d'origine, limiter la diffusion, restreindre l'utilisation ou indiquer la communicabilité.

Article 3

Gestion de la classification

1. Les autorités compétentes veillent à ce que les ICUE soient classifiées de manière appropriée, clairement identifiées en tant qu'informations classifiées, et qu'elles ne conservent leur niveau de classification qu'aussi longtemps que nécessaire.

2. Les ICUE ne sont pas déclassées ni déclassifiées, et aucun des marquages visés à l'article 2, paragraphe 3, n'est modifié ni supprimé sans le consentement écrit préalable de l'autorité d'origine.

3. Le Conseil approuve une politique de sécurité sur la création d'ICUE, qui comprend un guide pratique de la classification.

Article 4

Protection des informations classifiées

1. Les ICUE sont protégées conformément à la présente décision.

2. Il incombe au détenteur de tout élément d'ICUE de le protéger conformément à la présente décision.

3. Lorsque les États membres introduisent des informations classifiées portant un marquage national de classification de sécurité dans les structures ou réseaux de l'Union, le Conseil et le SGC protègent ces informations conformément aux règles applicables aux ICUE de niveau équivalent tel que prévu dans le tableau d'équivalence des classifications de sécurité figurant à l'appendice B.

4. Un ensemble d'ICUE peut justifier un niveau de protection correspondant à une classification plus élevée que celle appliquée à ses différentes composantes.

Article 5

Gestion des risques de sécurité

1. Les risques pesant sur les ICUE sont gérés dans le cadre d'une procédure. Cette dernière vise à déterminer les risques connus pesant sur la sécurité, à définir des mesures de sécurité permettant de ramener ces risques à un niveau acceptable conformément aux principes de base et aux normes minimales énoncés dans la présente décision et à appliquer ces mesures selon la notion de défense en profondeur, telle que définie à l'appendice A. L'efficacité de telles mesures fait l'objet d'une évaluation constante.

2. Les mesures de sécurité pour la protection des ICUE tout au long de leur cycle de vie sont proportionnées en particulier à leur classification de sécurité, à la forme sous laquelle se présentent les informations ou les matériels ainsi qu'à leur volume, au lieu et à la construction des établissements où se trouvent des ICUE et à la menace évaluée à l'échelle locale que représentent les activités malveillantes et/ou criminelles, y compris l'espionnage, le sabotage et le terrorisme.

3. Les plans d'urgence tiennent compte de la nécessité de protéger les ICUE en cas d'urgence afin de prévenir l'accès et la divulgation non autorisés ainsi que la perte d'intégrité ou de disponibilité.

4. Les mesures de prévention et de retour aux conditions opérationnelles visant à limiter l'impact de défaillances ou d'incidents graves sur le traitement et le stockage des ICUE sont prévues dans les plans de continuité de l'activité.

Article 6

Mise en œuvre de la présente décision

1. Le cas échéant, le Conseil approuve, sur recommandation du comité de sécurité, les politiques de sécurité énonçant les mesures destinées à mettre en œuvre la présente décision.

2. Le comité de sécurité peut arrêter à son niveau des lignes directrices en matière de sécurité en complément ou à l'appui de la présente décision et de toute politique de sécurité approuvée par le Conseil.

Article 7

Mesures de sécurité concernant le personnel

1. La sécurité du personnel passe par l'application de mesures visant à faire en sorte que l'accès aux ICUE ne soit accordé qu'aux personnes qui ont:

— un besoin d'en connaître,

— fait l'objet d'une habilitation de sécurité du niveau correspondant, lorsqu'il y a lieu, et

— été informées de leurs responsabilités.

2. Les procédures d'habilitation de sécurité concernant le personnel ont pour but de déterminer si une personne, compte tenu de sa loyauté, de son intégrité et de sa fiabilité, peut être autorisée à avoir accès à des ICUE.

3. Toutes les personnes au sein du SGC qui, en raison de leurs attributions, ont besoin d'accéder à des ICUE CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur ou de traiter de telles ICUE font l'objet d'une habilitation de sécurité du niveau correspondant avant que l'accès à ces ICUE leur soit accordé. Ces personnes doivent être autorisées par l'autorité investie du pouvoir de nomination du SGC à accéder aux ICUE jusqu'à un niveau de classification donné et jusqu'à une date donnée.

4. Le personnel des États membres visé à l'article 15, paragraphe 3, qui, en raison de ses attributions, peut avoir besoin d'accéder à des ICUE CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur fait l'objet d'une habilitation de sécurité du niveau correspondant ou est dûment autorisé en vertu de ses fonctions, conformément aux dispositions législatives et réglementaires nationales, avant que l'accès à de telles ICUE ne lui soit accordé.

5. Avant de se voir accorder l'accès à des ICUE et à intervalles réguliers par la suite, toutes les personnes concernées sont informées des responsabilités qui leur incombent en matière de protection des ICUE conformément à la présente décision et reconnaissent ces responsabilités.

6. Les modalités d'application du présent article figurent à l'annexe I.

Article 8

Sécurité physique

1. Par «sécurité physique», on entend l'application de mesures physiques et techniques de protection pour empêcher l'accès non autorisé aux ICUE.

2. Les mesures de sécurité physique sont destinées à faire obstacle à toute intrusion par la ruse ou par la force, à avoir un effet dissuasif, à empêcher et détecter les actes non autorisés et permettre d'établir une distinction entre les membres du personnel au regard de l'accès aux ICUE conformément au principe du besoin d'en connaître. Ces mesures sont déterminées sur la base d'une procédure de gestion des risques.

3. Les mesures physiques de sécurité sont mises en place pour tous les locaux, bâtiments, bureaux, salles et autres zones dans lesquels des ICUE sont traitées ou stockées, y compris les zones où se trouvent les systèmes d'information et de communication définis à l'article 10, paragraphe 2.

4. Des zones où sont stockées des ICUE CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur sont créées en tant que zones sécurisées conformément à l'annexe II et agréées par l'autorité de sécurité compétente.

5. Seuls des équipements ou des dispositifs agréés sont utilisés pour protéger les ICUE CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur.

6. Les modalités d'application du présent article figurent à l'annexe II.

Article 9

Gestion des informations classifiées

1. Par «gestion des informations classifiées», on entend l'application de mesures administratives pour contrôler les ICUE tout au long de leur cycle de vie afin de compléter les mesures prévues aux articles 7, 8 et 10 et de contribuer ainsi à la prévention et à la détection d'une compromission ou d'une perte délibérée ou accidentelle de telles informations. Ces mesures concernent en particulier la création, l'enregistrement, la duplication, la traduction, le déclassement, la déclassification, le transport et la destruction des ICUE.

2. Les informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur sont enregistrées à des fins de sécurité avant leur diffusion et lors de leur réception. Les autorités compétentes au sein du SGC et des États membres établissent un bureau d'ordre à cette fin. Les informations classifiées TRÈS SECRET UE/EU TOP SECRET sont enregistrées dans des bureaux d'ordre désignés.

3. Les services et les locaux dans lesquels les ICUE sont traitées ou stockées font l'objet d'une inspection régulière par l'autorité de sécurité compétente.

4. En dehors des zones physiquement protégées, les ICUE sont transmises entre les services et les locaux selon les modalités suivantes:

a) en règle générale, les ICUE sont transmises par voie électronique protégée par des produits cryptographiques agréés conformément à l'article 10, paragraphe 6;

b) si la voie visée au point a) n'est pas utilisée, les ICUE sont transportées:

   i) soit sur des supports électroniques (par exemple clé USB, CD, disque dur) protégés par des produits cryptographiques agréés conformément à l'article 10, paragraphe 6;

   ii) soit, dans tous les autres cas, de la manière prescrite par l'autorité de sécurité compétente conformément aux mesures de protection pertinentes prévues à l'annexe III.

5. Les modalités d'application du présent article figurent aux annexes III et IV.

Article 10

Protection des ICUE traitées dans les systèmes de communication et d'information

1. Par «assurance de l'information (AI) dans le domaine des systèmes d'information et de communication», on entend la certitude que ces systèmes protégeront les informations qu'ils traitent et fonctionneront comme ils le doivent, quand ils le doivent, sous le contrôle d'utilisateurs légitimes. Une AI efficace garantit des niveaux appropriés de confidentialité, d'intégrité, de disponibilité, de non-répudiation et d'authenticité. L'AI est fondée sur un processus de gestion des risques.

2. On entend par «système d'information et de communication» (SIC) tout système permettant le traitement d'informations sous forme électronique. Un SIC comprend l'ensemble des moyens nécessaires pour le faire fonctionner, y compris l'infrastructure, l'organisation, le personnel et les ressources d'information. La présente décision s'applique aux SIC traitant des ICUE.

3. Les SIC traitent des ICUE dans le respect de la notion d'AI.

4. Tous les SIC font l'objet d'un processus d'homologation. L'homologation vise à obtenir l'assurance que toutes les mesures de sécurité appropriées ont été mises en œuvre et que les ICUE et les SIC font l'objet d'un niveau suffisant de protection conformément à la présente décision. La déclaration d'homologation détermine le niveau maximal de classification des informations qui peuvent être traitées dans un SIC ainsi que les modalités et les conditions correspondantes.

5. Des mesures de sécurité sont mises en œuvre afin de protéger les SIC traitant des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL et d'un niveau de classification supérieur contre la compromission de ces informations par des émissions électromagnétiques non intentionnelles («mesures de sécurité TEMPEST»). Ces mesures de sécurité sont proportionnées au risque d'exploitation et au niveau de classification des informations.

6. Lorsque la protection des ICUE est assurée par des produits cryptographiques, ces produits doivent être approuvés comme suit:

a) la confidentialité des informations classifiées SECRET UE/EU SECRET et d'un niveau de classification supérieur est protégée par des produits cryptographiques agréés par le Conseil en tant qu'autorité d'agrément cryptographique (AAC), sur recommandation du comité de sécurité;

b) la confidentialité des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou RESTREINT UE/EU RESTRICTED est protégée par des produits cryptographiques agréés par le secrétaire général du Conseil (ci-après dénommé «le secrétaire général») en tant qu'AAC, sur recommandation du comité de sécurité.

Nonobstant le point b), au sein des systèmes nationaux des États membres, la confidentialité des ICUE CONFIDENTIEL UE/EU CONFIDENTIAL ou RESTREINT UE/EU RESTRICTED peut être protégée par des produits cryptographiques agréés par l'AAC d'un État membre.

7. Lors de la transmission des ICUE par voie électronique, des produits cryptographiques qui ont fait l'objet d'un agrément sont utilisés. Nonobstant cette exigence, des procédures spécifiques peuvent être appliquées en cas d'urgence ou dans le cadre de configurations techniques spécifiques comme le prévoit l'annexe IV.

8. Les autorités compétentes du SGC et des États membres créent respectivement les fonctions suivantes en matière d'AI:

a) une autorité chargée de l'AI (AAI);

b) une autorité TEMPEST (AT);

c) une autorité d'agrément cryptographique (AAC);

d) une autorité chargée de la distribution cryptographique (ADC).

9. Pour chaque système, les autorités compétentes du SGC et des États membres créent respectivement:

a) une autorité d'homologation de sécurité (AHS);

b) une autorité opérationnelle chargée de l'AI.

10. Les modalités d'application du présent article figurent à l'annexe IV.

Article 11

Sécurité industrielle

1. Par «sécurité industrielle», on entend l'application de mesures visant à assurer la protection des ICUE par des contractants ou des sous-traitants dans le cadre de négociations précontractuelles et tout au long du cycle de vie des contrats classifiés. De tels contrats ne doivent pas concerner l'accès à des informations classifiées TRÈS SECRET UE/EU TOP SECRET.

2. Le SGC peut, par voie contractuelle, confier à des entités industrielles ou autres immatriculées dans un État membre ou dans un État tiers ayant conclu un accord ou un arrangement administratif en vertu de l'article 13, paragraphe 2, point a) ou b), des tâches qui impliquent ou nécessitent l'accès, le traitement ou le stockage d'ICUE ou la communication de telles informations.

3. En tant qu'autorité contractante, le SGC veille à ce que les normes minimales de sécurité industrielle prévues dans la présente décision et mentionnées dans le contrat soient respectées lors de l'octroi de contrats classifiés à des entités industrielles ou autres.

4. L'autorité nationale de sécurité (ANS), l'autorité de sécurité désignée (ASD) ou toute autre autorité compétente de chaque État membre veille, autant que le permettent les dispositions législatives et réglementaires nationales, à ce que les contractants et les sous-traitants immatriculés sur le territoire dudit État prennent toutes les mesures appropriées pour protéger les ICUE dans le cadre de négociations précontractuelles et lors de l'exécution d'un contrat classifié.

5. L'ANS, l'ASD ou toute autre autorité compétente de chaque État membre veille, conformément aux dispositions législatives et réglementaires nationales, à ce que les contractants et les sous-traitants immatriculés sur le territoire de l'État membre concerné, qui participent à des contrats classifiés ou à des contrats de sous-traitance nécessitant l'accès à des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET au sein de leurs établissements, soient en possession, lors de l'exécution desdits contrats ou durant la phase précontractuelle, d'une habilitation nationale de sécurité d'établissement (HSE) du niveau de classification correspondant.

6. Lorsque les membres du personnel d'un contractant ou d'un sous-traitant doivent, en raison de leurs fonctions aux fins de l'exécution d'un contrat classifié, accéder à des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET, l'ANS/ASD ou toute autre autorité de sécurité compétente leur délivre une habilitation de sécurité du personnel (HSP), conformément aux dispositions législatives ou réglementaires nationales et dans le respect des normes minimales de sécurité définies à l'annexe I.

7. Les modalités d'application du présent article figurent à l'annexe V.

Article 12

Échange d'ICUE

1. Le Conseil détermine les conditions dans lesquelles il peut échanger les ICUE qu'il détient avec d'autres institutions, organes, organismes ou agences de l'Union européenne. Un cadre approprié peut être mis en place à cette fin, y compris au moyen de la conclusion d'accords interinstitutionnels ou d'autres arrangements lorsque cela est nécessaire à cet effet.

2. Un tel cadre vise à garantir que les ICUE font l'objet d'une protection appropriée à leur niveau de classification et conforme à des principes de base et normes minimales équivalents à ceux énoncés dans la présente décision.

Article 13

Échange d'informations classifiées avec des États tiers et des organisations internationales

1. Dans le cas où le Conseil établit qu'il est nécessaire d'échanger des ICUE avec un État tiers ou une organisation internationale, un cadre approprié est mis en place à cette fin.

2. Afin d'établir un tel cadre et de définir des règles réciproques relatives à la protection des informations classifiées échangées:

a) l'Union conclut avec les États tiers ou les organisations internationales des accords sur les procédures de sécurité concernant l'échange et la protection des informations classifiées (ci-après dénommés «accords sur la sécurité des informations»); ou

b) le secrétaire général peut conclure des arrangements administratifs au nom du SGC, conformément au paragraphe 17 de l'annexe VI, lorsque le niveau de classification des ICUE à communiquer n'est en règle générale pas supérieur à RESTREINT UE/EU RESTRICTED.

3. Les accords sur la sécurité des informations ou les arrangements administratifs visés au paragraphe 2 contiennent des dispositions pour garantir que, lorsque des États tiers ou des organisations internationales reçoivent des ICUE, ces informations bénéficient d'une protection conforme à leur niveau de classification et à des normes minimales qui ne sont pas moins strictes que celles prévues dans la présente décision.

4. La décision de communiquer des ICUE émanant du Conseil à un État tiers ou à une organisation internationale est prise par le Conseil, au cas par cas, en fonction de la nature et du contenu de ces informations, du besoin d'en connaître du destinataire et d'une appréciation des avantages que l'Union peut en retirer. Si l'autorité d'origine des informations classifiées à communiquer n'est pas le Conseil, le SGC lui demande au préalable son consentement écrit. Au cas où l'auteur ne peut être identifié, le Conseil assume cette responsabilité en lieu et place de l'auteur.

5. Des visites d'évaluation sont organisées pour s'assurer de l'efficacité des mesures de sécurité mises en place dans un État tiers ou une organisation internationale pour la protection des ICUE fournies ou échangées.

6. Les modalités d'application du présent article figurent à l'annexe VI.

Article 14

Infractions à la sécurité et compromission des ICUE

1. Une infraction à la sécurité est un acte ou une omission commis par une personne qui est contraire aux règles de sécurité énoncées dans la présente décision.

2. Il y a compromission lorsque, à la suite d'une infraction à la sécurité, des ICUE ont été divulguées en totalité ou en partie à des personnes non autorisées.

3. Toute infraction à la sécurité, réelle ou présumée, est immédiatement signalée à l'autorité de sécurité compétente.

4. Lorsqu'il est avéré ou qu'il existe des motifs raisonnables de supposer que des ICUE ont été compromises ou perdues, l'ANS ou une autre autorité compétente prend toutes les mesures appropriées conformément aux dispositions législatives et réglementaires applicables pour:

a) en informer l'autorité d'origine;

b) faire en sorte qu'une enquête soit menée par des membres du personnel n'étant pas directement concernés par l'infraction afin d'établir les faits;

c) évaluer le préjudice éventuel causé aux intérêts de l'Union ou des États membres;

d) éviter que les faits ne se reproduisent; et

e) informer les autorités compétentes des mesures prises.

5. Toute personne responsable d'une violation des règles de sécurité énoncées dans la présente décision est passible d'une sanction disciplinaire conformément aux dispositions législatives et réglementaires applicables. Toute personne responsable de la compromission ou de la perte d'ICUE est passible de sanctions disciplinaires et/ou peut faire l'objet d'une action en justice conformément aux dispositions législatives et réglementaires applicables.

Article 15

Responsabilité de la mise en œuvre

1. Le Conseil prend toutes les mesures nécessaires pour assurer la cohérence globale de l'application de la présente décision.

2. Le secrétaire général prend toutes les mesures nécessaires pour faire en sorte que, lors du traitement ou du stockage des ICUE ou de toute autre information classifiée, la présente décision soit appliquée dans les locaux utilisés par le Conseil et au sein du SGC, par les fonctionnaires et autres agents du SGC, le personnel détaché auprès du SGC et les contractants du SGC.

3. Les États membres prennent toutes les mesures appropriées, conformément à leurs dispositions législatives et réglementaires nationales respectives, pour faire en sorte que, lors du traitement ou du stockage des ICUE, la présente décision soit respectée par:

a) le personnel des représentations permanentes des États membres auprès de l'Union européenne ainsi que par les délégués nationaux assistant à des sessions du Conseil ou des réunions de ses instances préparatoires, ou participant à d'autres activités du Conseil;

b) les autres membres du personnel des administrations nationales des États membres, y compris le personnel détaché auprès de ces administrations, qu'ils soient en poste sur le territoire des États membres ou à l'étranger;

c) les autres personnes dans les États membres dûment autorisées, en raison de leurs fonctions, à avoir accès aux ICUE; et

d) les contractants des États membres, qu'ils soient sur le territoire des États membres ou à l'étranger.

Article 16

Organisation de la sécurité au sein du Conseil

1. Dans le cadre du rôle qui lui incombe et qui consiste à assurer la cohérence globale de l'application de la présente décision, le Conseil approuve:

a) les accords visés à l'article 13, paragraphe 2, point a);

b) les décisions autorisant la communication, ou consentant à la communication, d'ICUE provenant du Conseil ou détenues par ce dernier à des États tiers et des organisations internationales, conformément au principe du consentement de l'autorité d'origine;

c) un programme annuel de visites d'évaluation recommandé par le comité de sécurité pour effectuer des visites visant à évaluer les services et les locaux des États membres, des organes, des agences et des entités de l'Union qui appliquent la présente décision ou les principes y figurant, et pour effectuer des visites d'évaluation dans des États tiers et des organisations internationales afin de s'assurer de l'efficacité des mesures mises en œuvre pour la protection des ICUE; et

d) les politiques de sécurité prévues à l'article 6, paragraphe 1.

2. Le secrétaire général est l'autorité de sécurité du SGC. En cette qualité, le secrétaire général:

a) applique la politique de sécurité du Conseil et la réexamine périodiquement;

b) assure, avec les ANS des États membres, la coordination de toutes les questions de sécurité relatives à la protection des informations classifiées présentant un intérêt pour les activités du Conseil;

c) accorde aux fonctionnaires et autres agents du SGC ainsi qu'aux experts nationaux détachés auprès du SGC une autorisation d'accès à des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur, conformément à l'article 7, paragraphe 3;

d) le cas échéant, fait enquêter sur toute compromission ou perte réelle ou présumée d'informations classifiées détenues par le Conseil ou provenant de ce dernier et demande aux autorités de sécurité compétentes de participer à de telles enquêtes;

e) procède à des inspections périodiques des dispositions de sécurité destinées à assurer la protection des informations classifiées sur les locaux du SGC;

f) procède à des visites périodiques pour évaluer les dispositions de sécurité destinées à assurer la protection des ICUE dans les organes, les agences et les entités de l'Union qui appliquent la présente décision ou les principes y figurant;

g) procède, en collaboration et en accord avec l'ANS concernée, à des évaluations périodiques des dispositions de sécurité destinées à assurer la protection des ICUE dans les services et les locaux des États membres;

h) veille à ce que les mesures de sécurité soient coordonnées en tant que de besoin avec les autorités compétentes des États membres qui sont responsables de la protection des informations classifiées et, le cas échéant, des États tiers ou des organisations internationales, y compris en ce qui concerne la nature des menaces pesant sur la sécurité des ICUE et les moyens de les protéger; et

i) conclut les arrangements administratifs visés à l'article 13, paragraphe 2, point b).

Le bureau de sécurité du SGC est à la disposition du secrétaire général pour l'aider à s'acquitter de ces responsabilités.

3. Aux fins de la mise en œuvre de l'article 15, paragraphe 3, il conviendrait que les États membres:

a) désignent une ANS, figurant à l'appendice C, responsable des dispositions de sécurité destinées à assurer la protection des ICUE afin que:

i) les ICUE détenues par tout service, organisme ou agence national, public ou privé, sur le territoire national ou à l'étranger soient protégées conformément à la présente décision;

ii) les dispositions de sécurité destinées à assurer la protection des ICUE soient périodiquement inspectées ou évaluées;

iii) toutes les personnes employées dans une administration nationale ou par un contractant et susceptibles d'avoir accès à des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur détiennent une habilitation de sécurité correspondante ou soient dûment autorisées en vertu de leurs fonctions conformément aux dispositions législatives et réglementaires nationales;

iv) des programmes de sécurité soient mis au point en tant que de besoin de telle sorte que le risque de compromission ou de perte d'ICUE soit réduit au minimum;

v) les questions de sécurité liées à la protection des ICUE fassent l'objet d'une coordination avec les autres autorités nationales compétentes, y compris celles visées dans la présente décision; et

vi) des réponses soient apportées aux demandes d'habilitation de sécurité appropriées, en particulier celles émanant des organes, des agences, des entités et des opérations de l'Union mis en place en vertu du titre V, chapitre 2, du TUE, ainsi que des représentants spéciaux de l'Union européenne (RSUE) et de leurs équipes qui appliquent la présente décision ou les principes y figurant.

b) veillent à ce que leurs autorités compétentes communiquent à leur gouvernement et, par l'intermédiaire de ces derniers au Conseil, des informations sur la nature des menaces qui pèsent sur la sécurité des ICUE et des conseils sur les moyens de s'en protéger.

Article 17

Comité de sécurité

1. Un comité de sécurité est créé par la présente décision. Il examine et évalue toute question de sécurité relevant du champ d'application de la présente décision, et transmet des recommandations au Conseil, le cas échéant.

2. Le comité de sécurité est composé de représentants des ANS des États membres, un représentant de la Commission et du SEAE assistant à ses réunions. Il est présidé par le secrétaire général ou par son délégué désigné. Il se réunit sur instruction du Conseil ou à la demande du secrétaire général ou d'une ANS.

Des représentants des organes, des agences et des entités de l'Union qui appliquent la présente décision ou les principes y figurant peuvent être invités à assister à ses réunions lorsque les questions traitées les concernent.

3. Le comité de sécurité organise ses activités de manière à être en mesure de formuler des recommandations sur des aspects spécifiques de la sécurité. Il met en place une sous-division spécialisée dans les questions concernant l'assurance de l'information et d'autres sous-divisions spécialisées si nécessaire. Il établit le mandat de ces sous-divisions spécialisées et reçoit leurs rapports d'activités comprenant, le cas échéant, des recommandations, quelles qu'elles soient, destinées au Conseil.

Article 18

Remplacement de la décision précédente

1. La présente décision abroge et remplace la décision 2011/292/UE du Conseil ([1]).

2. Toutes les ICUE portant un marquage en application de la décision 2001/264/CE du Conseil ([2]) et de la décision 2011/292/UE continuent d'être protégées conformément aux dispositions pertinentes de cette décision.

Article 19

Entrée en vigueur

La présente décision entre en vigueur le jour de sa publication au *Journal officiel de l'Union européenne*.

Fait à Bruxelles, le 23 septembre 2013.

Par le Conseil

Le président

V. JUKNA

([1]) Décision 2011/292/UE du Conseil du 31 mars 2011 concernant les règles de sécurité aux fins de la protection des informations classifiées de l'Union européenne (JO L 141 du 27.5.2011, p. 17).

([2]) Décision 2001/264/CE du Conseil du 19 mars 2001 adoptant le règlement de sécurité du Conseil (JO L 101 du 11.4.2001, p. 1).

ANNEXES

ANNEXE I

Mesures de sécurité concernant le personnel

ANNEXE II

Sécurité physique

ANNEXE III

Gestion des informations classifiées

ANNEXE IV

Protection des ICUE traitées dans les SIC

ANNEXE V

Sécurité industrielle

ANNEXE VI

Échange d'informations classifiées avec des États tiers et des organisations internationales

ANNEXE I

MESURES DE SÉCURITÉ CONCERNANT LE PERSONNEL

I. INTRODUCTION

1. La présente annexe énonce les modalités d'application de l'article 7. Elle prévoit les critères permettant de déterminer si une personne, compte tenu de sa loyauté, de son intégrité et de sa fiabilité, peut être autorisée à avoir accès à des ICUE, ainsi que les procédures d'enquête et administratives à suivre à cet effet.

II. OCTROI DE L'ACCÈS AUX ICUE

2. Une personne ne peut se voir accorder l'accès à des informations classifiées qu'après:

   a) que son besoin d'en connaître a été établi;

   b) avoir été informée des règles et procédures de sécurité applicables à la protection des ICUE et avoir reconnu les responsabilités qui lui incombent en matière de protection de ces informations; et

   c) pour les informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur:

      — s'être vu accorder une HSP du niveau correspondant ou avoir été dûment autorisée en vertu de ses fonctions conformément aux dispositions législatives et réglementaires nationales; ou

      — dans le cas de fonctionnaires ou d'autres agents du SGC ou d'experts nationaux détachés, avoir été autorisée à accéder aux ICUE par l'autorité investie du pouvoir de nomination (AIPN) du SGC, conformément aux paragraphes 16 à 25 jusqu'à un niveau de classification donné et jusqu'à une date donnée.

3. Il appartient à chacun des États membres et au SGC de répertorier, au sein de leurs structures, les postes nécessitant l'accès à des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur et exigeant par conséquent une habilitation de sécurité du niveau correspondant.

III. RÈGLES EN MATIÈRE D'HABILITATION DE SÉCURITÉ DU PERSONNEL

4. Après réception d'une demande dûment autorisée, les ANS ou les autres autorités nationales compétentes sont chargées de veiller à la réalisation des enquêtes de sécurité relatives aux ressortissants de leur pays qui doivent accéder à des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur. Les normes d'enquête doivent être conformes aux dispositions législatives et réglementaires nationales aux fins de l'octroi d'une HSP ou de la fourniture d'une assurance pour la personne à laquelle doit être octroyée une autorisation d'accès à des ICUE, le cas échéant.

5. Si la personne concernée réside sur le territoire d'un autre État membre ou d'un État tiers, les autorités nationales compétentes sollicitent une aide auprès de l'autorité compétente de l'État de résidence conformément aux dispositions législatives et réglementaires nationales. Les États membres se prêtent assistance pour effectuer les enquêtes de sécurité, conformément aux dispositions législatives et réglementaires nationales.

6. Lorsque les dispositions législatives et réglementaires nationales le permettent, les ANS ou les autres autorités nationales compétentes peuvent effectuer les enquêtes relatives aux non-ressortissants qui doivent accéder à des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur. Les normes d'enquête doivent être conformes aux dispositions législatives et réglementaires nationales.

Critères à retenir dans le cadre des enquêtes de sécurité

7. Il convient d'établir, au moyen d'une enquête de sécurité, la loyauté, l'intégrité et la fiabilité d'une personne aux fins de l'octroi d'une habilitation de sécurité lui permettant d'accéder à des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur. L'autorité nationale compétente effectue une appréciation générale sur la base des conclusions de l'enquête. Parmi les principaux critères à retenir à cet effet, il y a lieu de déterminer, dans la mesure où les dispositions législatives et réglementaires nationales le permettent, si l'intéressé:

a) a commis ou a tenté de commettre un acte d'espionnage, de terrorisme, de sabotage, de trahison ou de sédition, seul ou en association avec d'autres, s'est rendu complice d'un tel acte ou a incité une autre personne à le commettre;

b) est ou a été lié à des espions, des terroristes, des saboteurs ou des personnes que l'on peut raisonnablement soupçonner de l'être, ou à des représentants d'organisations ou d'États étrangers, notamment des services de renseignement étrangers, qui sont susceptibles de menacer la sécurité de l'Union et/ou des États membres, à moins que ce lien ait été autorisé dans le cadre d'une mission officielle;

c) est ou a été membre d'une organisation qui, par des moyens violents ou subversifs ou par d'autres moyens illégaux, cherche, entre autres, à renverser le gouvernement d'un État membre, à modifier l'ordre constitutionnel d'un État membre ou à provoquer un changement de régime ou de politique dans un État membre;

d) est ou a été sympathisant d'une organisation décrite au point c), est ou a été lié de près à des membres d'une telle organisation;

e) a délibérément dissimulé, altéré ou falsifié des informations importantes, notamment du point de vue de la sécurité, ou a délibérément menti en remplissant un questionnaire de sécurité ou lors d'un entretien de sécurité;

f) a été reconnu coupable d'une ou de plusieurs infractions pénales;

g) a des antécédents de dépendance à l'alcool, d'usage de drogues illicites et/ou d'abus de drogues licites;

h) a ou a eu des comportements de nature à entraîner un risque de vulnérabilité au chantage ou à des pressions;

i) a fait preuve, en acte ou en parole, d'un manque d'honnêteté, de loyauté ou de fiabilité, ou s'est montré indigne de confiance;

j) s'est livré à des violations graves ou répétées du règlement de sécurité, a cherché ou a réussi à mener des activités non autorisées concernant les systèmes d'information et de communication; et

k) est susceptible de faire l'objet de pressions (par exemple, en raison de la possession d'une ou plusieurs nationalités d'États non membres de l'Union ou par l'intermédiaire de parents ou de proches qui pourraient être vulnérables face à des services de renseignement étrangers, des groupes terroristes ou d'autres organisations ou personnes se livrant à des activités subversives, dont les visées peuvent menacer les intérêts de l'Union et/ou des États membres dans le domaine de la sécurité).

8. Les antécédents financiers et médicaux de la personne concernée peuvent également être pris en considération, le cas échéant et dans le respect des dispositions législatives et réglementaires nationales, au cours de l'enquête de sécurité.

9. La conduite et la situation du conjoint, du cohabitant ou d'un membre de la famille proche peuvent également être pris en considération, le cas échéant et dans le respect des dispositions législatives et réglementaires nationales, au cours de l'enquête de sécurité.

Règles en matière d'enquête applicables à l'accès aux ICUE

Première délivrance d'une habilitation de sécurité

10. La première habilitation de sécurité donnant accès aux informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET se fonde sur une enquête de sécurité portant sur les cinq dernières années au moins, ou sur la période comprise entre l'âge de 18 ans et la date de l'enquête, la période la plus courte étant retenue; cette enquête comprend les éléments suivants:

a) un questionnaire national de sécurité concernant le personnel, correspondant au niveau de classification des ICUE auxquelles l'intéressé pourrait avoir à accéder, est rempli, puis transmis à l'autorité de sécurité compétente;

b) vérification de l'identité/de la citoyenneté/de la nationalité: la date et le lieu de naissance de l'intéressé ainsi que son identité doivent être vérifiés. Sa citoyenneté et/ou sa nationalité, passées et présentes, doivent être établies; ce processus vise notamment à déterminer s'il est susceptible de céder à des pressions d'origine étrangère, par exemple en raison de son lieu de résidence antérieur ou de contacts passés; et

c) vérification des antécédents aux niveaux national et local: il convient de procéder à des vérifications dans les fichiers de la sûreté et les casiers judiciaires, lorsque ces derniers existent, et/ou dans d'autres registres analogues des administrations ou de la police. Il convient de vérifier les fichiers des services répressifs dans le ressort desquels la personne a résidé ou a travaillé.

11. La première habilitation de sécurité donnant accès aux informations TRÈS SECRET UE/EU TOP SECRET se fonde sur une enquête de sécurité portant sur les dix dernières années au moins, ou sur la période comprise entre l'âge de 18 ans et la date de l'enquête, la période la plus courte étant retenue. Si des entretiens ont lieu conformément au point e), les enquêtes portent sur les sept dernières années au moins, ou sur la période comprise entre l'âge de 18 ans et la date de l'enquête, la période la plus courte étant retenue. Outre les critères indiqués au paragraphe 7 ci-dessus, les éléments ci-après font l'objet d'une enquête, dans la mesure où les dispositions législatives et réglementaires nationales le permettent, avant l'octroi d'une HSP de niveau TRÈS SECRET UE/EU TOP SECRET; ils peuvent aussi faire l'objet d'une enquête avant l'octroi d'une HSP de niveau CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET, dans les cas où les dispositions législatives et réglementaires nationales l'exigent:

a) situation financière: il y a lieu de rechercher des informations sur la situation financière de l'intéressé pour déterminer si, en raison de graves difficultés financières, il est susceptible de céder à des pressions étrangères ou nationales, ou pour mettre en lumière un éventuel enrichissement inexpliqué;

b) éducation: il y a lieu, afin de pouvoir vérifier le parcours éducatif de l'intéressé, de rechercher des informations dans les écoles, universités et autres établissements d'enseignement fréquentés par l'intéressé depuis l'âge de 18 ans ou pendant une période jugée appropriée par l'autorité menant l'enquête;

c) emploi: il y a lieu de rechercher des informations relatives à la situation actuelle et passée en matière d'emploi, en se reportant à des sources telles que les attestations de travail, les rapports sur le rendement ou l'efficacité, les employeurs ou les supérieurs hiérarchiques;

d) service militaire: le cas échéant, vérification des états de service de l'intéressé et du type de dispense obtenu; et

e) entretiens: lorsque la législation nationale le prévoit et l'autorise, un ou des entretiens sont menés avec la personne concernée. Des entretiens sont également menés avec d'autres personnes qui sont en mesure de porter un jugement objectif sur les antécédents, les activités, la loyauté, l'intégrité et la fiabilité de l'intéressé. Lorsque dans le cadre de la pratique nationale, on demande à la personne qui fait l'objet de l'enquête de mentionner des personnes de référence, celles-ci doivent être interrogées, sauf si des raisons valables s'y opposent.

12. Le cas échéant et conformément aux dispositions législatives et réglementaires nationales, des recherches complémentaires peuvent être menées pour exploiter toutes les informations pertinentes dont on dispose sur l'intéressé et pour corroborer des informations défavorables ou les infirmer.

Renouvellement d'une habilitation de sécurité

13. Après la première délivrance d'une habilitation de sécurité et pour autant que l'intéressé ait accompli une période de service ininterrompue auprès d'une administration nationale ou du SGC et qu'il ait toujours besoin d'avoir accès aux ICUE, l'habilitation de sécurité est réexaminée en vue de son renouvellement dans un délai ne dépassant pas cinq ans pour une habilitation TRÈS SECRET UE/EU TOP SECRET et dix ans pour une habilitation SECRET UE/EU SECRET ou CONFIDENTIEL UE/EU CONFIDENTIAL avec effet à compter de la date de notification des conclusions de la dernière enquête de sécurité sur laquelle elle était fondée. Toutes les enquêtes de sécurité à effectuer en vue du renouvellement d'une habilitation de sécurité couvrent la période écoulée depuis la dernière enquête.

14. En vue du renouvellement d'une habilitation de sécurité, les éléments énoncés aux paragraphes 10 et 11 font l'objet d'une enquête.

15. Les demandes de renouvellement sont présentées en temps voulu, compte tenu du délai nécessaire pour réaliser les enquêtes de sécurité. Néanmoins, lorsque l'ANS concernée ou une autre autorité nationale compétente a reçu la demande de renouvellement en question et le questionnaire de sécurité correspondant avant l'expiration d'une habilitation de sécurité et que l'enquête de sécurité nécessaire n'est pas achevée, l'autorité nationale compétente peut, lorsque les dispositions législatives et réglementaires nationales le permettent, proroger la validité de l'habilitation de sécurité existante pour une durée de douze mois au maximum. Si, à la fin de cette période de douze mois, l'enquête de sécurité n'est toujours pas achevée, l'intéressé est affecté à des fonctions qui ne nécessitent pas une habilitation de sécurité.

Procédures appliquées au sein du SGC en matière d'autorisation

16. En ce qui concerne les fonctionnaires et autres agents du SGC, l'autorité de sécurité du SGC transmet le questionnaire de sécurité rempli à l'ANS de l'État membre dont l'intéressé est ressortissant et demande qu'il soit procédé à une enquête de sécurité pour le niveau de classification des ICUE auxquelles l'intéressé devra avoir accès.

17. Si des informations utiles à une enquête de sécurité sont portées à la connaissance du SGC concernant une personne ayant demandé une habilitation de sécurité aux fins d'accès à des ICUE, le SGC, agissant conformément à la réglementation applicable, en avertit l'ANS compétente.

18. À l'issue de l'enquête de sécurité, l'ANS compétente notifie à l'autorité de sécurité du SGC les conclusions de l'enquête en question, à l'aide du modèle-type prévu par le comité de sécurité pour la correspondance.

    a) Lorsque, à l'issue de l'enquête de sécurité, on obtient l'assurance qu'il n'existe pas de renseignements défavorables de nature à mettre en doute la loyauté, l'intégrité et la fiabilité de l'intéressé, l'AIPN du SGC peut accorder à l'intéressé l'autorisation d'accéder à des ICUE du niveau de classification correspondant jusqu'à une date déterminée.

    b) Lorsque, à l'issue de l'enquête de sécurité, on n'obtient pas cette assurance, l'AIPN du SGC en informe l'intéressé, qui peut demander à être entendu par l'AIPN. Celle-ci peut demander à l'ANS compétente tout éclaircissement complémentaire qu'elle est en mesure de donner conformément à ses dispositions législatives et réglementaires nationales. En cas de confirmation des résultats, il n'est pas accordé d'autorisation aux fins de l'accès à des ICUE.

19. L'enquête de sécurité et ses résultats obéissent aux dispositions législatives et réglementaires en vigueur dans l'État membre concerné, y compris celles relatives aux recours. Les décisions de l'AIPN du SGC sont susceptibles de recours conformément au statut des fonctionnaires de l'Union européenne et au régime applicable aux autres agents de l'Union européenne, fixés dans le règlement (CEE, Euratom, CECA) n° 259/68 du Conseil [1] (ci-après dénommés «statut et régime applicable»).

20. Les experts nationaux détachés auprès du SGC pour occuper un poste nécessitant un accès à des ICUE CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur doivent présenter à l'autorité de sécurité du SGC avant de prendre leurs fonctions un certificat d'habilitation de sécurité du personnel (CHSP) valable leur donnant accès aux ICUE, sur la base de laquelle l'AIPN délivre une autorisation d'accès aux ICUE.

21. Le SGC acceptera l'autorisation d'accès à des ICUE octroyée par toute autre institution, organe ou agence de l'Union, pour autant qu'elle reste valable. L'autorisation couvrira toute fonction exercée par l'intéressé au sein du SGC. L'institution, l'organe ou l'agence de l'Union dans lequel la personne prend ses fonctions signalera le changement d'employeur à l'ANS concernée.

22. Si l'intéressé n'entame pas sa période de service dans un délai de douze mois à compter de la notification des conclusions de l'enquête de sécurité à l'AIPN du SGC ou si cette période de service connaît une interruption de douze mois au cours de laquelle l'intéressé n'occupe pas de poste au sein du SGC ou d'une administration nationale d'un État membre, les conclusions précitées sont soumises à l'ANS compétente afin que celle-ci confirme qu'elles restent valables et pertinentes.

[1] Règlement (CEE, Euratom, CECA) n° 259/68 du Conseil du 29 février 1968 fixant le statut des fonctionnaires des Communautés européennes ainsi que le régime applicable aux autres agents de ces Communautés, et instituant des mesures particulières temporairement applicables aux fonctionnaires de la Commission (JO L 56 du 4.3.1968, p. 1).

23. Si des informations sont portées à la connaissance du SGC concernant un risque de sécurité que représente une personne titulaire d'une autorisation d'accès à des ICUE, le SGC, agissant conformément à la réglementation applicable, en avertit l'ANS compétente et peut suspendre l'accès aux ICUE ou retirer l'autorisation d'accès à des ICUE.

24. Lorsqu'une ANS notifie au SGC que l'assurance visée au paragraphe 18, point a), n'est plus fournie concernant une personne titulaire d'une autorisation d'accès à des ICUE, l'AIPN du SGC peut demander à l'ANS concernée tout éclaircissement qu'elle est en mesure de donner dans le respect de ses dispositions législatives et réglementaires nationales. Si les informations défavorables sont confirmées, l'autorisation est retirée et la personne concernée n'est plus autorisée à avoir accès aux ICUE, ni à des postes où un tel accès est possible et où elle pourrait nuire à la sécurité.

25. Toute décision de retirer une autorisation à un fonctionnaire ou à un autre agent du SGC ou de suspendre une telle autorisation et, s'il y a lieu, les raisons la justifiant sont communiquées à la personne concernée, qui peut demander à être entendue par l'AIPN. Les informations communiquées par une ANS sont soumises aux dispositions législatives et réglementaires en vigueur dans l'État membre concerné, y compris celles relatives aux recours. Les décisions de l'AIPN du SGC sont susceptibles de recours conformément au statut et au régime applicable.

Registres des habilitations de sécurité et des autorisations

26. Chaque État membre et le SGC tiennent respectivement des registres des HSP et des autorisations accordées aux fins d'accès à des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur. Ces registres contiennent au minimum le niveau de classification des ICUE auxquelles l'intéressé peut se voir accorder l'accès, la date à laquelle l'habilitation de sécurité a été délivrée et sa durée de validité.

27. L'autorité de sécurité compétente peut délivrer un CHSP précisant le niveau de classification des ICUE auxquelles l'intéressé peut se voir accorder l'accès (CONFIDENTIEL UE/EU CONFIDENTIAL ou un niveau supérieur), la durée de validité de l'HSP donnant accès aux ICUE ou de l'autorisation d'accès à des ICUE correspondante et la date d'expiration du certificat proprement dit.

Exemptions de l'obligation d'HSP

28. L'accès aux ICUE dont bénéficient les personnes dans les États membres qui sont dûment autorisées en raison de leurs fonctions est déterminé conformément aux dispositions législatives et réglementaires nationales; ces personnes sont informées des obligations qui leur incombent en matière de sécurité en ce qui concerne la protection des ICUE.

IV. FORMATION ET SENSIBILISATION À LA SÉCURITÉ

29. Toutes les personnes qui se sont vu délivrer une habilitation de sécurité doivent reconnaître par écrit qu'elles sont conscientes de leurs obligations en matière de protection des ICUE et des conséquences qui pourraient résulter si des ICUE devaient être compromises. Le cas échéant, les États membres et le SGC tiennent un registre de ces déclarations écrites.

30. Toutes les personnes autorisées à avoir accès aux ICUE ou tenues de les traiter sont averties dans un premier temps et périodiquement informées par la suite des menaces pesant sur la sécurité, et elles doivent rendre compte immédiatement aux autorités de sécurité compétentes de toute démarche ou activité qu'elles jugent suspecte ou inhabituelle.

31. Toutes les personnes qui cessent d'exercer des fonctions nécessitant un accès aux ICUE sont informées, et le cas échéant reconnaissent par écrit, qu'elles ont l'obligation de continuer à protéger les ICUE.

V. CIRCONSTANCES EXCEPTIONNELLES

32. Lorsque les dispositions législatives et réglementaires nationales le permettent, une habilitation de sécurité délivrée par une autorité nationale compétente d'un État membre aux fins d'accès à des informations nationales classifiées peut, pendant une période temporaire dans l'attente de la délivrance d'une HSP aux fins d'accès à des ICUE, permettre à des fonctionnaires nationaux d'accéder à des ICUE jusqu'au niveau équivalent indiqué dans le tableau d'équivalence figurant à l'appendice B, dans les cas où un tel accès temporaire est requis dans l'intérêt de l'Union. Lorsque les dispositions législatives et réglementaires nationales ne permettent pas un tel accès temporaire à des ICUE, les ANS en informent le comité de sécurité.

33. En cas d'urgence, lorsque cela est dûment justifié dans l'intérêt du service et en attendant l'achèvement de l'enquête de sécurité complète, l'AIPN du SGC peut, après avoir consulté l'ANS de l'État membre dont l'intéressé est ressortissant et sous réserve des résultats des vérifications préliminaires effectuées pour s'assurer de l'absence d'informations défavorables, accorder à titre temporaire aux fonctionnaires et autres agents du SGC l'autorisation d'accéder à des ICUE pour une fonction déterminée. Ces autorisations temporaires sont valables pour une période ne dépassant pas six mois et ne donnent pas accès aux informations classifiées TRÈS SECRET UE/EU TOP SECRET. Toutes les personnes auxquelles a été délivrée une autorisation temporaire reconnaissent par écrit qu'elles sont conscientes de leurs obligations en matière de protection des ICUE et des conséquences qui pourraient résulter si des ICUE devaient être compromises. Le SGC tient un registre de ces déclarations écrites.

34. Lorsqu'une personne doit être affectée à un poste requérant une habilitation de sécurité dont le niveau dépasse d'un niveau celui qu'elle possède, l'affectation peut être décidée à titre provisoire, pour autant que les conditions suivantes soient réunies:

a) l'accès aux ICUE d'un niveau supérieur répond à une nécessité impérieuse qui doit être justifiée par écrit par le supérieur hiérarchique de la personne concernée;

b) l'accès doit être limité à des éléments particuliers des ICUE et servir aux attributions;

c) la personne détient une HSP valable ou une autorisation valable aux fins de l'accès à des ICUE;

d) des démarches ont été entreprises en vue d'obtenir une autorisation pour le niveau d'accès nécessaire pour le poste;

e) des contrôles satisfaisants ont été effectués par l'autorité compétente permettant d'établir l'absence de violations graves ou répétées du règlement de sécurité par la personne concernée;

f) l'affectation de la personne est approuvée par l'autorité compétente; et

g) une trace de l'accès exceptionnel, y compris une description des informations auxquelles accès a été donné, doit être conservée par le bureau d'ordre ou le bureau d'ordre subordonné compétent.

35. La procédure décrite ci-dessus est utilisée pour un accès ponctuel à des ICUE dont la classification dépasse d'un niveau le niveau d'habilitation de la personne concernée. Il ne convient pas de recourir de manière répétée à cette procédure.

36. Dans des circonstances très exceptionnelles, c'est-à-dire en cas de missions dans un environnement hostile ou au cours de périodes de tension internationale croissante lorsque des mesures d'urgence l'exigent, plus particulièrement afin de sauver des vies, les États membres et le secrétaire général peuvent accorder, si possible par écrit, un accès à des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET à des personnes qui ne détiennent pas l'habilitation de sécurité requise, à condition que l'accès accordé soit absolument indispensable et qu'il n'y ait pas de raison de douter de la loyauté, de l'intégrité et de la fiabilité de la personne concernée. Une trace de l'autorisation précisant les informations pour lesquelles l'accès a été approuvé doit être conservée.

37. Pour les informations classifiées TRÈS SECRET UE/EU TOP SECRET, un tel accès d'urgence est limité aux ressortissants d'États membres de l'Union s'étant vu octroyer l'accès soit à des informations dont le niveau de classification national équivaut à TRÈS SECRET UE/EU TOP SECRET soit à des informations classifiées SECRET UE/EU SECRET.

38. Le comité de sécurité est informé des cas où il est recouru à la procédure décrite aux paragraphes 36 et 37.

39. Lorsque les dispositions législatives et réglementaires d'un État membre édictent des règles plus strictes en matière d'autorisations temporaires, d'affectations provisoires ou d'accès ponctuel ou d'urgence des personnes concernées à des informations classifiées, les procédures prévues dans la présente section ne sont appliquées que dans les limites éventuellement imposées par les dispositions législatives et réglementaires nationales en vigueur.

40. Chaque année, le comité de sécurité reçoit un rapport sur le recours aux procédures énoncées dans la présente section.

VI. PARTICIPATION AUX SESSIONS ET RÉUNIONS DANS LE CADRE DU CONSEIL

41. Sous réserve du paragraphe 28, les personnes désignées pour participer à des sessions du Conseil ou à des réunions d'instances préparatoires du Conseil au sein desquelles des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur sont traitées, ne peuvent le faire qu'après confirmation de la situation de l'intéressé au regard de l'habilitation de sécurité. Pour les délégués, un CHSP ou une autre preuve d'habilitation de sécurité doit être transmis au bureau de sécurité du SGC par les autorités compétentes ou, à titre exceptionnel, présenté par le délégué concerné. Le cas échéant, il peut être fait usage d'une liste de noms récapitulative mentionnant les preuves d'habilitation de sécurité voulues.

42. Lorsqu'une HSP, accordée à des fins d'accès à des ICUE, est, pour des raisons de sécurité, retirée à une personne dont les fonctions requièrent la participation à des sessions du Conseil ou à des réunions d'instances préparatoires du Conseil, l'autorité compétente en informe le SGC.

VII. ACCÈS POTENTIEL AUX ICUE

43. Les courriers, les gardes et les escortes doivent disposer d'une habilitation de sécurité du niveau correspondant ou faire l'objet d'une enquête appropriée conformément aux dispositions législatives et réglementaires nationales, et être informés des procédures de sécurité applicables à la protection des ICUE ainsi que des obligations qui leur incombent en matière de protection des informations de cette nature qui leur sont confiées.

ANNEXE II

SÉCURITÉ PHYSIQUE

I. INTRODUCTION

1. La présente annexe énonce les modalités d'application de l'article 8. Elle prévoit les règles minimales de protection physique des locaux, bâtiments, bureaux, salles et autres zones où des ICUE sont traitées et stockées, y compris des zones où se trouvent des SIC.

2. Les mesures de sécurité physique sont destinées à prévenir l'accès non autorisé aux ICUE en:

   a) garantissant que les ICUE sont correctement traitées et stockées;

   b) permettant d'établir une distinction entre les membres du personnel au regard de l'accès aux ICUE sur la base de leur besoin d'en connaître et, le cas échéant, de leur habilitation de sécurité;

   c) ayant un effet dissuasif, en empêchant et en détectant les actes non autorisés; et

   d) en empêchant ou en retardant toute intrusion par la ruse ou par la force.

II. RÈGLES ET MESURES EN MATIÈRE DE SÉCURITÉ PHYSIQUE

3. Les mesures de sécurité physique sont choisies en fonction d'une évaluation de la menace réalisée par les autorités compétentes. Il convient que tant le SGC que les États membres appliquent une procédure de gestion du risque pour protéger les ICUE dans leurs locaux afin de garantir un niveau de protection physique qui soit proportionné au risque évalué. La procédure de gestion des risques tient compte de tous les facteurs pertinents, et notamment:

   a) du niveau de classification des ICUE;

   b) de la forme et du volume des ICUE, sachant que l'application de mesures de protection plus strictes pourrait être requise pour des volumes importants ou en cas de compilation d'ICUE;

   c) de l'environnement et de la structure des bâtiments ou des zones où se trouvent des ICUE; et

   d) de l'évaluation de la menace que constituent les services de renseignement prenant pour cible l'Union ou des États membres, ainsi que les actes de sabotage, le terrorisme et les activités subversives ou les autres activités criminelles.

4. En appliquant la notion de défense en profondeur, l'autorité de sécurité compétente détermine la bonne combinaison de mesures de sécurité physique qu'il convient de mettre en œuvre. Il peut s'agir d'une ou de plusieurs des mesures suivantes:

   a) barrière périmétrique: une barrière physique qui défend les limites d'une zone devant être protégée;

   b) système de détection des intrusions (SDI): un tel système peut être utilisé pour améliorer le niveau de sécurité d'une barrière périmétrique ou dans des salles et des bâtiments pour remplacer le personnel de sécurité ou l'aider dans sa tâche;

   c) contrôle des accès: il peut être exercé sur un site, un ou plusieurs bâtiments d'un site ou des zones ou salles à l'intérieur d'un bâtiment. Ce contrôle peut être exercé par des moyens électroniques ou électromécaniques, par un membre du personnel de sécurité et/ou un réceptionniste, ou par tout autre moyen physique;

   d) personnel de sécurité: un personnel de sécurité formé, supervisé et, au besoin, dûment habilité peut être employé, notamment, pour dissuader des personnes de planifier des intrusions clandestines;

   e) système de télévision en circuit fermé (CCTV): un tel système peut être utilisé par le personnel de sécurité pour effectuer des vérifications en cas d'incident ou de déclenchement de l'alarme des SDI sur des sites étendus ou des enceintes;

   f) éclairage de sécurité: un tel éclairage peut être utilisé pour dissuader un intrus potentiel ainsi que pour fournir la lumière nécessaire à une surveillance efficace, soit directement par le personnel de sécurité soit indirectement par l'intermédiaire d'un système de CCTV; et

   g) toute autre mesure physique appropriée destinée à avoir un effet dissuasif quant à l'accès non autorisé ou à détecter un tel accès, ou à prévenir la perte ou la détérioration d'ICUE.

5. L'autorité compétente peut être autorisée à mener des fouilles aux entrées et aux sorties afin d'avoir un effet dissuasif quant à l'introduction non autorisée de matériel dans des locaux ou des bâtiments ou au retrait non autorisé de toute ICUE des lieux précités.

6. Lorsque des ICUE risquent d'être vues, même accidentellement, des mesures appropriées sont prises pour parer à ce risque.

7. Pour les nouveaux établissements, les règles en matière de sécurité physique et leurs spécifications fonctionnelles doivent être définies lors de la planification et de la conception des établissements. Pour les établissements existants, les règles en matière de sécurité physique doivent être appliquées dans toute la mesure du possible.

III. ÉQUIPEMENT DESTINÉ À LA PROTECTION PHYSIQUE DES ICUE

8. Lors de l'achat de l'équipement destiné à la protection physique des ICUE (comme des meubles de sécurité, des déchiqueteuses, des serrures de porte, des systèmes électroniques de contrôle des accès, des SDI, des systèmes d'alarme), l'autorité de sécurité compétente veille à ce que cet équipement réponde aux normes techniques et aux conditions minimales agréées.

9. Les spécifications techniques de l'équipement devant servir à la protection physique des ICUE sont définies dans des lignes directrices en matière de sécurité, qu'il appartient au comité de sécurité d'approuver.

10. Les systèmes de sécurité sont périodiquement inspectés et l'équipement est entretenu à intervalles réguliers. L'entretien prend en compte les résultats des inspections afin de garantir un fonctionnement optimal continu de l'équipement.

11. Il convient de réévaluer à chaque inspection l'efficacité des différentes mesures de sécurité et du système de sécurité dans son ensemble.

IV. ZONES PHYSIQUEMENT PROTÉGÉES

12. Deux types de zones physiquement protégées, ou leurs équivalents au niveau national, sont créés en vue de la protection physique des ICUE:

    a) les zones administratives; et

    b) les zones sécurisées (dont les zones sécurisées du point de vue technique).

    Dans la présente décision, toutes les références aux zones administratives et aux zones sécurisées, y compris les zones sécurisées du point de vue technique, s'entendent comme visant également les zones équivalentes au niveau national.

13. Il appartient à l'autorité de sécurité compétente d'établir qu'une zone répond aux conditions requises pour être désignée comme zone administrative, zone sécurisée ou zone sécurisée du point de vue technique.

14. Pour les zones administratives:

    a) un périmètre défini est établi de façon visible afin de permettre le contrôle des personnes et, dans la mesure du possible, des véhicules;

    b) ne peuvent y pénétrer sans escorte que les personnes dûment autorisées par l'autorité compétente; et

    c) toutes les autres personnes sont escortées en permanence ou font l'objet de contrôles équivalents.

15. Pour les zones sécurisées:

    a) un périmètre défini et protégé est établi de façon visible et toutes les entrées et sorties sont contrôlées par un système de laissez-passer ou d'identification individuelle;

    b) ne peuvent y pénétrer sans escorte que les personnes habilitées et expressément autorisées à y entrer sur la base de leur besoin d'en connaître; et

    c) toutes les autres personnes sont escortées en permanence ou font l'objet de contrôles équivalents.

16. Lorsque le fait de pénétrer dans une zone sécurisée équivaut en pratique à un accès direct aux informations classifiées qu'elle renferme, les règles supplémentaires suivantes sont d'application:

    a) le niveau de classification le plus élevé qui s'applique aux informations conservées habituellement dans la zone doit être clairement indiqué;

    b) tous les visiteurs doivent disposer d'une autorisation spécifique pour pénétrer dans la zone, sont escortés en permanence et disposent de l'habilitation de sécurité correspondante, sauf si des mesures sont prises pour empêcher l'accès aux ICUE.

17. Les zones sécurisées qui sont protégées contre les écoutes sont qualifiées de zones sécurisées du point de vue technique. Les règles supplémentaires suivantes sont applicables:

    a) ces zones sont équipées de SDI, verrouillées lorsqu'elles ne sont pas occupées et gardées lorsqu'elles sont occupées. Toutes les clés sont contrôlées conformément à la section VI;

    b) toutes les personnes et tous les matériels entrant dans ces zones sont contrôlés;

    c) ces zones doivent faire l'objet, à intervalles réguliers, d'inspections physiques et/ou techniques selon les exigences de l'autorité de sécurité compétente. Ces inspections doivent également être effectuées après une entrée non autorisée, réelle ou présumée; et

    d) ces zones ne sont pas équipées de lignes de communication, de téléphones ou d'autres dispositifs de communication ou matériels électriques ou électroniques qui ne sont pas autorisés.

18. Nonobstant le paragraphe 17, point d), avant d'être utilisé dans des zones dans lesquelles sont organisées des réunions ou sont exécutées des tâches mettant en jeu des informations classifiées SECRET UE/EU SECRET et d'un niveau de classification supérieur, et lorsque la menace pesant sur des ICUE est jugée élevée, tout dispositif de communication et tout matériel électrique ou électronique est d'abord examiné par l'autorité de sécurité compétente pour vérifier qu'aucune information intelligible ne peut être transmise par inadvertance ou de manière illicite par ces équipements en dehors du périmètre de la zone sécurisée.

19. Les zones sécurisées qui ne sont pas occupées vingt-quatre heures sur vingt-quatre par le personnel de service sont, au besoin, inspectées après les heures normales de travail et à intervalles aléatoires en dehors de ces heures, sauf si un SDI a été installé.

20. Des zones sécurisées et des zones sécurisées du point de vue technique peuvent être temporairement établies dans une zone administrative en vue de la tenue d'une réunion classifiée ou à toute autre fin similaire.

21. Des procédures d'exploitation de sécurité sont arrêtées pour chacune des zones sécurisées et précisent:

    a) le niveau de classification des ICUE traitées ou stockées dans la zone;

    b) les mesures de surveillance et de protection qu'il convient de mettre en place;

    c) les personnes autorisées à pénétrer dans la zone en raison de leur besoin d'en connaître et en fonction de leur habilitation;

    d) le cas échéant, les procédures applicables aux escortes ou à la protection des ICUE lorsque d'autres personnes sont autorisées à pénétrer dans la zone; et

    e) les autres mesures et procédures applicables.

22. Les chambres fortes sont installées dans des zones sécurisées. Les murs, les planchers, les plafonds, les fenêtres et les portes verrouillables sont approuvés par l'autorité de sécurité compétente et offrent une protection équivalente à celle d'un meuble de sécurité approuvé pour le stockage d'ICUE du même niveau de classification.

V. MESURES DE PROTECTION PHYSIQUES APPLICABLES AU TRAITEMENT ET AU STOCKAGE DES ICUE

23. Les ICUE RESTREINT UE/EU RESTRICTED peuvent être traitées:

    a) dans une zone sécurisée;

    b) dans une zone administrative à condition que les personnes non autorisées ne puissent avoir accès aux ICUE; ou

    c) en dehors d'une zone sécurisée ou d'une zone administrative à condition que le détenteur les transporte conformément aux dispositions de l'annexe III, paragraphes 28 à 41, et se soit engagé à se conformer aux mesures compensatoires prévues dans les instructions de sécurité émises par l'autorité de sécurité compétente pour empêcher que des personnes non autorisées aient accès aux ICUE.

24. Les ICUE RESTREINT UE/EU RESTRICTED sont stockées dans un meuble de bureau adapté et fermé dans une zone administrative ou dans une zone sécurisée. Ces informations peuvent être temporairement stockées en dehors d'une zone sécurisée ou d'une zone administrative à condition que le détenteur se soit engagé à se conformer aux mesures compensatoires prévues dans les instructions de sécurité émises par l'autorité de sécurité compétente.

25. Les ICUE CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET peuvent être traitées:

a) dans une zone sécurisée;

b) dans une zone administrative à condition que les personnes non autorisées ne puissent avoir accès aux ICUE; ou

c) en dehors d'une zone sécurisée ou d'une zone administrative à condition que le détenteur:

i) transporte les ICUE conformément aux dispositions de l'annexe III, paragraphes 28 à 41;

ii) se soit engagé à se conformer aux mesures compensatoires prévues dans les instructions de sécurité émises par l'autorité de sécurité compétente pour empêcher que des personnes non autorisées aient accès aux ICUE;

iii) exerce en personne un contrôle permanent sur les ICUE; et

iv) si les documents sont sous forme papier, qu'il en ait informé le bureau d'ordre compétent.

26. Les ICUE CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET sont stockées dans une zone sécurisée, soit dans un meuble de sécurité soit dans une chambre forte.

27. Les ICUE TRÈS SECRET UE/EU TOP SECRET sont traitées dans une zone sécurisée.

28. Les ICUE TRÈS SECRET UE/EU TOP SECRET sont stockées dans une zone sécurisée, selon l'une des modalités suivantes:

a) dans un meuble de sécurité conformément au paragraphe 8, moyennant un ou plusieurs des contrôles supplémentaires suivants:

i) protection ou vérification en permanence par un membre habilité du personnel de sécurité ou du personnel de service;

ii) un système de détection des intrusions approuvé auquel on associe du personnel de sécurité prêt à intervenir en cas d'incident;

b) dans une chambre forte équipée d'un système de détection des intrusions à laquelle on associe du personnel de sécurité prêt à intervenir en cas d'incident.

29. Les règles régissant le transport des ICUE en dehors des zones physiquement protégées figurent à l'annexe III.

VI. CONTRÔLE DES CLÉS ET COMBINAISONS UTILISÉES POUR LA PROTECTION DES ICUE

30. L'autorité de sécurité compétente définit les procédures de gestion des clés et des combinaisons pour les bureaux, les salles, les chambres fortes et les meubles de sécurité. Ces procédures protègent d'un accès non autorisé.

31. Les combinaisons doivent être mémorisées par le plus petit nombre possible de personnes qui ont besoin de les connaître. Les combinaisons des meubles de sécurité et des chambres fortes servant au stockage d'ICUE doivent être changées:

a) à la réception d'un nouveau meuble;

b) lors de tout changement du personnel connaissant la combinaison;

c) en cas de compromission, réelle ou présumée;

d) lorsqu'une serrure a fait l'objet d'un entretien ou d'une réparation; et

e) au moins tous les douze mois.

ANNEXE III

GESTION DES INFORMATIONS CLASSIFIÉES

I. INTRODUCTION

1. La présente annexe énonce les modalités d'application de l'article 9. Elle prévoit les mesures administratives visant à contrôler les ICUE tout au long de leur cycle de vie en vue de contribuer à la prévention et à la détection d'une compromission ou d'une perte délibérée ou accidentelle de telles informations.

II. GESTION DE LA CLASSIFICATION

Classifications et marquages

2. Les informations sont classifiées dans les cas où elles doivent être protégées compte tenu de leur confidentialité.

3. L'autorité d'origine des ICUE est chargée de déterminer le niveau de classification de sécurité, conformément aux lignes directrices applicables en matière de classification, et de la diffusion initiale des informations.

4. Le niveau de classification des ICUE est fixé conformément à l'article 2, paragraphe 2, et en se reportant à la politique de sécurité qui doit être approuvée conformément à l'article 3, paragraphe 3.

5. La classification de sécurité est clairement et correctement indiquée, indépendamment de la forme sous laquelle se présentent les ICUE: format papier, forme orale, électronique ou autre.

6. Les différentes parties d'un document donné (pages, paragraphes, sections, annexes, appendices et pièces jointes) peuvent nécessiter une classification différente et doivent alors porter le marquage afférent, y compris lorsqu'elles sont stockées sous forme électronique.

7. Le niveau général de classification d'un document ou d'un dossier est au moins aussi élevé que celui de sa partie portant la classification la plus élevée. Lorsqu'il rassemble des informations provenant de plusieurs sources, le document final est examiné pour en fixer le niveau général de classification de sécurité car il peut requérir un niveau de classification supérieur à celui de chacune des parties qui le composent.

8. Dans la mesure du possible, les documents dont toutes les parties n'ont pas le même niveau de classification sont structurés de manière que les parties ayant des niveaux de classification différents puissent au besoin être aisément identifiées et séparées des autres.

9. Les lettres ou notes d'envoi accompagnant des pièces jointes portent le plus haut niveau de classification attribué à ces dernières. L'autorité d'origine indique clairement leur niveau de classification lorsqu'elles sont séparées de leurs pièces jointes, au moyen d'un marquage approprié, par exemple:

   CONFIDENTIEL UE/EU CONFIDENTIAL

   Sans pièce(s) jointe(s) RESTREINT UE/EU RESTRICTED

Marquages

10. Outre l'un des marquages de classification de sécurité prévus à l'article 2, paragraphe 2, les ICUE peuvent porter des marquages complémentaires, tels que:

    a) un identifiant désignant l'autorité d'origine;

    b) des marquages restrictifs, des mots-codes ou des acronymes utilisés pour préciser le domaine d'activité sur lequel porte le document ou pour indiquer une diffusion particulière en fonction du besoin d'en connaître ou des restrictions d'utilisation;

    c) des marquages relatifs à la communicabilité; ou

    d) le cas échéant, la date ou l'événement particulier à partir desquels elles peuvent être déclassées ou déclassifiées.

Abréviations indiquant la classification

11. Des abréviations uniformisées indiquant la classification peuvent être utilisées pour préciser le niveau de classification des différents paragraphes d'un texte. Les abréviations ne remplacent pas la mention de la classification en toutes lettres.

12. Les abréviations uniformisées ci-après peuvent être utilisées dans les documents classifiés de l'Union européenne pour indiquer le niveau de classification de sections ou blocs de texte de moins d'une page:

TRÈS SECRET UE/EU TOP SECRET	TS-UE/EU-TS
SECRET UE/EU SECRET	S-UE/EU-S
CONFIDENTIEL UE/EU CONFIDENTIAL	C-UE/EU-C
RESTREINT UE/EU RESTRICTED	R-UE/EU-R

Création d'ICUE

13. Lors de la création de documents classifiés de l'Union européenne:

a) sur chaque page figure un marquage indiquant clairement le niveau de classification;

b) chaque page est numérotée;

c) le document porte un numéro de référence et un sujet qui n'est pas lui-même une information classifiée, sauf s'il s'est vu apposer un marquage à ce titre;

d) le document est daté; et

e) les documents classifiés SECRET UE/EU SECRET ou d'un niveau de classification supérieur portent un numéro d'exemplaire sur chaque page dès lors qu'ils doivent être diffusés en plusieurs exemplaires.

14. Lorsqu'il n'est pas possible d'appliquer le paragraphe 13 à des ICUE, d'autres mesures appropriées sont prises conformément aux lignes directrices en matière de sécurité qui doivent être arrêtées en vertu de l'article 6, paragraphe 2.

Déclassement et déclassification des ICUE

15. Au moment de la création du document classifié, l'autorité d'origine indique, si possible et notamment en ce qui concerne les informations classifiées RESTREINT UE/EU RESTRICTED, si les ICUE qui y figurent peuvent ou non être déclassées ou déclassifiées à une date donnée ou après un événement spécifique.

16. Le SGC réexamine régulièrement les ICUE en sa possession pour déterminer si leur niveau de classification est toujours d'application. Le SGC instaure un système pour réexaminer le niveau de classification des ICUE dont il est l'auteur, au moins une fois tous les cinq ans. Un tel réexamen n'est pas nécessaire lorsque l'autorité d'origine a indiqué dès le départ que les informations seraient automatiquement déclassées ou déclassifiées et que celles-ci se sont vu apposer les marquages correspondants.

III. ENREGISTREMENT DES ICUE À DES FINS DE SÉCURITÉ

17. Pour chacune des entités structurées qui existent au sein du SGC et des administrations nationales des États membres et dans lesquelles des ICUE sont traitées, on détermine un bureau d'ordre compétent chargé de veiller à ce que les ICUE soient traitées conformément à la présente décision. Les bureaux d'ordre sont conçus comme des zones sécurisées telles que définies à l'annexe II.

18. Aux fins de la présente décision, on entend par enregistrement à des fins de sécurité (ci-après dénommé «enregistrement») l'application de procédures permettant de garder la trace du cycle de vie d'un matériel, y compris de sa diffusion et de sa destruction.

19. Tout matériel classifié CONFIDENTIEL UE/EU CONFIDENTIAL et d'un niveau de classification supérieur est enregistré par un bureau d'ordre déterminé à chaque fois qu'il parvient à une entité structurée ou qu'il en sort.

20. Le bureau d'ordre central du SGC garde une trace de toutes les informations classifiées communiquées par le Conseil et le SGC à des États tiers et à des organisations internationales, ainsi que de toutes les informations classifiées reçues d'États tiers ou d'organisations internationales.

21. Dans le cas d'un SIC, les procédures d'enregistrement peuvent être mises en œuvre au moyen de processus intervenant au sein du SIC même.

22. Le Conseil approuve une politique de sécurité sur l'enregistrement des ICUE à des fins de sécurité.

Bureaux d'ordre TRÈS SECRET UE/EU TOP SECRET

23. Un bureau d'ordre est désigné dans les États membres et au SGC pour faire fonction d'autorité centrale de réception et de diffusion des informations classifiées TRÈS SECRET UE/EU TOP SECRET. S'il y a lieu, les bureaux d'ordre subordonnés peuvent être désignés pour traiter ces informations à des fins d'enregistrement.

24. Ces bureaux d'ordre subordonnés ne peuvent transmettre de documents TRES SECRET UE/EU TOP SECRET directement à d'autres bureaux d'ordre subordonnés rattachés au même bureau d'ordre TRES SECRET UE/EU TOP SECRET central sans l'autorisation expresse et écrite de ce dernier ni à des bureaux d'ordre extérieurs.

IV. DUPLICATION ET TRADUCTION DES DOCUMENTS CLASSIFIÉS DE L'UNION EUROPÉENNE

25. Les documents classifiés TRÈS SECRET UE/EU TOP SECRET ne doivent pas être dupliqués ou traduits sans le consentement écrit préalable de l'autorité d'origine.

26. Lorsque l'autorité d'origine de documents classifiés SECRET UE/EU SECRET et d'un niveau de classification inférieur n'a pas imposé de restrictions à leur duplication ou à leur traduction, lesdits documents peuvent être dupliqués ou traduits sur instruction du détenteur.

27. Les mesures de sécurité applicables au document original le sont aussi à ses copies et à ses traductions.

V. TRANSPORT DES ICUE

28. Le transport des ICUE est soumis aux mesures de protection énoncées aux paragraphes 30 à 41. Lorsque les ICUE sont transportées par des supports électroniques, et nonobstant l'article 9, paragraphe 4, les mesures de protection énoncées ci-après peuvent être complétées par des contre-mesures techniques appropriées prescrites par l'autorité de sécurité compétente, de façon à réduire au minimum le risque de perte ou de compromission.

29. Les autorités de sécurité compétentes au sein du SGC et dans les États membres donnent des instructions sur le transport des ICUE conformément à la présente décision.

À l'intérieur d'un même bâtiment ou d'un groupe autonome de bâtiments

30. Les ICUE transportées à l'intérieur d'un même bâtiment ou d'un groupe autonome de bâtiments sont dissimulées en vue de prévenir l'observation de leur contenu.

31. À l'intérieur d'un même bâtiment ou d'un groupe autonome de bâtiments, les informations classifiées TRÈS SECRET UE/EU TOP SECRET sont transportées dans une enveloppe sécurisée avec pour seule mention le nom du destinataire.

À l'intérieur de l'Union

32. Les ICUE transportées entre des bâtiments ou des locaux à l'intérieur de l'Union européenne sont emballées de manière à être protégées de toute divulgation non autorisée.

33. Le transport d'informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET à l'intérieur de l'Union s'effectue par l'un des moyens suivants:

a) le courrier militaire, gouvernemental ou diplomatique, selon le cas;

b) le transport par porteur, à condition:

i) que le porteur ne se sépare pas des ICUE, à moins que leur stockage ne soit assuré conformément aux règles énoncées à l'annexe II;

ii) que les ICUE ne soit pas déballées pendant le transport ni lues dans des lieux publics;

iii) que la personne soit informée des responsabilités qui lui incombent en matière de sécurité; et

iv) que la personne soit, si nécessaire, munie d'un certificat de courrier.

c) les services postaux ou les services de courrier commercial, à condition:

i) qu'ils soient agréés par l'ANS compétente conformément aux dispositions législatives et réglementaires nationales; et

ii) qu'ils appliquent les mesures de protection appropriées conformément aux exigences minimales qui seront prévues dans les lignes directrices en matière de sécurité arrêtées en vertu de l'article 6, paragraphe 2.

En cas de transport d'un État membre vers un autre État membre, les dispositions du point c) sont limitées aux informations classifiées jusqu'au niveau CONFIDENTIEL UE/EU CONFIDENTIAL.

34. Les informations classifiées RESTREINT UE/EU RESTRICTED peuvent aussi être transportées par des services postaux ou par des services de courrier commercial. Un certificat de courrier n'est pas requis pour le transport de telles informations.

35. Le matériel classifié CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET (par exemple, équipement ou machine) qui ne peut être transporté par les moyens visés au paragraphe 33 est transporté en tant que fret par des sociétés de transport commercial conformément à l'annexe V.

36. Le transport des informations classifiées TRÈS SECRET UE/EU TOP SECRET, entre des bâtiments ou des locaux à l'intérieur de l'Union, s'effectue par courrier militaire, gouvernemental ou diplomatique, selon le cas.

De l'Union vers le territoire d'un État tiers

37. Les ICUE transportées de l'Union vers le territoire d'un État tiers sont emballées de manière à être protégées de toute divulgation non autorisée.

38. Le transport des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET de l'Union vers le territoire d'un État tiers s'effectue par l'un des moyens suivants:

a) le courrier militaire ou diplomatique;

b) le transport par porteur, à condition:

i) que le paquet porte un sceau officiel ou soit emballé de manière à indiquer qu'il s'agit d'un envoi officiel ne devant pas être soumis à contrôle douanier ou de sécurité;

ii) que la personne soit munie d'un certificat de courrier identifiant le paquet et l'autorisant à le transporter;

iii) que le porteur ne se sépare pas des ICUE, à moins que leur stockage ne soit assuré conformément aux règles énoncées à l'annexe II;

iv) que les ICUE ne soit pas déballées pendant le transport ni lues dans des lieux publics; et

v) que la personne soit informée des responsabilités qui lui incombent en matière de sécurité.

39. Le transport des informations CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET communiquées par l'Union à un État tiers ou à une organisation internationale est conforme aux dispositions applicables au titre d'un accord sur la sécurité des informations ou d'un arrangement administratif conclu en vertu de l'article 13, paragraphe 2, point a) ou b).

40. Les informations classifiées RESTREINT UE/EU RESTRICTED peuvent aussi être transportées par des services postaux ou par des services de courrier commercial.

41. Le transport des informations classifiées TRÈS SECRET UE/EU TOP SECRET, de l'Union vers le territoire d'un État tiers, s'effectue par courrier militaire ou diplomatique.

VI. DESTRUCTION DES ICUE

42. Les documents classifiés de l'Union européenne qui ne sont plus nécessaires peuvent être détruits, sans préjudice de la réglementation applicable en matière d'archivage.

43. Les documents faisant l'objet d'un enregistrement en application de l'article 9, paragraphe 2, de la présente décision sont détruits par le bureau d'ordre compétent sur instruction du détenteur ou d'une autorité compétente. Les cahiers d'enregistrement et les autres informations relatives aux enregistrements sont actualisés en conséquence.

44. La destruction de documents classifiés SECRET UE/EU SECRET ou TRÈS SECRET UE/EU TOP SECRET est effectuée en présence d'un témoin justifiant de l'habilitation de sécurité correspondant au moins au niveau de classification du document à détruire.

45. L'agent du bureau d'ordre et le témoin, lorsque la présence de ce dernier est requise, signent un procès-verbal de destruction qui est rempli dans le bureau d'ordre. Le bureau d'ordre conserve les procès-verbaux de destruction des documents TRÈS SECRET UE/EU TOP SECRET pendant dix ans au minimum, et ceux des documents CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET pendant cinq ans au minimum.

46. Les documents classifiés, y compris ceux dont la classification est RESTREINT UE/EU RESTRICTED, sont détruits par des méthodes répondant aux normes de l'Union applicables ou à des normes équivalentes, ou homologuées par les États membres conformément aux normes techniques nationales, pour empêcher leur reconstitution totale ou partielle.

47. La destruction des supports de données informatiques utilisés pour des ICUE s'effectue conformément à l'annexe IV, paragraphe 37.

48. En cas d'urgence, s'il existe un risque imminent de divulgation non autorisée, les ICUE sont détruites par le détenteur de manière à ce qu'elles ne puissent pas être reconstituées en tout ou en partie. L'autorité d'origine et le bureau d'ordre d'origine sont informés de la destruction en urgence d'ICUE enregistrées.

VII. VISITES D'ÉVALUATION

49. Le terme «visite d'évaluation» utilisé ci-après désigne:

a) toute inspection ou visite d'évaluation visée à l'article 9, paragraphe 3, et à l'article 16, paragraphe 2, points e), f) et g); ou

b) toute visite d'évaluation visée à l'article 13, paragraphe 5,

ayant pour but d'évaluer l'efficacité des mesures mises en œuvre pour protéger les ICUE.

50. Les visites d'évaluation sont notamment menées aux fins suivantes:

a) veiller à ce que les normes minimales requises fixées dans la présente décision en matière de protection des ICUE soient respectées;

b) mettre l'accent sur l'importance de la sécurité et d'une gestion efficace des risques au sein des entités inspectées;

c) recommander des contre-mesures pour atténuer l'impact particulier de la perte de confidentialité, d'intégrité ou de disponibilité des informations classifiées; et

d) renforcer les programmes mis en place par les autorités de sécurité en matière de formation et de sensibilisation à la sécurité.

51. Avant la fin de chaque année civile, le Conseil adopte le programme de visites d'évaluation prévu à l'article 16, paragraphe 1, point c), pour l'année suivante. Les dates exactes de chaque visite d'évaluation sont fixées en accord avec l'organe ou l'agence de l'Union, l'État membre, l'État tiers ou l'organisation internationale concerné(e).

Conduite des visites d'évaluation

52. Les visites d'évaluation sont effectuées en vue de contrôler les prescriptions, les réglementations et les procédures applicables dans l'entité visitée et de vérifier que les pratiques en vigueur au sein de l'entité satisfont aux principes de base et aux normes minimales fixés par la présente décision et par les dispositions qui régissent l'échange d'informations classifiées avec cette entité.

53. Les visites d'évaluation se déroulent en deux phases. Avant la visite proprement dite, une réunion préparatoire est organisée, si nécessaire, avec l'entité concernée. À l'issue de cette réunion préparatoire, l'équipe d'évaluation établit, de concert avec ladite entité, un programme de visite détaillé couvrant tous les secteurs de la sécurité. L'équipe d'évaluation devrait avoir accès à tous les lieux, notamment aux bureaux d'ordre et aux points de présence SIC, où sont traitées des ICUE.

54. Les visites d'évaluation effectuées dans les administrations nationales des États membres, dans des États tiers et dans les organisations internationales sont réalisées en totale coopération avec les responsables de l'entité, de l'État tiers ou de l'organisation internationale faisant l'objet de la visite.

55. Les visites d'évaluation effectuées auprès d'organes, d'agences et d'entités de l'Union qui appliquent la présente décision ou les principes y figurant sont menées avec l'aide de spécialistes de l'ANS dans le ressort de laquelle se situe l'organe ou l'agence.

56. Dans le cadre des visites d'évaluation effectuées auprès des organes, agences et entités de l'Union qui appliquent la présente décision ou les principes y figurant, ainsi que dans des États tiers et des organisations internationales, le concours et l'assistance des experts des ANS peuvent être sollicités conformément à des modalités à définir par le comité de sécurité.

Rapports

57. À l'issue de la visite d'évaluation, les principales conclusions et recommandations sont présentées à l'entité ayant fait l'objet de la visite. Un rapport de visite d'évaluation est ensuite établi. Lorsque des mesures correctives et des recommandations ont été proposées, le rapport doit contenir suffisamment d'éléments précis pour étayer les conclusions dégagées. Le rapport est transmis à l'autorité compétente de l'entité ayant fait l'objet de la visite.

58. En ce qui concerne les visites d'évaluation effectuées dans les administrations nationales des États membres:

a) le projet de rapport d'évaluation est transmis à l'ANS concernée afin de vérifier qu'il ne contient pas d'erreur de fait et qu'aucune information d'un niveau de classification supérieur à RESTREINT UE/EU RESTRICTED n'y figure; et

b) sauf si l'ANS de l'État membre en question demande de surseoir à une diffusion générale, les rapports d'évaluation sont diffusés au comité de sécurité. Le rapport est classifié RESTREINT UE/EU RESTRICTED.

Un rapport périodique est établi sous la responsabilité de l'autorité de sécurité du SGC (bureau de sécurité) pour souligner les enseignements qui ont été tirés des visites d'évaluation effectuées dans les États membres au cours d'une période précise et est examiné par le comité de sécurité.

59. En ce qui concerne les visites d'évaluation dans les États tiers et les organisations internationales, le rapport est diffusé au comité de sécurité. Le rapport reçoit, au minimum, la classification RESTREINT UE/EU RESTRICTED. Toute mesure corrective est vérifiée lors d'une visite de suivi et signalée au comité de sécurité.

60. En ce qui concerne les visites d'évaluation effectuées auprès des organes, agences et entités de l'Union qui appliquent la présente décision ou les principes y figurant, les rapports de visite d'évaluation sont diffusés au comité de sécurité. Le projet de rapport de visite d'évaluation est transmis à l'agence ou à l'organe concerné(e) afin de vérifier qu'il ne contient pas d'erreur de fait et qu'aucune information d'un niveau de classification supérieur à RESTREINT UE/EU RESTRICTED n'y figure. Toute mesure corrective est vérifiée lors d'une visite de suivi et signalée au comité de sécurité.

61. L'autorité de sécurité du SGC procède régulièrement à des inspections des entités structurées du SGC aux fins prévues au paragraphe 50.

Liste de contrôle

62. L'autorité de sécurité du SGC (bureau de sécurité) établit et met à jour une liste de contrôle des éléments à vérifier au cours d'une visite d'évaluation. Cette liste de contrôle est transmise au comité de sécurité.

63. Les informations nécessaires pour compléter la liste de contrôle sont obtenues, notamment au cours de la visite, auprès des services chargés de la gestion de la sécurité de l'entité faisant l'objet de l'inspection. Sitôt complétée avec les réponses détaillées obtenues, la liste de contrôle est classifiée en accord avec l'entité inspectée. Elle ne fait pas partie du rapport d'inspection.

ANNEXE IV

PROTECTION DES ICUE TRAITÉES DANS LES SIC

I. INTRODUCTION

1. La présente annexe énonce les modalités d'application de l'article 10.

2. Les propriétés et les notions d'AI figurant ci-après sont essentielles pour la sécurité et l'exécution correcte des opérations dans le cadre d'un SIC.

Authenticité: garantie que l'information est véridique et émane de sources dignes de foi.

Disponibilité: caractéristique de l'information selon laquelle elle est accessible et utilisable, à la demande d'une entité autorisée.

Confidentialité: propriété selon laquelle les informations ne sont pas divulguées à des personnes ou à des entités non autorisées et l'accès à ces informations n'est pas accordé à des processus non autorisés.

Intégrité: propriété consistant à préserver l'exactitude et le caractère complet des informations et éléments.

Non-répudiation: la possibilité de prouver qu'une action ou un événement a eu lieu, de sorte qu'il ne peut être contesté par la suite.

II. PRINCIPES D'ASSURANCE DE L'INFORMATION

3. Les dispositions énoncées ci-après constituent les éléments fondamentaux permettant de garantir la sécurité de tout SIC traitant des ICUE. Les modalités précises de mise en œuvre de ces dispositions sont définies dans les politiques et les lignes directrices en matière de sécurité d'AI.

Gestion des risques de sécurité

4. La gestion des risques de sécurité fait partie intégrante de la définition, de l'élaboration, de l'exploitation et de la maintenance d'un SIC. La gestion des risques (évaluation, traitement, acceptation et communication) est mise en œuvre conjointement, dans le cadre d'un processus itératif, par les représentants des détenteurs de systèmes, les autorités responsables du projet, les autorités chargées de l'exploitation et les autorités d'homologation de sécurité selon une procédure d'évaluation des risques ayant fait ses preuves, transparente et pouvant être parfaitement comprise. Le domaine d'application du SIC et ses ressources sont clairement définis dès le début du processus de gestion des risques.

5. Les autorités compétentes examinent les menaces potentielles qui pèsent sur le SIC, tiennent à jour les évaluations des menaces et veillent à leur exactitude afin que celles-ci rendent compte de l'environnement opérationnel du moment. Elles actualisent en permanence leurs connaissances relatives aux questions de vulnérabilité et revoient régulièrement l'évaluation de la vulnérabilité afin de suivre l'évolution de la technologie de l'information.

6. Le traitement des risques de sécurité vise à appliquer un ensemble de mesures de sécurité offrant un équilibre satisfaisant entre les besoins des utilisateurs, les coûts et le risque de sécurité résiduel.

7. Les exigences spécifiques, l'étendue et le niveau de détail fixés par l'AHS compétente aux fins de l'homologation d'un SIC sont proportionnés au risque évalué, compte tenu de tous les facteurs pertinents, y compris le niveau de classification des ICUE qui sont traitées dans le SIC. Dans le cadre de l'homologation, le risque résiduel fait l'objet d'un énoncé formel et est accepté par une autorité responsable.

Sécurité du SIC tout au long de son cycle de vie

8. Assurer la sécurité d'un SIC tout au long de son cycle de vie, de son lancement à son retrait, est une obligation.

9. Le rôle de chaque acteur d'un SIC et les interactions entre ces acteurs, en termes de sécurité du système, doivent être clairement déterminés pour chaque phase du cycle de vie.

10. Tout SIC, y compris les mesures de sécurité techniques et non techniques dont il fait l'objet, est soumis à des essais de sécurité au cours du processus d'homologation afin de s'assurer que le niveau d'assurance requis est atteint et de vérifier qu'il est correctement mis en œuvre, intégré et configuré.

11. Des évaluations, inspections et examens de sécurité sont réalisés à intervalles réguliers durant la phase opérationnelle ainsi que dans le cadre de la maintenance d'un SIC, de même qu'en toute circonstance exceptionnelle.

12. Les documents relatifs à la sécurité d'un SIC évoluent tout au long du cycle de vie de celui-ci, évolution qui s'inscrit pleinement dans le cadre du processus de gestion du changement et de la configuration.

Meilleures pratiques

13. Le SGC et les États membres travaillent de concert à l'élaboration des meilleures pratiques destinées à protéger les ICUE traitées par un SIC. Les lignes directrices concernant les meilleures pratiques énoncent des mesures visant à assurer la sécurité du SIC sur le plan technique et physique ainsi qu'au niveau de l'organisation et des procédures et dont l'efficacité pour lutter contre certaines menaces et vulnérabilités a été démontrée.

14. Il convient, aux fins de la protection des ICUE traitées par un SIC, de mettre à profit les enseignements tirés par les entités travaillant dans le domaine de l'AI, que ce soit au sein ou en dehors de l'Union.

15. La diffusion et la mise en œuvre ultérieure des meilleures pratiques contribuent à atteindre un niveau équivalent d'assurance dans l'ensemble des SIC traitant des ICUE et exploités par le SGC et les États membres.

Défense en profondeur

16. Afin d'atténuer les risques qui pèsent sur un SIC, un éventail de mesures de sécurité techniques et non techniques organisées en plusieurs niveaux de défense doit être mis en œuvre. Ces niveaux sont notamment les suivants:

    a) *la dissuasion:* mesures de sécurité visant à dissuader un éventuel adversaire de projeter une attaque du SIC;

    b) *la prévention:* mesures de sécurité visant à empêcher ou à stopper une attaque du SIC;

    c) *la détection:* mesures de sécurité visant à déceler une attaque du SIC en train de se produire;

    d) *la résilience:* mesures de sécurité visant à faire en sorte que l'attaque n'ait un impact que sur un nombre aussi faible que possible d'informations ou de ressources du SIC et à prévenir d'autres dommages; et

    e) *le retour aux conditions opérationnelles:* mesures de sécurité visant à rétablir la sécurité du SIC.

    La rigueur de ces mesures de sécurité est déterminée sur la base d'une évaluation des risques.

17. L'ANS ou une autre autorité compétente s'assure:

    a) que les capacités de cyber défense sont mises en œuvre afin de faire face aux menacées dont l'ampleur dépasse les limites de l'organisation ou du pays touché; et

    b) que les réactions sont coordonnées et que les informations sur ces menaces et incidents et sur l'ensemble des risques qui en découlent sont partagées (capacités de réaction en cas d'urgence informatique).

Principes du minimalisme et du moindre privilège

18. Seuls sont mis en œuvre les fonctions, dispositifs et services indispensables pour répondre aux exigences opérationnelles.

19. Les utilisateurs d'un SIC et les processus automatisés se voient uniquement accorder les droits d'accès, les privilèges ou les autorisations requises pour mener à bien leur tâche, afin de limiter tout dommage résultant d'accidents, d'erreurs ou d'utilisations non autorisées des ressources du SIC.

20. Les procédures d'enregistrement mises en œuvre par un SIC, le cas échéant, sont vérifiées dans le cadre du processus d'homologation.

Sensibilisation à l'assurance de l'information

21. La sensibilisation aux risques et aux mesures de sécurité disponibles constitue la première ligne de défense destinée à assurer la sécurité des SIC. En particulier, tout le personnel intervenant dans le cycle de vie d'un SIC, y compris les utilisateurs, doit bien comprendre:

    a) que les défaillances en matière de sécurité peuvent porter gravement atteinte aux SIC;

    b) le préjudice potentiel que peuvent causer à autrui l'interconnectivité et l'interdépendance; et

    c) la responsabilité et l'obligation de rendre des comptes qui lui incombent concernant la sécurité du SIC, selon les fonctions qui sont les siennes dans le cadre des systèmes et processus.

22. Afin que les responsabilités en matière de sécurité soient bien comprises, une formation et une sensibilisation à l'AI sont obligatoires pour tout le personnel concerné, y compris les cadres supérieurs et les utilisateurs du SIC.

Évaluation et approbation des produits de sécurité informatique

23. Le niveau de confiance requis dans les mesures de sécurité, défini comme un niveau d'assurance, est déterminé à l'issue du processus de gestion des risques et conformément aux politiques et lignes directrices applicables en matière de sécurité.

24. Le niveau d'assurance fait l'objet d'une vérification au moyen de procédés et de méthodes reconnus à l'échelon international ou agréés au niveau national. Il s'agit principalement d'évaluations, de contrôles et d'audits.

25. Les produits cryptographiques destinés à protéger les ICUE sont évalués et agréés par une AAC nationale d'un État membre.

26. Avant d'être recommandés au Conseil ou au secrétaire général pour agrément, en application de l'article 10, paragraphe 6, ces produits cryptographiques doivent avoir satisfait à une évaluation par seconde partie réalisée par une autorité dûment qualifiée (AQUA) d'un État membre n'intervenant pas dans la conception ni dans la fabrication de l'équipement concerné. L'ampleur de l'évaluation par seconde partie nécessaire dépend du niveau de classification maximal envisagé des ICUE que ces produits doivent protéger. Le Conseil approuve une politique de sécurité concernant l'évaluation et l'agrément de produits cryptographiques.

27. Lorsque des motifs opérationnels particuliers le justifient, le Conseil ou le secrétaire général, selon le cas, peut, sur recommandation du comité de sécurité, ne pas respecter les exigences prévues aux paragraphes 25 et 26 de la présente annexe et délivrer un agrément à titre provisoire pour une période spécifique, en application de la procédure énoncée à l'article 10, paragraphe 6.

28. Le Conseil, statuant sur recommandation du comité de sécurité, peut accepter le processus d'évaluation, de sélection et d'homologation des produits cryptographiques qui est en place dans un État tiers ou dans une organisation internationale et peut en conséquence tenir ces produits cryptographiques comme homologués aux fins de la protection des ICUE communiquées à cet État tiers ou à cette organisation internationale.

29. L'AQUA est une AAC d'un État membre qui a été agréée, sur la base de critères définis par le Conseil, pour procéder à la deuxième évaluation des produits cryptographiques destinés à protéger les ICUE.

30. Le Conseil approuve une politique de sécurité concernant la qualification et l'approbation des produits de sécurité informatique non cryptographiques.

Transmission à l'intérieur de zones sécurisées et de zones administratives

31. Nonobstant les dispositions de la présente décision, lorsque la transmission d'ICUE s'effectue uniquement à l'intérieur de zones sécurisées ou de zones administratives, une transmission non chiffrée ou d'un niveau de chiffrement inférieur peut être envisagée compte tenu des résultats d'un processus de gestion des risques et avec l'accord de l'AHS.

Interconnexion sécurisée des SIC

32. Aux fins de la présente décision, on entend par «interconnexion» la connexion directe d'au moins deux systèmes informatiques permettant à ceux-ci d'échanger des données et d'autres ressources en matière d'information (communication, par exemple) de façon unidirectionnelle ou multidirectionnelle.

33. Un SIC doit de prime abord considérer tout système informatique interconnecté comme n'étant pas fiable et mettre en œuvre des mesures de protection destinées à contrôler les échanges d'informations classifiées.

34. Lorsqu'un SIC est interconnecté avec un autre système électronique, les conditions de base suivantes doivent être réunies:

a) les conditions opérationnelles ou d'activités pour ces interconnexions sont définies et approuvées par les autorités compétentes;

b) l'interconnexion est soumise à un processus de gestion des risques et d'homologation et est approuvée par les AHS compétentes; et

c) des services de protection en bordure (SPB) sont mis en place à la périphérie de tout SIC.

35. Il ne peut y avoir aucune interconnexion entre un SIC homologué et un réseau non protégé ou public, sauf lorsque le SIC comporte un système de protection en bordure homologué installé à cette fin entre le SIC et le réseau non protégé ou public. Les mesures de sécurité applicables à une telle interconnexion sont examinées par l'autorité chargée de l'assurance de l'information compétente et approuvées par l'AHS compétente.

    Lorsque le réseau public ou non protégé sert uniquement à des fins de transmission et que les données sont chiffrées au moyen d'un produit cryptographique agréé conformément à l'article 10, une telle connexion n'est pas considérée comme une interconnexion.

36. Un SIC homologué pour traiter des informations TRÈS SECRET UE/EU TOP SECRET ne peut pas être interconnecté directement ou en cascade à un réseau non protégé ou public.

Supports de données informatiques

37. Les supports de données informatiques sont détruits conformément aux procédures approuvées par l'autorité de sécurité compétente.

38. Les supports de données informatiques sont réutilisés, déclassés ou déclassifiés conformément aux lignes directrices en matière de sécurité qui doivent être arrêtées en vertu de l'article 6, paragraphe 2.

Situations d'urgence

39. Nonobstant les dispositions de la présente décision, les procédures spécifiques décrites ci-après peuvent être appliquées dans les situations d'urgence, telles que les crises, les conflits ou les guerres, imminentes ou effectives, ou dans des circonstances opérationnelles exceptionnelles.

40. Sous réserve du consentement de l'autorité compétente, les ICUE peuvent être transmises au moyen de produits cryptographiques agréés pour un niveau de classification inférieur ou sans faire l'objet d'un chiffrement dans le cas où tout retard causerait un préjudice indéniablement plus important que celui qui découlerait de la divulgation du matériel classifié et dans les conditions suivantes:

    a) l'expéditeur et le destinataire ne possèdent pas le dispositif de chiffrement nécessaire ou ne possèdent aucun dispositif de chiffrement; et

    b) le matériel classifié ne peut être communiqué en temps voulu par aucun autre moyen.

41. Les informations classifiées transmises dans les conditions visées au paragraphe 39 ne portent aucun marquage ni indication qui les distinguerait d'informations non classifiées ou pouvant être protégées à l'aide d'un produit cryptographique disponible. Leur destinataire est informé, sans délai et par d'autres moyens, du niveau de classification.

42. Lorsque des informations sont transmises en application du paragraphe 39, un rapport est par la suite adressé à ce sujet à l'autorité compétente et au comité de sécurité.

III. AUTORITÉS COMPÉTENTES EN MATIÈRE D'ASSURANCE DE L'INFORMATION

43. Les États membres et le SGC instituent les autorités compétentes en matière d'AI ci-après. Ces autorités ne doivent pas nécessairement être dotées d'entités structurées distinctes. Elles sont investies de mandats distincts. Cependant, ces autorités et leurs responsabilités connexes peuvent être associées ou intégrées dans la même entité structurée ou se partager entre différentes entités structurées, à condition que l'on veille à éviter au niveau interne tout conflit d'intérêt et tout chevauchement des tâches.

Autorité chargée de l'assurance de l'information

44. L'AAI s'acquitte des tâches suivantes:

    a) définir les politiques et les lignes directrices de sécurité en matière d'AI et en surveiller l'efficacité et la pertinence;

    b) conserver et gérer les données techniques relatives aux produits cryptographiques;

    c) veiller à ce que les mesures en matière d'AI sélectionnées aux fins de la protection des ICUE soient conformes aux orientations régissant leur éligibilité et leur sélection;

    d) veiller à ce que les produits cryptographiques soient sélectionnés conformément aux orientations régissant leur éligibilité et leur sélection;

    e) coordonner la formation et la sensibilisation à l'AI;

    f) mener des consultations avec le fournisseur du système, les intervenants en matière de sécurité et les représentants des utilisateurs au sujet des politiques et des lignes directrices de sécurité en matière d'AI; et

    g) veiller à ce que les sous-divisions spécialisées du comité de sécurité disposent, de par leur composition, des compétences requises en matière d'AI.

Autorité TEMPEST

45. L'autorité TEMPEST (AT) est chargée de veiller à la conformité des SIC aux stratégies et lignes directrices TEMPEST. Elle approuve les contre-mesures TEMPEST pour les installations et les produits destinés à protéger des ICUE jusqu'à un certain niveau de classification dans leur environnement opérationnel.

Autorité d'agrément cryptographique

46. L'autorité d'agrément cryptographique (AAC) est chargée de veiller à ce que les produits cryptographiques soient conformes aux politiques respectives des différents États membres et du Conseil en matière cryptographique. Elle agrée les produits cryptographiques pour la protection d'ICUE jusqu'à un certain niveau de classification dans leur environnement opérationnel. S'agissant des États membres, l'AAC est en outre chargée de l'évaluation des produits cryptographiques.

Autorité de distribution cryptographique

47. L'autorité de distribution cryptographique (ADC) s'acquitte des tâches suivantes:

a) gérer le matériel cryptographique de l'Union européenne et en rendre compte;

b) veiller à ce que les procédures et les circuits appropriés soient mis en place pour rendre compte de tout le matériel cryptographique de l'Union européenne et en assurer la manutention, le stockage et la distribution en toute sécurité; et

c) assurer le transfert et la reprise du matériel cryptographique de l'Union européenne auprès des personnes ou des services utilisateurs.

Autorité d'homologation de sécurité

48. L'autorité d'homologation de sécurité de chaque système s'acquitte des tâches suivantes:

a) veiller à ce que les SIC soient conformes aux politiques et lignes directrices de sécurité pertinentes, délivrer une déclaration d'homologation pour les SIC en vue du traitement des ICUE jusqu'à un certain niveau de classification dans leur environnement opérationnel et indiquant les conditions et modalités de l'homologation ainsi que les critères dont l'existence justifie une nouvelle homologation;

b) mettre en place un processus d'homologation de sécurité conforme aux politiques pertinentes et indiquant clairement les conditions d'homologation que doivent remplir les SIC relevant de sa responsabilité;

c) définir une stratégie d'homologation de sécurité qui indique le niveau de précision du processus d'homologation en fonction du niveau d'assurance requis;

d) étudier et approuver les documents se rapportant à la sécurité, y compris en ce qui concerne la gestion des risques et les énoncés des risques résiduels, les énoncés des impératifs de sécurité propres à un système (ci-après dénommés «SSRS»), les documents concernant la vérification de la mise en œuvre des mesures de sécurité et les procédures d'exploitation de sécurité (ci-après dénommées «SecOP»), et veiller à ce qu'ils soient conformes aux politiques et aux règles du Conseil en matière de sécurité;

e) vérifier la mise en œuvre des mesures de sécurité en rapport avec les SIC en effectuant elle-même ou en finançant des évaluations, des inspections ou des réexamens en la matière;

f) définir les exigences en matière de sécurité (par exemple les niveaux d'habilitation de sécurité du personnel) applicables aux postes sensibles dans le cadre d'un SIC;

g) accepter la sélection des produits cryptographiques et TEMPEST ayant fait l'objet d'une approbation qui sont utilisés pour assurer la sécurité d'un SIC;

h) approuver, le cas échéant dans le cadre d'une approbation conjointe, l'interconnexion d'un SIC à d'autres SIC; et

i) mener des consultations avec le fournisseur du système, les intervenants en matière de sécurité et les représentants des utilisateurs au sujet de la gestion des risques de sécurité, et notamment du risque résiduel, et des conditions et modalités de la déclaration d'homologation.

49. L'AHS du SGC est chargée de l'homologation de tous les SIC exploités dans le cadre de la compétence du SGC.

50. L'AHS compétente d'un État membre est chargée de l'homologation des SIC et des éléments des SIC exploités dans le cadre de la compétence d'un État membre.

51. Un comité conjoint d'homologation de sécurité (CHS) est chargé de l'homologation des SIC qui sont du ressort aussi bien de l'AHS du SGC que des AHS des États membres. Ce comité est composé d'un représentant de l'AHS de chaque État membre, un représentant de l'AHS de la Commission assistant à ses réunions. Les autres entités disposant de nœuds de connexion avec un SIC sont invitées à assister aux réunions lorsque celles-ci portent sur le système considéré.

Le CHS est présidé par un représentant de l'AHS du SGC. Il statue par consensus entre les représentants des AHS des institutions, des États membres et des autres entités disposant de nœuds de connexion avec le SIC considéré. Le CHS rend compte à intervalles réguliers de ses activités au comité de sécurité et notifie à celui-ci toute déclaration d'homologation.

Autorité opérationnelle chargée de l'assurance de l'information

52. L'autorité opérationnelle chargée de l'AI pour chaque système s'acquitte des tâches suivantes:

a) élaborer des documents relatifs à la sécurité de chaque système conformes à la politique et aux lignes directrices en matière de sécurité, et notamment les SSRS, y compris en ce qui concerne le risque résiduel, les SecOP et le volet cryptographique du processus d'homologation des SIC;

b) participer à la sélection et à la mise à l'essai des mesures, dispositifs et logiciels de sécurité technique propres à un système, superviser leur mise en œuvre et s'assurer qu'ils sont installés, configurés et entretenus de manière sûre conformément aux documents de sécurité pertinents;

c) participer à la sélection des mesures et des dispositifs de sécurité TEMPEST lorsque les SSRS le prévoient, et veiller à ce qu'ils soient installés et entretenus de manière sûre en coopération avec l'AT;

d) assurer le suivi de la mise en œuvre et de l'application des SecOP et, s'il y a lieu, déléguer les responsabilités opérationnelles de sécurité au détenteur du système;

e) gérer et utiliser les produits cryptographiques, assurer la protection des éléments chiffrés et contrôlés et, au besoin, assurer la production de variables cryptographiques;

f) procéder au réexamen et à des analyses de sécurité et à des tests, notamment afin d'établir les rapports nécessaires sur les risques encourus, comme l'exige l'AHS;

g) dispenser une formation sur l'AI propre à chaque SIC; et

h) mettre en œuvre et gérer des mesures de sécurité propres à chaque SIC.

ANNEXE V

SÉCURITÉ INDUSTRIELLE

I. INTRODUCTION

1. La présente annexe énonce les modalités d'application de l'article 11. Elle prévoit des mesures de sécurité générales applicables aux entités industrielles ou autres dans le cadre de négociations précontractuelles et tout au long du cycle de vie des contrats classifiés attribués par le SGC.

2. Le Conseil approuve des lignes directrices en matière de sécurité industrielle indiquant en particulier les modalités précises en ce qui concerne les HSE, les annexes de sécurité (AS), les visites, la transmission et le transport des ICUE.

II. ASPECTS LIÉS À LA SÉCURITÉ DANS UN CONTRAT CLASSIFIÉ

Guide de la classification de sécurité (GCS)

3. Avant de lancer un appel d'offres en vue de l'attribution d'un contrat classifié ou d'attribuer un tel contrat, le SGC, en sa qualité d'autorité contractante, détermine la classification de sécurité de toute information devant être fournie aux soumissionnaires et aux contractants, ainsi que la classification de sécurité de toute information devant être créée pour le contractant. Dans cette perspective, le SGC élabore un guide de la classification de sécurité (GCS), qui sera utilisé aux fins de l'exécution du contrat.

4. Les principes ci-après sont appliqués pour déterminer le niveau de classification de sécurité des différents éléments d'un contrat classifié:

a) dans le cadre de l'élaboration d'un GCS, le SGC tient compte de tous les aspects pertinents en matière de sécurité, y compris de la classification de sécurité attribuée aux informations fournies et dont l'utilisation aux fins du contrat a été approuvée par l'autorité d'origine desdites informations;

b) le niveau général de classification du contrat ne peut pas être inférieur à la classification la plus élevée de l'un de ses éléments; et

c) le cas échéant, le SGC se met en rapport avec les ANS/ASD ou toute autre autorité de sécurité compétente des États membres dans l'éventualité d'une modification touchant au niveau de classification des informations créées par les contractants ou fournies à ceux-ci dans le cadre de l'exécution d'un contrat et lors de toute modification ultérieure du GCS.

Annexe de sécurité (AS)

5. Les impératifs de sécurité propres à un contrat sont exposés dans une AS. Le cas échéant, l'AS contient le GCS et fait partie intégrante du contrat ou du contrat de sous-traitance classifié.

6. L'AS contient les dispositions imposant au contractant et/ou au sous-traitant de respecter les normes minimales énoncées dans la présente décision. Le non-respect de ces normes minimales peut constituer un motif suffisant de résiliation du contrat.

Instructions de sécurité relatives à un programme/un projet (ISP)

7. En fonction de la portée des programmes ou des projets impliquant l'accès à des ICUE ou leur traitement ou stockage, l'autorité contractante chargée de gérer le projet ou le programme considéré peut élaborer des ISP. Les ISP doivent être approuvées par les ANS/ASD ou toute autre autorité de sécurité compétente des États membres associées aux ISP et peuvent contenir d'autres exigences en matière de sécurité.

III. HABILITATION DE SÉCURITÉ D'ÉTABLISSEMENT (HSE)

8. Une HSE est délivrée par l'ANS/ASD ou toute autre autorité de sécurité compétente d'un État membre afin d'indiquer, conformément aux dispositions législatives et réglementaires nationales, que l'entité industrielle ou autre est en mesure, au sein de ses établissements, de garantir aux ICUE la protection adaptée au niveau de classification approprié (CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET). La HSE est communiquée au SGC, en sa qualité d'autorité contractante, avant que le contractant ou le sous-traitant ou un contractant ou un sous-traitant potentiel ne se voie communiquer des ICUE ou accorder un accès aux ICUE.

9. Lorsqu'elle délivre une HSE, l'ANS/ASD compétente veille au minimum à:

a) évaluer l'intégrité de l'entité industrielle ou autre;

b) évaluer les éléments relatifs à la propriété et au contrôle de l'entité ainsi que toute possibilité d'influence indue pouvant être considérés comme constituant un risque de sécurité;

c) vérifier que l'entité industrielle ou toute autre entité a mis en place un système de sécurité dans ses établissements, qui comporte toutes les mesures de sécurité appropriées pour protéger des informations ou du matériel classifiés CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET conformément aux prescriptions de la présente décision;

d) vérifier que le statut en matière de sécurité des directeurs, des propriétaires et des employés qui doivent avoir accès à du matériel classifié CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET a été établi conformément aux prescriptions de la présente décision; et

e) vérifier que l'entité industrielle ou toute autre entité a nommé un officier de sécurité d'établissement qui est responsable vis-à-vis de sa direction du respect des obligations en matière de sécurité au sein de l'entité.

10. S'il y a lieu, le SGC, en sa qualité d'autorité contractante, avertit l'ANS/ASD ou toute autre autorité de sécurité compétente qu'une HSE est nécessaire dans la phase précontractuelle ou pour l'exécution du contrat. Une HSE ou une HSP est requise dans la phase précontractuelle lorsque des ICUE CONFIDENTIEL UE/EU CONFIDENTAL ou SECRET UE/EU SECRET doivent être fournies dans la phase de soumission des offres.

11. L'autorité contractante n'attribue pas de contrat classifié au soumissionnaire sélectionné tant que l'ANS/ASD ou toute autre autorité de sécurité compétente de l'État membre dans lequel le contractant ou le soumissionnaire concerné est immatriculé, ne lui a pas confirmé qu'une HSE appropriée a été délivrée.

12. L'ANS/ASD ou toute autre autorité de sécurité compétente ayant délivré une HSE notifie au SGC, en sa qualité d'autorité contractante, les modifications éventuellement apportées à ladite HSE. Dans le cadre d'un contrat de sous-traitance, l'ANS/ASD ou toute autre autorité de sécurité compétente en est informée.

13. Le retrait d'une HSE par l'ANS/ASD concernée ou toute autre autorité de sécurité compétente constitue pour le SGC, en sa qualité d'autorité contractante, un motif suffisant pour résilier un contrat classifié ou exclure un soumissionnaire de la procédure d'appel d'offres.

IV. CONTRATS ET CONTRATS DE SOUS-TRAITANCE CLASSIFIÉS

14. Lorsque des ICUE sont communiquées à un soumissionnaire durant la phase précontractuelle, l'appel d'offres contient une disposition prévoyant que le soumissionnaire qui ne présente pas d'offre ou qui n'est pas sélectionné sera tenu de restituer tous les documents classifiés dans un délai spécifié.

15. Une fois qu'un contrat ou un contrat de sous-traitance classifié a été attribué, le SGC, en sa qualité d'autorité contractante, notifie les dispositions en matière de sécurité que comporte le contrat classifié à l'ANS/ASD ou à toute autre autorité de sécurité compétente dont relève le contractant ou le sous-traitant.

16. Lorsqu'il est mis fin à un tel contrat, le SGC, en sa qualité d'autorité contractante, (et/ou l'ANS/ASD ou toute autre autorité de sécurité compétente, selon qu'il conviendra, dans le cas d'un contrat de sous-traitance) avertit immédiatement l'ANS/ASD ou toute autre autorité de sécurité compétente de l'État membre dans lequel le contractant ou le sous-traitant est immatriculé.

17. En principe, le contractant ou le sous-traitant est tenu de restituer à l'autorité contractante les ICUE en sa possession, dès que le contrat ou le contrat de sous-traitance classifié arrive à expiration.

18. Des dispositions spéciales concernant l'élimination d'ICUE durant l'exécution du contrat ou à son expiration figurent dans l'AS.

19. Lorsque le contractant ou le sous-traitant est autorisé à conserver des ICUE après l'expiration d'un contrat, les normes minimales figurant dans la présente demeurent d'application et la confidentialité des ICUE est protégée par le contractant ou le sous-traitant.

20. Les conditions dans lesquelles le contractant peut sous-traiter des activités sont définies dans l'appel d'offres et le contrat.

21. Un contractant doit obtenir l'autorisation du SGC, en sa qualité d'autorité contractante, avant de pouvoir sous-traiter des éléments d'un contrat classifié. Aucun contrat de sous-traitance ne peut être attribué à des entités industrielles ou autres immatriculées dans un État non membre de l'Union européenne n'ayant pas conclu avec l'Union un accord sur la sécurité des informations.

22. Il incombe au contractant de veiller à ce que toutes les activités de sous-traitance soient réalisées en conformité avec les normes minimales définies dans la présente décision et de s'abstenir de fournir des ICUE à un sous-traitant sans l'autorisation écrite préalable de l'autorité contractante.

23. En ce qui concerne les ICUE créées ou traitées par le contractant ou le sous-traitant, les droits qui incombent à l'autorité d'origine sont exercés par l'autorité contractante.

V. VISITES LIÉES À DES CONTRATS CLASSIFIÉS

24. Lorsque le personnel du SGC, des contractants ou des sous-traitants doit avoir accès à des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET dans leurs locaux respectifs aux fins de l'exécution d'un contrat classifié, les visites sont organisées en liaison avec les ANS/ASD ou toute autre autorité de sécurité compétente concernée. Toutefois, dans le cadre de projets spécifiques, les ANS/ASD peuvent également convenir d'une procédure selon laquelle ces visites peuvent être organisées directement.

25. Tous les visiteurs sont en possession d'une HSP adéquate et jouissent d'un accès aux ICUE liées au contrat attribué par le SGC sur la base du principe du besoin d'en connaître.

26. Les visiteurs se voient uniquement accorder l'accès aux ICUE liées à l'objectif de la visite.

VI. TRANSMISSION ET TRANSPORT DES ICUE

27. En ce qui concerne la transmission des ICUE par voie électronique, les dispositions pertinentes de l'article 10 et de l'annexe IV s'appliquent.

28. En ce qui concerne le transport d'ICUE, les dispositions pertinentes de l'annexe III s'appliquent, conformément aux dispositions législatives et réglementaires nationales.

29. En ce qui concerne le transport de matériel classifié en tant que fret, les principes ci-après s'appliquent pour déterminer les mesures de sécurité à mettre en œuvre:

a) la sécurité est assurée à tous les stades pendant le transport, du point d'origine jusqu'à la destination finale;

b) le degré de protection accordé à un envoi est déterminé en fonction du niveau de classification le plus élevé du matériel qu'il contient;

c) une HSE du niveau approprié est obtenue pour les sociétés assurant le transport. En pareil cas, le personnel manipulant l'envoi fait l'objet d'une habilitation de sécurité conformément à l'annexe I;

d) avant tout transfert transfrontalier de matériel classifié CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET, un plan de transport est établi par l'expéditeur et approuvé par les ANS/ASD ou toute autre autorité de sécurité compétente concernées;

e) les trajets sont directs dans la mesure du possible, et aussi rapides que les circonstances le permettent; et

f) chaque fois que cela est possible, les itinéraires ne devraient passer que par des États membres. Les itinéraires passant par des États autres que les États membres ne devraient être suivis qu'à condition d'avoir été autorisés par l'ANS/ASD ou toute autre autorité de sécurité compétente des États de l'expéditeur et du destinataire.

VII. TRANSFERT D'ICUE AUX CONTRACTANTS ÉTABLIS DANS DES ÉTATS TIERS

30. Les ICUE sont transférées aux contractants et sous-traitants établis dans des États tiers conformément aux mesures de sécurité convenues entre le SGC, en sa qualité d'autorité contractante, et l'ANS/ASD de l'État tiers concerné dans lequel le contractant est immatriculé.

VIII. INFORMATIONS CLASSIFIÉES RESTREINT UE/EU RESTRICTED

31. En liaison, s'il y a lieu, avec l'ANS/ASD de l'État membre, le SGC, en sa qualité d'autorité contractante, est habilité à effectuer des inspections dans les établissements des contractants/sous-traitants, en vertu de dispositions contractuelles, afin de vérifier que les mesures de sécurité adaptées pour la protection des ICUE de niveau RESTREINT UE/EU RESTRICTED ont été mises en place, comme l'exige le contrat.

32. Dans la mesure où cela est nécessaire en vertu des dispositions légales et réglementaires nationales, les ANS/ASD, ou toute autre autorité de sécurité compétente, doivent être informées par le SGC, en sa qualité d'autorité contractante, des contrats ou des contrats de sous-traitance contenant des informations classifiées RESTREINT UE/EU RESTRICTED.

33. Les contractants ou sous-traitants et leur personnel ne sont pas tenus d'être en possession d'une HSE ou d'une HSP pour les contrats attribués par le SGC et comportant des informations classifiées RESTREINT UE/EU RESTRICTED.

34. Le SGC, en sa qualité d'autorité contractante, examine les réponses aux appels d'offres portant sur des contrats nécessitant l'accès à des informations classifiées RESTREINT UE/EU RESTRICTED, nonobstant les exigences en matière d'HSE ou d'HSP pouvant être prévues par les dispositions législatives et réglementaires nationales.

35. Les conditions régissant la sous-traitance d'activités par un contractant sont conformes au paragraphe 21.

36. Lorsqu'un contrat prévoit le traitement d'informations classifiées RESTREINT UE/EU RESTRICTED dans un SIC exploité par un contractant, le SGC, en sa qualité d'autorité contractante, veille à ce que les exigences techniques et administratives à remplir concernant l'homologation du SIC soient précisées dans le contrat ou tout contrat de sous-traitance; ces exigences sont proportionnées au risque évalué, compte tenu de tous les facteurs pertinents. La portée de l'homologation dudit SIC est décidée d'un commun accord par l'autorité contractante et l'ANS/ASD compétente.

ANNEXE VI

ÉCHANGE D'INFORMATIONS CLASSIFIÉES AVEC DES ÉTATS TIERS ET DES ORGANISATIONS INTERNATIONALES

I. INTRODUCTION

1. La présente annexe énonce les modalités d'application de l'article 13.

II. CADRES RÉGISSANT L'ÉCHANGE D'INFORMATIONS CLASSIFIÉES

2. Lorsque le Conseil décide qu'il existe un besoin durable d'échanger des informations classifiées,

   — un accord sur la sécurité des informations est conclu, ou

   — un arrangement administratif est conclu,

   conformément à l'article 13, paragraphe 2, et aux sections III et IV et en vertu d'une recommandation du comité de sécurité.

3. Lorsque des ICUE créées aux fins d'une opération PSDC doivent être communiquées à des États tiers ou à des organisations internationales participant à cette opération, et lorsque aucun des cadres prévus au paragraphe 2 n'existe, l'échange d'ICUE avec l'État tiers ou l'organisation internationale contributeur est régi, conformément à la section V ci-dessous, par:

   — un accord-cadre de participation,

   — un accord de participation ad hoc, ou

   — à défaut d'un des accords susmentionnés, un arrangement administratif ad hoc.

4. À défaut d'un des cadres mentionnés aux paragraphes 2 et 3, et lorsque décision est prise de communiquer des ICUE à un État tiers ou à une organisation internationale sur une base exceptionnelle ad hoc dans le respect des dispositions prévues dans la section VI, il est demandé à l'État tiers ou à l'organisation internationale concerné(e) de donner par écrit des assurances garantissant que toute ICUE qui lui est communiquée bénéficie d'une protection conforme aux principes de base et aux normes minimales énoncés dans la présente décision.

III. ACCORDS SUR LA SÉCURITÉ DES INFORMATIONS

5. Les accords sur la sécurité des informations fixent les principes de base et les normes minimales régissant l'échange d'informations classifiées entre l'Union et un État tiers ou une organisation internationale.

6. Les accords sur la sécurité des informations prévoient des modalités techniques d'application qui doivent être arrêtées d'un commun accord entre les autorités de sécurité compétentes des institutions et organes de l'Union concernés et l'autorité de sécurité compétente de l'État tiers ou de l'organisation internationale concerné(e). Ces modalités tiennent compte du niveau de protection offert par les règlements, les structures et les procédures de sécurité en vigueur au sein de l'État tiers ou de l'organisation internationale concerné(e). Elles sont approuvées par le comité de sécurité.

7. Les ICUE ne peuvent faire l'objet d'un échange par voie électronique en application d'un accord sur la sécurité des informations, sauf disposition expresse de l'accord ou des modalités techniques d'application correspondantes.

8. Lorsque le Conseil conclut un accord de sécurité des informations avec un tiers, un bureau d'ordre est désigné au sein de chaque partie comme principal point d'entrée et de sortie des échanges d'informations classifiées.

9. Afin d'évaluer l'efficacité des règlements, structures et procédures de sécurité en vigueur dans l'État tiers ou l'organisation internationale concerné(e), des visites d'évaluation sont menées d'un commun accord avec l'État tiers ou l'organisation internationale concerné(e). Ces visites d'évaluation sont menées conformément aux dispositions pertinentes de l'annexe III et ont pour finalité d'évaluer:

   a) le cadre réglementaire applicable à la protection des informations classifiées;

   b) tous les aspects spécifiques de la politique de sécurité et du mode d'organisation de la sécurité dans l'État tiers ou l'organisation internationale susceptibles d'avoir une incidence sur le niveau des informations classifiées qui peuvent être échangées;

   c) les mesures et les procédures de sécurité effectivement en place; et

   d) les procédures d'habilitation de sécurité pour le niveau de classification des ICUE à communiquer.

10. L'équipe chargée de mener la visite d'évaluation au nom de l'Union détermine si les règles et procédures de sécurité mises en œuvre dans l'État tiers ou l'organisation internationale concerné(e) sont adaptées pour garantir la protection des ICUE au niveau requis.

11. Les conclusions de ces visites sont consignées dans un rapport, sur la base duquel le comité de sécurité fixe le niveau maximal de classification des ICUE qui peuvent être communiquées sur support papier et le cas échéant par voie électronique avec la tierce partie concernée, ainsi que toute condition particulière régissant l'échange d'informations avec celle-ci.

12. Tout est mis en œuvre pour qu'une visite complète d'évaluation de la sécurité soit menée dans l'État tiers ou l'organisation internationale concerné(e) avant l'approbation par le comité de sécurité des modalités d'application, afin d'établir la nature et l'efficacité du système de sécurité en place. Toutefois, lorsque cela n'est pas possible, le bureau de sécurité du SGC remet au comité de sécurité un rapport le plus complet qui soit, fondé sur les informations dont il dispose, qui contient des informations sur le règlement de sécurité applicable et le mode d'organisation de la sécurité dans l'État tiers ou l'organisation internationale concerné(e).

13. Le rapport relatif à la visite d'évaluation ou, en l'absence d'un tel rapport, le rapport visé au paragraphe 12 est transmis au comité de sécurité, qui doit le juger satisfaisant, avant que des ICUE soient effectivement transmises à l'État tiers ou à l'organisation internationale concerné(e).

14. Les autorités de sécurité compétentes des institutions et organes de l'Union notifient à l'État tiers ou à l'organisation internationale la date à compter de laquelle l'Union sera en mesure de communiquer des ICUE en application de l'accord, ainsi que le niveau maximal de classification des ICUE qui peuvent faire l'objet d'un échange sur support papier ou par voie électronique.

15. Des visites de suivi de l'évaluation sont effectuées au besoin, en particulier dans les circonstances suivantes:

a) il est nécessaire de relever le niveau de classification des ICUE pouvant être communiquées;

b) il a été porté à la connaissance de l'Union que les modalités de sécurité de l'État tiers ou de l'organisation internationale ont fait l'objet de modifications fondamentales susceptibles d'avoir un effet sur la manière dont elle protège les ICUE; ou

c) il y a eu un incident grave impliquant la divulgation non autorisée d'ICUE.

16. Lorsque l'accord sur la sécurité des informations est en vigueur et que des informations classifiées sont échangées avec l'État tiers ou l'organisation internationale concerné(e), le comité de sécurité peut décider de modifier le niveau maximal de classification des ICUE pouvant être échangées au format papier ou par voie électronique, en particulier à la lumière de toute visite de suivi de l'évaluation.

IV. ARRANGEMENTS ADMINISTRATIFS

17. Lorsqu'il existe un besoin durable d'échanger, avec un État tiers ou une organisation internationale, des informations dont le niveau de classification n'est en principe pas supérieur à RESTREINT UE/EU RESTRICTED, et que le comité de sécurité a établi que la partie en question ne dispose pas d'un système de sécurité suffisamment développé lui permettant de conclure un accord sur la sécurité des informations, le secrétaire général peut, sous réserve de l'approbation du Conseil, conclure un arrangement administratif au nom du SGC avec les autorités compétentes de l'État tiers ou de l'organisation internationale concerné(e).

18. Si, pour des raisons opérationnelles urgentes, un cadre doit être mis en place rapidement pour échanger des informations classifiées, le Conseil peut décider exceptionnellement qu'un arrangement administratif soit conclu pour échanger des informations dont le niveau de classification est supérieur à RESTREINT UE/EU RESTRICTED.

19. Les arrangements administratifs prennent, en règle générale, la forme d'un échange de lettres.

20. Une visite d'évaluation telle que visée au paragraphe 9 est réalisée, et le rapport y relatif ou, en l'absence d'un tel rapport, le rapport visé au paragraphe 12 est transmis au comité de sécurité, qui doit le juger satisfaisant, avant que des ICUE soient effectivement transmises à l'État tiers ou à l'organisation internationale concerné(e).

21. Les ICUE ne peuvent faire l'objet d'aucun échange par voie électronique en application d'un arrangement administratif, sauf disposition expresse de l'arrangement.

V. ÉCHANGE D'INFORMATIONS CLASSIFIÉES DANS LE CADRE D'OPÉRATIONS PSDC

22. Les accords-cadres de participation régissent la participation des États tiers ou des organisations internationales aux opérations PSDC. Ces accords contiennent des dispositions relatives à la communication des ICUE créées aux fins des opérations PSDC aux États tiers ou aux organisations internationales contributeurs. Le niveau maximal de classification des ICUE qui peuvent être échangées est RESTREINT UE/EU RESTRICTED pour les opérations PSDC civiles et CONFIDENTIEL UE/EU CONFIDENTIAL pour les opérations PSDC militaires, sauf disposition contraire prévue dans la décision établissant chaque opération PSDC.

23. Les accords de participation ad hoc conclus pour une opération PSDC particulière comprennent des dispositions relatives à la communication des ICUE créées aux fins de ladite opération à l'État tiers ou à l'organisation internationale y participant. Le niveau maximal de classification des ICUE qui peuvent être échangées est RESTREINT UE/EU RESTRICTED pour les opérations PSDC civiles et CONFIDENTIEL UE/EU CONFIDENTIAL pour les opérations PSDC militaires, sauf disposition contraire prévue dans la décision établissant chaque opération PSDC.

24. En l'absence d'accord sur la sécurité des informations et dans l'attente de la conclusion d'un accord de participation, la communication des ICUE créées aux fins de l'opération à un État tiers ou à une organisation internationale participant à l'opération est régie par un arrangement administratif que doit conclure le haut représentant ou fait l'objet d'une décision sur leur communication ad hoc, conformément aux dispositions de la section VI. Les ICUE ne seront échangées en application de cet arrangement qu'aussi longtemps que la participation de l'État tiers ou de l'organisation internationale sera envisagée. Le niveau maximal de classification des ICUE qui peuvent être échangées est RESTREINT UE/EU RESTRICTED pour les opérations PSDC civiles et CONFIDENTIEL UE/EU CONFIDENTIAL pour les opérations PSDC militaires, sauf disposition contraire prévue dans la décision établissant chaque opération PSDC.

25. Les dispositions relatives aux informations classifiées devant figurer dans les accords-cadres de participation, les accords de participation ad hoc et les arrangements administratifs ad hoc visés aux paragraphes 22 à 24 prévoient que l'État tiers ou l'organisation internationale concerné(e) veille à ce que son personnel détaché dans le cadre de toute opération protège les ICUE conformément au règlement de sécurité du Conseil, ainsi qu'aux autres instructions formulées par les autorités compétentes, y compris la chaîne de commandement de l'opération.

26. Si un accord sur la sécurité des informations est conclu ultérieurement entre l'Union et un État tiers ou une organisation internationale contributeur, l'accord sur la sécurité des informations se substitue aux dispositions relatives à l'échange d'informations classifiées énoncées dans tout accord-cadre de participation, accord de participation ad hoc ou arrangement administratif ad hoc pour ce qui concerne l'échange et le traitement des ICUE.

27. Aucun échange d'ICUE par voie électronique n'est autorisé au titre d'un accord-cadre de participation, d'un accord de participation ad hoc ou d'un arrangement administratif ad hoc conclu avec un État tiers ou une organisation internationale, sauf disposition expresse de l'accord ou l'arrangement en question.

28. Les ICUE créées aux fins d'une opération PSDC peuvent être divulguées au personnel détaché par des États tiers ou des organisations internationales dans le cadre de cette opération, conformément aux dispositions des paragraphes 22 à 27. Lorsque l'accès aux ICUE est autorisé dans les locaux ou via le SIC d'une opération PSDC, il convient d'appliquer des mesures (y compris l'enregistrement des ICUE divulguées) permettant d'atténuer le risque de perte ou de compromission. Ces mesures sont définies dans les documents de planification ou de mission pertinents.

29. En l'absence d'accord sur la sécurité des informations, la communication d'ICUE, en cas de besoin opérationnel spécifique et immédiat, à l'État hôte sur le territoire duquel une opération PSDC est menée peut être régie par un arrangement administratif que doit conclure le haut représentant. Cette possibilité est prévue dans la décision établissant l'opération PSDC. Seules peuvent être communiquées dans de telles circonstances les ICUE créées aux fins de l'opération PSDC dont le niveau de classification n'est pas supérieur à RESTREINT UE/EU RESTRICTED, sauf si un niveau de classification supérieur est prévu dans la décision établissant l'opération PSDC. Dans le cadre d'un tel arrangement administratif, l'État hôte est tenu de s'engager à protéger les ICUE conformément à des normes minimales qui ne sont pas moins strictes que celles prévues dans la présente décision.

30. En l'absence d'accord sur la sécurité des informations, la communication d'ICUE aux États tiers concernés et aux organisations internationales concernées, autres que ceux et celles qui participent à une opération PSDC, peut être régie par un arrangement administratif que doit conclure le haut représentant. Le cas échéant, cette possibilité, ainsi que toutes les conditions qui lui sont liées, est prévue dans la décision établissant l'opération PSDC. Seules peuvent être communiquées dans de telles circonstances les ICUE créées aux fins de l'opération PSDC dont le niveau de classification n'est pas supérieur à RESTREINT UE/EU RESTRICTED, sauf si un niveau de classification supérieur est prévu dans la décision établissant l'opération PSDC. Dans le cadre d'un tel arrangement administratif, l'État tiers ou l'organisation internationale en question est tenu(e) de s'engager à protéger les ICUE conformément à des normes minimales qui ne sont pas moins strictes que celles prévues dans la présente décision.

31. Aucune modalité d'application ou visite d'évaluation n'est requise préalablement à la mise en œuvre des dispositions relatives à la communication d'ICUE au titre des paragraphes 22, 23 et 24.

VI. COMMUNICATION AD HOC EXCEPTIONNELLE D'ICUE

32. Si aucun cadre n'existe conformément aux sections III à V, et si le Conseil ou l'une de ses instances préparatoires décide qu'il est nécessaire, à titre exceptionnel, de communiquer des ICUE à un État tiers ou à une organisation internationale, le SGC:

a) vérifie, dans la mesure du possible, auprès des autorités de sécurité de l'État tiers ou de l'organisation internationale concerné(e) que son règlement, ses structures et ses procédures de sécurité permettent de garantir que les ICUE qui lui seront communiquées bénéficieront d'une protection conforme à des normes qui ne sont pas moins strictes que celles prévues dans la présente décision; et

b) invite le comité de sécurité à formuler, sur la base des informations disponibles, une recommandation concernant la confiance qui peut être accordée au règlement, aux structures et aux procédures de sécurité en vigueur dans l'État tiers ou l'organisation internationale auquel les ICUE doivent être communiquées.

33. Si le comité de sécurité émet une recommandation favorable à la communication des ICUE, la question est soumise au Comité des représentants permanents (Coreper), qui statue sur leur communication.

34. Si le comité de sécurité émet une recommandation défavorable quant à la communication des ICUE:

a) pour les questions relatives à la PESC/PSDC, le comité politique et de sécurité débat de la question et formule une recommandation en vue d'une décision du Coreper;

b) pour toutes les autres questions, le Coreper examine la question et prend une décision.

35. Lorsque cela est jugé nécessaire, et sous réserve du consentement préalable écrit de l'autorité d'origine, le Coreper peut décider que les informations classifiées ne peuvent être communiquées qu'en partie ou qu'après avoir été déclassées ou déclassifiées, ou que les informations à communiquer seront préparées sans indiquer de référence à l'origine ou au niveau initial de classification de l'Union européenne.

36. Lorsqu'une décision de communiquer des ICUE a été prise, le SGC transmet le document concerné, qui porte un marquage relatif à la communicabilité indiquant l'État tiers ou l'organisation internationale auquel ce document a été communiqué. Avant la communication effective ou au moment de celle-ci, la tierce partie concernée s'engage par écrit à protéger les ICUE qui lui sont transmises conformément aux principes de base et aux normes minimales prévus dans la présente décision.

VII. AUTORISATION DE COMMUNIQUER DES ICUE À DES ÉTATS TIERS OU À DES ORGANISATIONS INTERNATIONALES

37. Lorsqu'il existe, conformément au paragraphe 2, un cadre pour l'échange d'informations classifiées avec un État tiers ou une organisation internationale, le Conseil prend la décision d'autoriser le secrétaire général à communiquer des ICUE à l'État tiers ou à l'organisation internationale concerné(e), dans le respect du principe du consentement de l'autorité d'origine. Le secrétaire général peut déléguer ce pouvoir à de hauts fonctionnaires du SGC.

38. Lorsqu'il existe, conformément au paragraphe 2, premier tiret, un accord sur la sécurité des informations, le Conseil peut prendre la décision d'autoriser le haut représentant à communiquer à l'État tiers ou à l'organisation internationale en question des ICUE provenant du Conseil dans le domaine de la Politique de sécurité et de défense commune, après avoir obtenu le consentement de l'autorité d'origine de chacune des sources que ces ICUE contiennent. Le haut représentant peut déléguer ce pouvoir à de hauts fonctionnaires du SEAE ou à des RSUE.

39. Lorsqu'il existe, conformément au paragraphe 2 ou 3, un cadre pour l'échange d'informations classifiées avec un État tiers ou une organisation internationale, le haut représentant est autorisé à communiquer des ICUE, conformément à la décision établissant l'opération PSDC et au principe du consentement de l'autorité d'origine. Le haut représentant peut déléguer ce pouvoir à de hauts fonctionnaires du SEAE, à une opération de l'Union, à des commandants de force ou de mission, ou à des chefs de mission de l'Union.

Appendices

Appendice A

Définitions

Appendice B

Équivalence des classifications de sécurité

Appendice C

Liste des autorités nationales de sécurité (ANS)

Appendice D

Liste des abréviations

Appendice A

DÉFINITIONS

Aux fins de la présente décision, on entend par:

«annexe de sécurité (AS)», un ensemble de conditions contractuelles spéciales, établi par l'autorité contractante, qui fait partie intégrante de tout contrat classifié impliquant l'accès à des ICUE ou la création de telles informations, dans lequel sont définis les conditions de sécurité ou les éléments du contrat qui doivent être protégés pour des raisons de sécurité;

«assurance de l'information», voir l'article 10, paragraphe 1;

«autorisation d'accès aux ICUE», une décision de l'AIPN du SGC prise en fonction d'une assurance donnée par une autorité compétente d'un État membre attestant qu'un fonctionnaire ou un autre agent du SGC ou un expert national détaché auprès du SGC peut, pour autant que son besoin d'en connaître ait été établi et qu'il ait été correctement informé des responsabilités qui lui incombent en la matière, être autorisé à avoir accès aux ICUE jusqu'à un niveau de classification donné (CONFIDENTIEL UE/EU CONFIDENTIAL ou supérieur) jusqu'à une date donnée;

«autorité d'origine», l'institution, l'organe ou l'agence de l'Union, l'État membre, l'État tiers ou l'organisation internationale sous l'autorité duquel/de laquelle les informations classifiées ont été créées et/ou introduites dans les structures de l'Union;

«autorité de sécurité désignée (ASD)», l'autorité responsable devant l'autorité nationale de sécurité (ANS) d'un État membre qui est chargée de communiquer à des entités industrielles ou autres la politique nationale dans tous les domaines relevant de la sécurité industrielle et de fournir des orientations et une aide pour sa mise en œuvre. Les fonctions de l'ASD peuvent être exercées par l'ANS ou par toute autre autorité compétente;

«certificat d'habilitation de sécurité du personnel (CHSP)», un certificat délivré par une autorité compétente attestant qu'une personne a obtenu une habilitation de sécurité et détient un certificat d'habilitation de sécurité valable ou une autorisation de l'AIPN permettant l'accès à des ICUE, et indiquant le niveau de classification des ICUE auxquelles la personne peut être autorisée à avoir accès (CONFIDENTIEL UE/EU CONFIDENTIAL ou supérieur), la durée de validité de l'HSP correspondante et la date d'expiration du certificat;

«contractant», une personne physique ou morale dotée de la capacité juridique de conclure des contrats;

«contrat classifié», un contrat conclu par le SGC avec un contractant en vue de la fourniture de biens, de la réalisation de travaux ou de la prestation de services, dont l'exécution requiert ou implique l'accès à des ICUE ou la création de telles informations;

«contrat de sous-traitance classifié», un contrat conclu par un contractant du SGC avec un autre contractant (c'est-à-dire le sous-traitant) en vue de la fourniture de biens, de la réalisation de travaux ou de la prestation de services, dont l'exécution requiert ou implique l'accès à des ICUE ou la création de telles informations;

«cycle de vie d'un SIC», la durée totale d'existence d'un SIC, laquelle comprend le lancement, la conception, la planification, l'analyse des besoins, l'élaboration, le développement, la mise à l'essai, la mise en œuvre, l'exploitation, la maintenance et le démantèlement;

«déclassement», le passage à un niveau de classification de sécurité inférieur;

«déclassification», la suppression de toute classification de sécurité;

«défense en profondeur», l'application d'un éventail de mesures de sécurité organisées en plusieurs niveaux de défense;

«détenteur», une personne dûment autorisée qui, sur la base d'un besoin d'en connaître avéré, est en possession d'un élément d'ICUE et à laquelle il incombe par conséquent d'en assurer la protection;

«document», toute information enregistrée quelles que soient sa forme ou ses caractéristiques physiques;

«enquête de sécurité», les procédures d'enquête menées par l'autorité compétente d'un État membre, dans le respect de ses dispositions législatives et réglementaires nationales, en vue d'obtenir l'assurance qu'il n'existe pas de renseignements défavorables de nature à empêcher une personne d'obtenir une HSP ou une autorisation lui permettant d'avoir accès à des ICUE jusqu'à un niveau déterminé (CONFIDENTIEL UE/EU CONFIDENTIAL ou supérieur);

«enregistrement», voir annexe III, paragraphe 18;

«entité industrielle ou autre», une entité s'occupant de la fourniture de biens, de la réalisation de travaux ou de la prestation de services; il peut s'agir d'une entité industrielle, commerciale ou scientifique, ou d'une entité de service, de recherche, d'enseignement ou de développement ou d'une personne exerçant une activité indépendante;

«gestion des informations classifiées», voir article 9, paragraphe 1;

«guide de la classification de sécurité (GCS)», un document qui décrit les éléments d'un programme ou d'un contrat qui sont classifiés, et précise les niveaux de classification de sécurité applicables. Le GCS peut être étoffé tout au long de la durée du programme ou du contrat et les éléments d'information peuvent être reclassifiés ou déclassés; lorsqu'il existe, le GCS fait partie de l'AS;

«habilitation de sécurité d'établissement (HSE)», une décision administrative prise par une ANS ou une ASD selon laquelle, du point de vue de la sécurité, un établissement peut assurer un niveau suffisant de protection pour les ICUE d'un niveau de classification de sécurité déterminé;

«habilitation de sécurité du personnel (HSP)», une déclaration émanant d'une autorité compétente d'un État membre établie à la suite d'une enquête de sécurité menée par les autorités compétentes d'un État membre et attestant qu'une personne peut être autorisée à avoir accès aux ICUE jusqu'à un niveau de classification donné (CONFIDENTIEL UE/EU CONFIDENTIAL ou supérieur) jusqu'à une date donnée;

«homologation», la procédure conduisant à une déclaration formelle de l'autorité d'homologation de sécurité (AHS) indiquant qu'un système est agréé pour fonctionner à un niveau de classification déterminé, selon un mode d'exploitation de sécurité spécifique dans son environnement opérationnel et à un niveau de risque acceptable, pour autant qu'un ensemble approuvé de mesures de sécurité ait été mis en place sur le plan technique et physique, ainsi qu'au niveau de l'organisation et des procédures;

«informations classifiées de l'Union européenne» (ICUE), voir article 2, paragraphe 1;

«instructions de sécurité relatives à un programme/un projet (ISP)», une liste des procédures de sécurité appliquées à un programme ou à un projet spécifique en vue d'uniformiser ces procédures. Elles peuvent être revues tout au long de la durée du programme ou du projet;

«interconnexion», voir annexe IV, paragraphe 32;

«matériel», tout document, support de données ou élément de machine ou d'équipement, déjà fabriqué ou en cours de fabrication;

«matériel cryptographique», les algorithmes cryptographiques, les modules matériels et logiciels cryptographiques, et les produits comprenant les modalités de mise en œuvre et la documentation y relative, ainsi que les éléments de mise à la clé;

«menace», la cause potentielle d'un incident non souhaité susceptible de porter atteinte à une organisation ou à tout système qu'elle utilise. Les menaces peuvent être accidentelles ou délibérées (malveillantes); elles sont caractérisées par des éléments menaçants, des cibles potentielles et des méthodes d'attaque;

«mesures de sécurité concernant le personnel», voir article 7, paragraphe 1;

«mode d'exploitation de sécurité», la définition des conditions d'exploitation d'un SIC, compte tenu de la classification des informations traitées et des niveaux d'habilitation, des autorisations formelles d'accès et du besoin d'en connaître de ses utilisateurs. Il existe quatre modes d'exploitation pour le traitement ou la transmission d'informations classifiées: le mode exclusif, le mode dominant, le mode par cloisonnement et le mode multiniveau; on entend par:

— «mode exclusif», un mode d'exploitation selon lequel toutes les personnes ayant accès au SIC sont habilitées au plus haut niveau de classification des informations traitées au sein du SIC, et ont un besoin commun d'en connaître pour toutes les informations traitées au sein du SIC,

— «mode dominant», un mode d'exploitation dans lequel toutes les personnes ayant accès au SIC sont habilitées au plus haut niveau de classification des informations au sein du SIC, mais n'ont pas toutes un besoin commun d'en connaître pour les informations traitées au sein du SIC; une personne seule peut autoriser l'accès à l'information,

— «mode par cloisonnement», un mode d'exploitation dans lequel toutes les personnes ayant accès au SIC sont habilitées au plus haut niveau de classification des informations traitées au sein du SIC, mais ne bénéficient pas toutes d'une autorisation formelle d'accéder à toutes les informations traitées au sein du SIC; une telle autorisation formelle suppose que le contrôle d'accès fasse l'objet d'une gestion centrale formelle par opposition au pouvoir détenu par une personne seule d'accorder l'accès,

— «mode multiniveau», un mode d'exploitation dans lequel les personnes ayant accès au SIC ne sont pas toutes habilitées au plus haut niveau de classification des informations traitées au sein du SIC, et n'ont pas toutes un besoin commun d'en connaître pour les informations traitées au sein du SIC;

«opération PSDC», une opération militaire ou civile de gestion de crise mise en place en vertu du titre V, chapitre 2, du traité sur l'Union européenne;

«procédure de gestion des risques de sécurité», l'ensemble de la procédure consistant à identifier, contrôler et limiter les événements aléatoires susceptibles d'avoir des répercussions sur la sécurité d'une organisation ou de tout système qu'elle utilise. La procédure couvre l'ensemble des activités liées aux risques, y compris l'évaluation, le traitement, l'acceptation et la communication;

«produit cryptographique», un produit dont la fonction première et principale est la fourniture de services de sécurité (confidentialité, intégrité, disponibilité, authenticité, non-répudiation) par l'intermédiaire d'un ou de plusieurs mécanismes cryptographiques;

«ressource», tout ce qui présente de l'utilité pour une organisation, ses activités et la continuité de celles-ci, y compris les ressources en matière d'information dont l'organisation a besoin pour s'acquitter de sa mission;

«risque», la possibilité qu'une menace donnée se concrétise en tirant parti des vulnérabilités internes et externes d'une organisation ou d'un des systèmes qu'elle utilise et cause ainsi un préjudice à l'organisation ou à ses ressources matérielles ou immatérielles. Il se mesure en tenant compte à la fois de la probabilité de voir se concrétiser des menaces et de l'impact de celles-ci.

— L'«acceptation des risques» consiste à décider d'accepter qu'un risque résiduel subsiste au terme du traitement des risques.

— L'«évaluation des risques» consiste à déterminer les menaces et les vulnérabilités et à procéder à l'analyse des risques correspondants, c'est-à-dire à examiner leur probabilité et leur impact.

— La «communication des risques» consiste à sensibiliser la communauté des utilisateurs du SIC aux risques, à informer les autorités d'homologation de ces risques et à faire rapport à leur sujet aux autorités responsables de l'exploitation.

— Le «traitement des risques» consiste à atténuer, à éliminer, à réduire (par un ensemble approprié de mesures sur le plan technique, physique ou au niveau de l'organisation ou des procédures), à transférer ou à surveiller les risques;

«risque résiduel», le risque qui subsiste après que des mesures de sécurité ont été mises en œuvre, étant entendu qu'il est impossible de contrer toutes les menaces et d'éliminer toutes les vulnérabilités;

«sécurité industrielle», voir article 11, paragraphe 1;

«sécurité physique», voir article 8, paragraphe 1;

«système d'information et de communication (SIC)», voir article 10, paragraphe 2;

«TEMPEST», l'analyse, l'étude et le contrôle des émissions électromagnétiques susceptibles de compromettre les informations, ainsi que les mesures destinées à les éliminer;

«traitement» d'ICUE, l'ensemble des actions dont les ICUE sont susceptibles de faire l'objet tout au long de leur cycle de vie. Sont ainsi visés leur création, leur traitement, leur transport, leur déclassement, leur déclassification et leur destruction. En ce qui concerne les SIC, sont en outre compris leur collecte, leur affichage, leur transmission et leur stockage;

«vulnérabilité», toute faiblesse de quelque nature que ce soit dont une ou plusieurs menaces est susceptible de tirer parti pour se concrétiser. La vulnérabilité peut résulter d'une omission ou être liée à un contrôle défaillant en termes de rigueur, d'exhaustivité ou d'homogénéité; elle peut être de nature technique, procédurale, physique, organisationnelle ou opérationnelle.

Appendice B

ÉQUIVALENCE DES CLASSIFICATIONS DE SÉCURITÉ

UE	TRÈS SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Belgique	Très Secret (Loi 11.12.1998) Zeer Geheim (Wet 11.12.1998)	Secret (Loi 11.12.1998) Geheim (Wet 11.12.1998)	Confidentiel (Loi 11.12.1998) Vertrouwelijk (Wet 11.12.1998)	Note (1) ci-dessous
Bulgarie	Строго секретно	Секретно	Поверително	За служебно ползване
République tchèque	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Danemark	YDERST HEMMELIGT	HEMMELIGT	FORTROLIGT	TIL TJENESTEBRUG
Allemagne	STRENG GEHEIM	GEHEIM	VS (2) — VERTRAULICH	VS — NUR FÜR DEN DIENSTGEBRAUCH
Estonie	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Irlande	Top Secret	Secret	Confidential	Restricted
Grèce	Άκρως Απόρρητο Abr: ΑΑΠ	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Espagne	SECRETO	RESERVADO	CONFIDENCIAL	DIFUSIÓN LIMITADA
France	Très Secret Défense	Secret Défense	Confidentiel Défense	note (3) ci-dessous
Croatie	VRLO TAJNO	TAJNO	POVJERLJIVO	OGRANIČENO
Italie	Segretissimo	Segreto	Riservatissimo	Riservato
Chypre	Άκρως Απόρρητο Abr: (ΑΑΠ)	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Lettonie	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Lituanie	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Luxembourg	Très Secret Lux	Secret Lux	Confidentiel Lux	Restreint Lux
Hongrie	Szigorúan titkos!	Titkos!	Bizalmas!	Korlátozott terjesztésű!
Malte	L-Ogħla Segretezza Top Secret	Sigriet Secret	Kunfidenzjali Confidential	Ristrett Restricted (4)
Pays-Bas	Stg. ZEER GEHEIM	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep. VERTROUWELIJK
Autriche	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Pologne	Ściśle Tajne	Tajne	Poufne	Zastrzeżone
Portugal	Muito Secreto	Secreto	Confidencial	Reservado

UE	TRÈS SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Roumanie	Strict secret de importanță deosebită	Strict secret	Secret	Secret de serviciu
Slovénie	STROGO TAJNO	TAJNO	ZAUPNO	INTERNO
Slovaquie	Prísne tajné	Tajné	Dôverné	Vyhradené
Finlande	ERITTÄIN SALAINEN YTTERST HEMLIG	SALAINEN HEMLIG	LUOTTAMUKSELLINEN KONFIDENTIELL	KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG
Suède ([5])	HEMLIG/TOP SECRET HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET	HEMLIG/SECRET HEMLIG	HEMLIG/CONFIDENTIAL HEMLIG	HEMLIG/RESTRICTED HEMLIG
Royaume-Uni	UK TOP SECRET	UK SECRET	UK CONFIDENTIAL	UK RESTRICTED

([1]) La classification «Diffusion restreinte/Beperkte Verspreiding» n'est pas une classification de sécurité en Belgique. La Belgique traite et protège les informations RESTREINT UE/EU RESTRICTED d'une manière qui n'est pas moins stricte que les normes et procédures décrites dans le règlement de sécurité du Conseil de l'Union européenne.

([2]) Allemagne: VS = Verschlusssache.

([3]) La France n'utilise pas la catégorie de classification «RESTREINT» dans son système national. Elle traite et protège les informations RESTREINT UE/EU RESTRICTED d'une manière qui n'est pas moins stricte que les normes et procédures décrites dans le règlement de sécurité du Conseil de l'Union européenne.

([4]) Les marquages de classification de sécurité en maltais et en anglais utilisés par Malte peuvent l'être indifféremment.

([5]) Suède: les marquages de classification de sécurité de la première ligne sont utilisés par les autorités chargées de la défense et les marquages de la deuxième ligne par les autres autorités.

Appendice C

LISTE DES AUTORITÉS NATIONALES DE SÉCURITÉ (ANS)

BELGIQUE
Autorité nationale de Sécurité
SPF affaires étrangères, commerce extérieur et coopération au développement
15, rue des Petits Carmes
1000 Bruxelles

Téléphone secrétariat: +32 25014542
Télécopieur: +32 25014596
Adresse électronique: nvo-ans@diplobel.fed.be

BULGARIE
State Commission on Information Security
90 Cherkovna Str.
1505 Sofia

Téléphone: +359 29333600
Télécopieur: +359 29873750
Adresse électronique: dksi@government.bg
Site web: www.dksi.bg

RÉPUBLIQUE TCHÈQUE
Národní bezpečnostní úřad
(National Security Authority)
Na Popelce 2/16
150 06 Praha 56

Téléphone: +420 257283335
Télécopieur: +420 257283110
Adresse électronique: czech.nsa@nbu.cz
Site web: www.nbu.cz

DANEMARK
Politiets Efterretningstjeneste
(Danish Security Intelligence Service)
Klausdalsbrovej 1
2860 Søborg

Téléphone: +45 33148888
Télécopieur: +45 33430190

Forsvarets Efterretningstjeneste
(Danish Defence Intelligence Service)
Kastellet 30
2100 Copenhagen Ø

Téléphone: +45 33325566
Télécopieur: +45 33931320

ALLEMAGNE
Bundesministerium des Innern
Referat ÖS III 3
Alt-Moabit 101 D
D-11014 Berlin

Téléphone: +49 30186810
Télécopieur: +49 30186811441
Adresse électronique: oesIII3@bmi.bund.de

ESTONIE
National Security Authority Department
Estonian Ministry of Defence
Sakala 1
15094 Tallinn

Téléphone: +372 7170019, +372 7170117
Télécopieur: +372 7170213
Adresse électronique: nsa@mod.gov.ee

IRLANDE
National Security Authority
Department of Foreign Affairs
76 - 78 Harcourt Street
Dublin 2

Téléphone: +353 14780822
Télécopieur: +353 14082959

GRÈCE
Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ)
Διεύθυνση Ασφαλείας και Αντιπληροφοριών
ΣΤΓ 1020 -Χολαργός (Αθήνα)
Ελλάδα

Τηλ.: +30 2106572045 (ώρες γραφείου)
+30 2106572009 (ώρες γραφείου)
Φαξ: +30 2106536279
+30 2106577612

Hellenic National Defence General Staff (HNDGS)
Counter Intelligence and Security Directorate (NSA)
227-231 HOLARGOS
STG 1020 ATHÈNES

Téléphone: +30 2106572045
+30 2106572009
Télécopieur: +30 2106536279
+30 2106577612

ESPAGNE
Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Avenida Padre Huidobro s/n
28023 Madrid

Téléphone: +34 913725000
Télécopieur: +34 913725808
Adresse électronique: nsa-sp@areatec.com

FRANCE
Secrétariat général de la défense et de la sécurité nationale
Sous-direction «Protection du secret» (SGDSN/PSD)
51, boulevard de la Tour-Maubourg
75700 Paris 07 SP

Téléphone: +33 171758177
Télécopieur: +33 171758200

CROATIE
Office of the National Security Council
Croatian NSA
Jurjevska 34
10000 Zagreb
Croatie

Téléphone: +385 14681222
Télécopieur: +385 14686049
www.uvns.hr

ITALIE
Presidenza del Consiglio dei Ministri
D.I.S. - U.C.Se.
Via di Santa Susanna, 15
00187 Roma

Téléphone: +39 0661174266
Télécopieur: +39 064885273

CHYPRE
ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ
ΣΤΡΑΤΙΩΤΙΚΟ ΕΠΙΤΕΛΕΙΟ ΤΟΥ ΥΠΟΥΡΓΟΥ
Εθνική Αρχή Ασφάλειας (ΕΑΑ)
Υπουργείο Άμυνας
Λεωφόρος Εμμανουήλ Ροΐδη 4
1432 Λευκωσία, Κύπρος

Τηλέφωνα: +357 22807569, +357 22807643,
+357 22807764
Τηλεομοιότυπο: +357 22302351

Ministry of Defence
Minister's Military Staff
National Security Authority (NSA)
4 Emanuel Roidi street
1432 Nicosia

Téléphone: +357 22807569, +357 22807643,
+357 22807764
Télécopieur: +357 22302351
Adresse électronique: cynsa@mod.gov.cy

LETTONIE
National Security Authority
Constitution Protection Bureau of the Republic of Latvia
P.O. Box 286
LV-1001 Riga

Téléphone: +371 67025418
Télécopieur: +371 67025454
Adresse électronique: ndi@sab.gov.lv

LITUANIE
Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija
(The Commission for Secrets Protection Coordination of the Republic of Lituania
National Security Authority)
Gedimino 40/1
LT-01110 Vilnius

Téléphone: +370 706 66701, +370 706 66702
Télécopieur: +370 706 66700
Adresse électronique: nsa@vsd.lt

LUXEMBOURG
Autorité nationale de sécurité
Boîte postale 2379
1023 Luxembourg

Téléphone: +352 24782210 central
+352 24782253 direct
Télécopieur: +352 24782243

HONGRIE
Nemzeti Biztonsági Felügyelet
(National Security Authority of Hungary)
H-1024 Budapest, Szilágyi Erzsébet fasor 11/B

Téléphone: +36 (1) 7952303
Télécopieur: +36 (1) 7950344
Adresse postale:
H-1357 Budapest, PO Box 2
Adresse électronique: nbf@nbf.hu
Site web: www.nbf.hu

MALTE
Ministry for Home Affairs and National Security
P.O. Box 146
MT-Valletta

Téléphone: +356 21249844
Télécopieur: +356 25695321

PAYS-BAS
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Postbus 20010
2500 EA Den Haag

Téléphone: +31 703204400
Télécopieur: +31 703200733

Ministerie van Defensie
Beveiligingsautoriteit
Postbus 20701
2500 ES Den Haag

Téléphone: +31 703187060
Télécopieur: +31 703187522

AUTRICHE
Informationssicherheitskommission
Bundeskanzleramt
Ballhausplatz 2
1014 Wien

Téléphone: +43 1531152594
Télécopieur: +43 1531152615
Adresse électronique: ISK@bka.gv.at

POLOGNE Agencja Bezpieczeństwa Wewnętrznego – ABW (Internal Security Agency) 2A Rakowiecka St. 00-993 Warszawa Téléphone: +48 225857360 Télécopieur: +48 225858509 Adresse électronique: nsa@abw.gov.pl Site web: www.abw.gov.pl	**SLOVAQUIE** Národný bezpečnostný úrad (National Security Authority) Budatínska 30 P.O. Box 16 850 07 Bratislava Téléphone: +421 268692314 Télécopieur: +421 263824005 Site web: www.nbusr.sk
PORTUGAL Presidência do Conselho de Ministros Autoridade Nacional de Segurança Rua da Junqueira, 69 1300-342 Lisboa Téléphone: +351 213031710 Télécopieur: +351 213031711	**FINLANDE** National Security Authority Ministry for Foreign Affairs P.O. Box 453 FI-00023 Government Téléphone 1: +358 16055890 Télécopieur: +358 916055140 Adresse électronique: NSA@formin.fi
ROUMANIE Oficiul Registrului Național al Informațiilor Secrete de Stat (Romanian NSA – ORNISS National Registry Office for Classified Information) Strada Mureș nr. 4012275 Bucharest Téléphone: +40 212245830 Télécopieur: +40 212240714 Adresse électronique: nsa.romania@nsa.ro Site web: www.orniss.ro	**SUÈDE** Utrikesdepartementet (Ministry for Foreign Affairs) UD-RS S-103 39 Stockholm Téléphone: +46 84051000 Télécopieur: +46 87231176 Adresse électronique: ud-nsa@foreign.ministry.se
SLOVÉNIE Urad Vlade RS za varovanje tajnih podatkov Gregorčičeva 27 1000 Ljubljana Téléphone: +386 14781390 Télécopieur: +386 14781399 Adresse électronique: gp.uvtp@gov.si	**ROYAUME-UNI** UK National Security Authority Room 335, 3rd Floor 70 Whitehall London SW1A 2AS Téléphone 1: +44 2072765645 Téléphone 2: +44 2072765497 Télécopieur: +44 2072765651 Adresse électronique: UK-NSA@cabinet-office.x.gsi.gov.uk

Appendice D

LISTE DES ABRÉVIATIONS

Acronyme	Signification
AAC	Autorité d'agrément cryptographique
AAI	Autorité chargée de l'assurance de l'information
ADC	Autorité de distribution cryptographique
AHS	Autorité d'homologation de sécurité
AI	Assurance de l'information
ANS	Autorité nationale de sécurité
AQUA	Autorité dûment qualifiée
AS	Annexes de sécurité
ASD	Autorité de sécurité désignée
AT	Autorité TEMPEST
CCTV	Closed Circuit Television – système de télévision en circuit fermé
CHS	Comité d'homologation de sécurité
CHSP	Certificat d'habilitation de sécurité du personnel
Coreper	Comité des représentants permanents
DSCE	direction de la sécurité de la Commission européenne
GCS	Guide de la classification de sécurité
HSE	Habilitation de sécurité d'établissement
HSP	Habilitation de sécurité du personnel
ICUE	Informations classifiées de l'Union européenne
ISP	Instructions de sécurité relatives à un programme/un projet
PESC	Politique étrangère et de sécurité commune
PSDC	Politique de sécurité et de défense commune
RSUE	Représentant spécial de l'Union européenne
SDI	Système de détection des intrusions
SecOP	Security Operating Procedures – procédures d'exploitation de sécurité
SGC	secrétariat général du Conseil
SIC	Systèmes d'information et de communication
SPB	Services de protection en bordure
SSRS	System-Specific Security Requirement Statement — énoncés des impératifs de sécurité propres à un système

SERVICE EUROPÉEN POUR L'ACTION EXTÉRIEURE

Décision de la haute représentante de l'Union pour les affaires étrangères et la politique de sécurité du 15 juin 2011 relative aux règles de sécurité applicables au service européen pour l'action extérieure

(2011/C 304/05)

LA HAUTE REPRÉSENTANTE,

vu la décision 2010/427/UE du Conseil fixant l'organisation et le fonctionnement du service européen pour l'action extérieure («SEAE»), et notamment son article 10,

vu l'avis du comité visé à l'article 10, paragraphe 1, de la décision du Conseil susmentionnée,

considérant ce qui suit:

(1) En tant qu'organe de l'Union européenne fonctionnant de manière autonome, le SEAE devrait être doté de règles de sécurité, telles que visées à l'article 10, paragraphe 1, de la décision 2010/427/UE du Conseil.

(2) La haute représentante doit fixer pour le SEAE des règles englobant tous les aspects de la sécurité afin que ce dernier soit en mesure de gérer efficacement les risques menaçant son personnel, ses biens matériels et les informations qu'il détient et de s'acquitter des responsabilités qui lui incombent en ce qui concerne l'obligation de vigilance à cet égard.

(3) Les règles de sécurité applicables au SEAE devraient contribuer à la mise en place d'un cadre général complet et plus cohérent au sein de l'Union européenne pour ce qui est de la protection des informations classifiées, en s'appuyant sur les règles de sécurité du Conseil et sur les dispositions de la Commission en matière de sécurité.

(4) Il convient, en particulier, de garantir au personnel du SEAE, à ses biens matériels et aux informations qu'il détient un niveau de protection conforme aux meilleures pratiques en usage au Conseil, à la Commission européenne, dans les États membres et, s'il y a lieu, dans les organisations internationales.

(5) Les principes de base et les normes minimales de protection des informations classifiées appliqués au SEAE doivent être équivalents à ceux appliqués au Conseil et à la Commission européenne.

(6) Il importe de fixer l'organisation de la sécurité dans le SEAE et l'allocation des tâches relatives à la sécurité au sein des structures du SEAE.

(7) La haute représentante doit prendre toutes les mesures qui s'imposent pour appliquer ces règles avec l'appui des États membres, du secrétariat général du Conseil et de la Commission européenne.

(8) La haute représentante s'appuie sur les compétences techniques existant en la matière dans les États membres, au secrétariat général du Conseil et à la Commission européenne, si nécessaire, en mettant notamment en place une architecture de sécurité appropriée,

A ADOPTÉ LA PRÉSENTE DÉCISION:

Article premier

Objet et champ d'application

1. La présente décision arrête les règles en matière de sûreté et de sécurité applicables au service européen pour l'action extérieure (ci-après les «règles de sécurité applicables au SEAE»). Elle définit le cadre réglementaire général permettant à ce dernier de gérer efficacement les risques menaçant son personnel, ses biens matériels et les informations qu'il détient et de s'acquitter des responsabilités qui lui incombent en ce qui concerne l'obligation de vigilance à cet égard.

2. Les règles de sécurité applicables au SEAE s'appliquent à tous les membres de son personnel (à savoir aux fonctionnaires et autres agents, aux experts nationaux détachés et aux agents locaux) et du personnel des délégations de l'Union, indépendamment de leur origine ou statut administratif (ci-après le «personnel»).

3. La haute représentante prend toute mesure nécessaire pour appliquer ces règles au sein du SEAE et se doter des moyens nécessaires englobant tous les aspects de la sécurité avec le soutien des services compétents des États membres, du secrétariat général du Conseil et de la Commission.

4. Dès l'entrée en vigueur de la présente décision, des dispositifs transitoires peuvent être utilisés, s'il y a lieu, en concluant des accords, au niveau des services, avec les services compétents du secrétariat général du Conseil et de la Commission.

5. La haute représentante réexamine périodiquement ces règles de sécurité. Elle assure la cohérence globale de l'application de la présente décision.

6. Le cas échéant, la haute représentante approuve, sur recommandation du comité visé à l'article 9, paragraphe 6, les politiques de sécurité énonçant les mesures destinées à mettre en œuvre la présente décision. Ce comité peut arrêter à son niveau des lignes directrices en matière de sécurité en complément ou à l'appui de la présente décision.

7. En mettant en œuvre le paragraphe 6, le comité tient pleinement compte des politiques et lignes directrices en matière de sécurité en vigueur au Conseil et à la Commission européenne, de manière à maintenir une certaine cohérence entre les mesures de sécurité applicables au SEAE, au Conseil et à la Commission.

Article 2

Gestion des risques de sécurité

1. Afin de déterminer ses besoins en matière de protection, le SEAE applique une méthode globale d'évaluation des risques pour la sécurité, en concertation avec le Bureau de sécurité du secrétariat général du Conseil et la direction de la sécurité de la Commission européenne. Le comité visé à l'article 9, paragraphe 6, est consulté au sujet de son application au sein du SEAE.

2. Les risques pesant sur le personnel, les biens matériels et les informations sont gérés dans le cadre d'une procédure. Cette dernière vise à déterminer les risques connus pesant sur la sécurité, à définir des mesures de sécurité permettant de ramener ces risques à un niveau acceptable et à appliquer ces mesures selon le principe de défense en profondeur. L'efficacité de telles mesures fait l'objet d'une évaluation constante.

3. Les rôles, responsabilités et tâches fixés dans la présente décision sont sans préjudice de la responsabilité qui incombe à chaque membre du personnel du SEAE de faire preuve de bon sens et de discernement pour ce qui a trait à sa propre sécurité, ni de l'obligation qui lui est faite de respecter toutes les règles, réglementations, procédures et consignes de sécurité applicables.

4. Le SEAE prend toutes les mesures raisonnables pour garantir la sécurité de son personnel, de ses biens matériels et des informations qu'il détient et pour éviter tout dommage raisonnablement prévisible s'y rapportant, conformément à l'article 1er, paragraphe 3.

5. Les mesures de sécurité applicables au SEAE visant à protéger les informations classifiées tout au long de leur cycle de vie sont proportionnées en particulier à leur classification de sécurité, à la forme sous laquelle se présentent les informations ou les matériels ainsi qu'à leur volume, au lieu et à la construction des établissements où se trouvent des informations classifiées et à la menace, notamment celle évaluée à l'échelle locale que représentent les activités malveillantes et/ou criminelles, y compris l'espionnage, le sabotage et le terrorisme.

Article 3

Protection des informations

1. La haute représentante, après avoir consulté le comité visé à l'article 10, paragraphe 1, de la décision 2010/427/UE du Conseil fixant l'organisation et le fonctionnement du SEAE, décide des règles à appliquer pour la protection des informations classifiées, équivalentes à celles fixées dans la décision 2011/292/UE du Conseil concernant les règles de sécurité aux fins de la protection des informations classifiées de l'UE [1] (ci-après les «ICUE»). En attendant l'adoption de ces règles, le SEAE applique mutatis mutandis le règlement de sécurité du Conseil susmentionné. La haute représentante prend toutes les mesures qui s'imposent pour appliquer ce règlement au sein du SEAE, en vertu de l'article 1er, paragraphe 3.

2. Lorsque les États membres introduisent des informations classifiées portant un marquage national de classification de sécurité dans les structures ou réseaux du SEAE, ce dernier protège ces informations conformément aux règles applicables aux ICUE de niveau équivalent, ainsi que prévu dans les règles applicables en vertu de l'article 3, paragraphe 1.

3. En ce qui concerne la protection des informations sensibles non classifiées, les mesures de sécurité au sein du SEAE doivent être proportionnées à leur sensibilité et/ou à l'incidence sur les intérêts de l'UE de leur divulgation non autorisée.

Article 4

Sécurité physique

1. Il convient de mettre en place des mesures physiques de sécurité appropriées, et notamment de prendre des dispositions relatives aux contrôles des accès, pour l'ensemble des locaux, bâtiments, bureaux, salles et autres zones du SEAE, y compris les zones où se trouvent les systèmes d'information et de communication traitant des informations classifiées. Ces mesures doivent être prises en tenant compte de la conception et de la planification des bâtiments.

2. Si nécessaire, des mesures physiques de sécurité sont mises en place pour la protection des membres du personnel et des personnes à leur charge.

3. Les mesures visées aux paragraphes 1 et 2 sont proportionnées au risque évalué pesant sur le personnel, les visiteurs, les biens matériels et les informations.

4. Les zones du SEAE où sont stockées des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur, ou équivalent, sont créées en tant que zones sécurisées conformément aux règles applicables en vertu de l'article 3, paragraphe 1, et doivent être approuvées par l'autorité de sécurité compétente au sein du SEAE.

Article 5

Habilitation de sécurité du personnel

1. L'accès aux informations classifiées et les procédures d'habilitation de sécurité concernant le personnel sont régis par les prescriptions figurant dans les règles applicables en vertu de l'article 3, paragraphe 1.

2. Tous les agents qui, en raison de leurs attributions, peuvent avoir besoin d'accéder à des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur, ou équivalent, font l'objet d'une habilitation

[1] Décision 2011/292/UE du Conseil du 31 mars 2011 concernant les règles de sécurité aux fins de la protection des informations classifiées de l'UE (JO L 141 du 27.5.2011, p. 17).

de sécurité du niveau correspondant avant de pouvoir accéder à de telles informations classifiées. Toutefois, les agents locaux ne doivent pas avoir accès aux ICUE, sauf si les conditions prévues dans les règles applicables en vertu de l'article 3, paragraphe 1, en disposent ainsi et en conformité avec elles.

3. Les procédures d'habilitation de sécurité concernant le personnel du SEAE figurent dans les règles applicables en vertu de l'article 3, paragraphe 1. Ces procédures offrent un niveau d'assurance équivalent à celui prévu dans les procédures appliquées par la Commission européenne et le secrétariat général du Conseil.

Article 6

Sécurité des systèmes de communication et d'information

1. Le SEAE protège les informations traitées dans les systèmes d'information et de communication (ci-après «SIC») contre les menaces pesant sur leur confidentialité, leur intégrité, leur disponibilité, leur authenticité et leur non-répudiation.

2. Tous les SIC traitant des informations classifiées font l'objet d'un processus d'homologation. Le SEAE applique un système de gestion de l'homologation de sécurité en concertation avec le secrétariat général du Conseil et la Commission européenne.

3. Lorsque la protection des ICUE est assurée par des produits cryptographiques, ces produits doivent être agréés par l'autorité d'agrément cryptographique du SEAE, sur recommandation du comité visé à l'article 10, paragraphe 1, de la décision 2010/427/UE du Conseil fixant l'organisation et le fonctionnement du SEAE, conformément à l'article 10 de la décision 2011/292/UE du Conseil concernant les règles de sécurité aux fins de la protection des informations classifiées de l'UE.

4. Pour autant que de besoin, la haute représentante institue les autorités compétentes en matière d'assurance de l'information ci-après, en vertu de l'article 3, paragraphe 1:

a) une autorité chargée de l'assurance de l'information;

b) une autorité TEMPEST;

c) une autorité d'agrément cryptographique;

d) une autorité de distribution cryptographique.

5. Pour chaque système, la haute représentante institue les autorités compétentes suivantes, en vertu de l'article 3, paragraphe 1:

a) une autorité d'homologation de sécurité;

b) une autorité opérationnelle chargée de l'assurance de l'information.

Article 7

Sensibilisation et formation en matière de sécurité

1. La haute représentante veille à l'élaboration et à la mise en œuvre de programmes de sensibilisation et de formation en matière de sécurité au sein du SEAE et fait en sorte que les membres du personnel et, s'il y a lieu, les personnes à leur charge, bénéficient d'actions de formation et de sensibilisation proportionnées aux risques inhérents à leur lieu de résidence.

2. Avant de se voir accorder l'accès à des informations classifiées et à intervalles réguliers par la suite, le personnel est informé des responsabilités qui lui incombent en matière de protection des ICUE, conformément aux règles applicables en vertu de l'article 3, paragraphe 1, et reconnait ces responsabilités.

Article 8

Infractions à la sécurité et compromission des informations classifiées

1. Toute infraction à la sécurité, réelle ou présumée, est immédiatement signalée à la direction de la sécurité du SEAE, qui en informe les autorités compétentes de la Commission, du secrétariat général du Conseil ou des États membres, si nécessaire.

2. Lorsqu'il est avéré ou qu'il existe des motifs raisonnables de supposer que des informations classifiées ont été compromises ou perdues, la direction de la sécurité du SEAE en informe la direction de la sécurité de la Commission européenne, le secrétariat général du Conseil ou les États membres, selon le cas, et prend toutes les mesures nécessaires conformément aux règles applicables en vertu de l'article 3, paragraphe 1.

3. Tout membre du personnel qui enfreint les règles de sécurité énoncées dans la présente décision est passible d'une sanction disciplinaire conformément aux dispositions législatives et réglementaires applicables. Toute personne responsable de la compromission ou de la perte d'informations classifiées est passible de sanctions disciplinaires et/ou peut faire l'objet d'une action en justice conformément aux dispositions législatives et réglementaires applicables.

Article 9

Organisation de la sécurité au sein du SEAE

1. La haute représentante est l'autorité du SEAE compétente en matière de sécurité. En cette qualité, elle veille en particulier:

a) à ce que les mesures de sécurité fassent l'objet, si nécessaire, d'une coordination avec les autorités compétentes des États membres, du secrétariat général du Conseil, de la Commission européenne et, s'il y a lieu, de pays tiers ou d'organisations internationales sur toutes les questions de sécurité présentant un intérêt pour les activités du SEAE, notamment en ce qui concerne la nature des menaces qui pèsent sur la sécurité de son personnel, de ses biens matériels et des informations qu'il détient, et les conseils sur les moyens de s'en protéger;

b) à ce que les aspects liés à la sécurité soient pleinement pris en compte dès le départ pour l'ensemble des activités du SEAE;

c) à ce que des habilitations de sécurité du personnel de l'UE soient accordées au personnel du SEAE, conformément à l'article 5, paragraphe 2, avant qu'il ne soit autorisé à accéder à des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur, ou équivalent;

d) à ce qu'un système de registres relatif à la sécurité soit établi au sein du SEAE, qui garantisse que les informations classifiées soient traitées conformément aux règles applicables en vertu de l'article 3, paragraphe 1, et qui garde une trace de toutes les informations classifiées communiquées par le SEAE à des pays tiers et à des organisations internationales, ainsi que de toutes les informations classifiées reçues de pays tiers ou d'organisations internationales;

e) à ce que les inspections de sécurité visées à l'article 11 soient réalisées;

f) à ce que des enquêtes soient menées sur toute infraction à la sécurité, réelle ou présumée, notamment toute compromission ou perte d'informations classifiées détenues par le SEAE ou provenant de ce dernier, et à ce qu'il soit demandé aux autorités de sécurité compétentes de participer à de telles enquêtes;

g) à ce que des mécanismes et des plans de gestion des incidents et de leurs conséquences soient mis en place, de manière à réagir rapidement et efficacement en cas d'incidents de sécurité;

h) à ce que des mesures appropriées soient prises en cas de non-respect de la présente décision par le personnel.

2. La haute représentante peut, si nécessaire, conclure des accords administratifs, notamment en ce qui concerne l'échange d'informations classifiées avec des pays tiers ou des organisations internationales, sans préjudice de l'article 218, paragraphe 3, du traité sur le fonctionnement de l'Union européenne. Le comité visé à l'article 9, paragraphe 6, sera consulté avant leur conclusion.

3. Le secrétaire général exécutif veille à ce que les mesures physiques et organisationnelles appropriées soient mises en place pour garantir la sécurité du personnel et des visiteurs, des biens matériels et des informations dans l'ensemble des locaux du SEAE. Il est assisté dans sa tâche par le directeur opérationnel et la direction de la sécurité du SEAE.

4. La direction de la sécurité du SEAE est responsable de l'organisation de toutes les questions ayant trait à la sécurité au sein du SEAE. Elle se tient à la disposition de la haute représentante, à laquelle elle peut rendre compte, au besoin, conformément à son mandat. En vertu de l'article 10, paragraphe 3, de la décision 2010/427/UE du Conseil fixant l'organisation et le fonctionnement du SEAE, la direction de la sécurité est assistée par les services compétents des États membres.

5. Chaque chef de délégation de l'Union est responsable de la mise en œuvre de l'ensemble des mesures relatives à la sécurité de sa délégation, dont il gère la sécurité du personnel, des visiteurs, des biens matériels et des informations. Il est assisté dans sa mission par la direction de la sécurité du SEAE, par le personnel de la délégation exerçant des tâches et fonctions ayant trait à la sécurité et par le personnel de sécurité en poste, si nécessaire.

6. Un Comité de sécurité est créé par la présente décision. La haute représentante prend conseil auprès du Comité de sécurité, qui examine et évalue toute question de sécurité relevant du champ d'application de la présente décision et émet des recommandations, le cas échéant. Le Comité de sécurité est composé d'experts de la sécurité compétents représentant chaque État membre, le secrétariat général du Conseil et la direction de la sécurité de la Commission européenne. Il est présidé par la haute représentante ou par son délégué désigné et se réunit sur instruction de celle-ci ou à la demande de l'un quelconque de ses membres. Le Comité de sécurité organise ses activités de manière à être en mesure de formuler des recommandations sur des aspects spécifiques de la sécurité entrant dans le champ d'application de la présente décision.

7. Le chef de la direction de la sécurité du SEAE rencontre régulièrement, et aussi souvent que nécessaire, le directeur de la sécurité du secrétariat général du Conseil et le directeur de la direction de la sécurité de la Commission européenne, en vue de s'entretenir de questions présentant un intérêt commun.

Article 10

Sécurité des missions PSDC et du RSUE

La responsabilité de chaque chef de mission ou du représentant spécial de l'UE (RSUE) au regard de la sécurité de la mission ou de l'équipe est définie dans la décision du Conseil relative à l'établissement de la mission du RSUE et à sa nomination. Chaque chef de mission ou le RSUE peut être assisté par la direction de la sécurité du SEAE pour veiller à ce que la politique approuvée par le Conseil en matière de sécurité du personnel déployé à l'extérieur de l'UE dans le cadre d'une capacité opérationnelle relevant du titre V, chapitre 2, du traité sur l'Union européenne soit dûment mise en œuvre. Il convient pour ce faire de mettre en place les mécanismes de liaison ad hoc.

Article 11

Inspections de sécurité

1. La haute représentante veille à ce que des inspections de sécurité soient réalisées afin de s'assurer du respect des règles de sécurité et des réglementations protégeant le personnel, les biens matériels et les informations au sein du SEAE, ainsi que dans le cadre des missions prévues au titre V, chapitre 2, du TUE.

2. Le SEAE s'appuie, si nécessaire, sur les compétences techniques existant en la matière dans les États membres, au secrétariat général du Conseil et à la Commission européenne.

3. La haute représentante adopte un programme annuel pour les inspections de sécurité.

Article 12

Planification de la continuité des activités

La direction de la sécurité du SEAE assiste le secrétaire général exécutif dans la gestion des aspects des processus opérationnels du SEAE se rapportant à la sécurité, dans le cadre de la planification globale de la continuité des activités du SEAE.

Article 13

Entrée en vigueur

La présente décision entre en vigueur le jour de sa signature.

Fait à Bruxelles, le 15 juin 2011.

La haute représentante

C. ASHTON

Council of the
European Union

Brussels, 16 December 2016
(OR. en)

15643/16

CSC 378

NOTE

From:	General Secretariat of the Council
To:	Delegations
Subject:	**Guidelines on Industrial Security**

Delegations will find attached the "Guidelines on Industrial Security" as approved by the Council Security Committee on 13 December 2016.

GUIDELINES ON INDUSTRIAL SECURITY

I. INTRODUCTION

1. These guidelines, agreed by the Council Security Committee in accordance with paragraph 2 of Annex V to the Council security rules[1] (hereinafter 'CSR'), are designed to support implementation of the CSR, and in particular Article 11 and Annex V thereto.

2. These guidelines also take into account Articles 7 and 22 of the Defence and Security Directive[2].

3. These guidelines lay down specific requirements to ensure the protection of EU classified information (hereinafter 'EUCI') by industrial or other entities in pre-contract negotiations and throughout the life-cycle of classified contracts let by the General Secretariat of the Council (GSC) and in subcontracts let by GSC prime contractors.

4. The GSC will apply these security guidelines when entrusting by contract tasks involving or entailing access to or the handling or storage of EUCI by industrial or other entities.

5. When entrusting by contract tasks involving or entailing access to or the handling or storage of EUCI by a contractor or subcontractor, Member States should use these security guidelines as a benchmark.

6. EU agencies and bodies established under Title V, Chapter 2 of the TEU, Europol and Eurojust should use these security guidelines as a reference for implementing security rules in their own structures.

---

[1] Council Decision 2013/488/EU of 23 September 2013 on the security rules for protecting EU classified information (OJ L 274, 15.10.2013, p. 1).

[2] Directive 2009/81/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of procedures for the award of certain works contracts, supply contracts and service contracts by contracting authorities or entities in the fields of defence and security (OJ L 216, 20.8.2009, p. 76).

II. RESPONSIBILITY WITHIN THE GSC

7. Each GSC Authorising Officer, as part of his or her responsibilities as described in the Financial Regulation[3], will ensure that the minimum standards on industrial security set out in Article 11 of and Annex V to the CSR and in these guidelines are referred to in the contract, and where appropriate in the invitation to tender, and complied with when letting classified contracts.

8. To that effect, the Authorising Officer concerned must seek the advice of the GSC Security Office on issues regarding the classified nature of the contract and the elements of the procedure at all stages.

9. In respect of the requirements of these guidelines, the GSC must cooperate closely with the NSA/DSA or any other relevant competent authority of the Member States concerned, in particular concerning Facility Security Clearances (hereinafter 'FSCs') and Personnel Security Clearances (hereinafter 'PSCs'), visit procedures and transportation plans.

III. PRE-CONTRACTUAL STAGE AND NEGOTIATION OF GSC CLASSIFIED CONTRACTS

Classified contracts

10. A classified contract is a contract to be entered into by the GSC with a contractor for the supply of goods, execution of works or provision of services, the performance of which requires or involves access or potential access to or the creation of EUCI.

[3] Regulation (EU, Euratom) No 966/2012 of the European Parliament and of the Council of 25 October 2012 on the financial rules applicable to the general budget of the Union and repealing Council Regulation (EC, Euratom) No 1605/2002 (OJ L 298, 26.10.2012, p. 1).

11. No classified contract may be awarded to industrial or other entities registered in a non-EU Member State which has not concluded a security of information agreement with the EU or entered into an administrative arrangement with the GSC. Should the security of information agreement or administrative arrangement not cover industrial security aspects, a review of the agreement/arrangement is necessary before an entity registered in that non-EU Member State may be awarded a classified contract.

12. Prior to launching an invitation to tender or letting a classified contract, the Authorising Officer, in liaison with the GSC Security Office, must determine the security classification of any information that may be provided to bidders. The Authorising Officer, in liaison with the GSC, will also determine the maximum security classification of any information generated in the performance of the contract, or at least the anticipated volume and type of information to be produced or handled, and the need for a classified Communication and Information System (hereinafter 'CIS'). For that purpose the contracting authority must prepare, in accordance with the 'Policy on creating EUCI'[4], a Security Classification Guide (hereinafter 'SCG') to be used for the performance of the contract.

13. All contractors who are required to handle or store information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET within their facilities, either during the performance of the classified contract itself or during the pre-contractual stage, must hold a Facility Security Clearance (hereinafter 'FSC') at the required level. The following identifies the three scenarios that may arise during the tendering phase for a classified contract involving EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET level:

a) No access to EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET level during the tendering phase

When the contract notice, invitation to tender or call for proposals concerns a contract that will involve EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET

[4] 10872/11.

UE/EU SECRET level, but does not require the bidder to handle such information at the tender stage, a bidder not holding an FSC at the required level must not be excluded from the bidding process.

b) Access to EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET level at the premises of the contracting authority during the tendering phase

Access will be granted to contractor personnel who are in possession of a Personnel Security Clearance (hereinafter 'PSC') at the required level and who have a need-to know. The contracting authority will verify with the respective NSA/DSA whether an FSC is also required under national laws and regulations at this stage, before such access is granted.

Where EUCI is provided to a bidder at the tender stage, a non-disclosure agreement must be signed, obliging the bidder to handle and protect EUCI provided to him in accordance with the CSR.

c) Handling or storage of EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET level at the premises of the bidder during the tendering phase

When the contract notice, invitation to tender or call for proposals requires bidders to handle or store EUCI at their premises, the bidder holds an FSC at the required level. In such circumstances the contracting authority will obtain an assurance from the relevant NSA/DSA that the bidder has been granted an appropriate FSC. Access will be granted to contractor personnel who are in possession of a PSC at the required level and who have a need-to-know.

Where EUCI is provided to a bidder at the tender stage, a non-disclosure agreement must be signed, obliging the bidder to handle and protect EUCI provided to him in accordance with the CSR.

An FSC is not required for access to classified information at RESTREINT UE/EU RESTRICTED level, either at the tender stage or for the performance of the contract. However, some EU Member States require an FSC for contracts and subcontracts at RESTREINT UE/EU RESTRICTED level under their national laws and regulations, as listed in Annex III to these guidelines. Such national requirements shall not put additional obligations on other Member States nor exclude bidders or contractors/subcontractors from Member States not having such FSC requirements for access to RESTREINT UE/EU RESTRICTED information for related contracts/subcontracts or a competition for such, while these contracts shall be performed in Member States according to their national laws and regulations.

14. Where an FSC is required for the performance of a classified contract, the contracting authority will submit a request to the contractor's NSA/DSA using a Facility Security Clearance Information Sheet (hereinafter 'FSCIS'); for guidance, an example of an FSCIS[5] is provided in Annex II, Appendix D. The classified contract will not be awarded until the contractor's NSA/DSA has confirmed the bidder's FSC. Response to an FSCIS should be provided within ten working days of the date of the request.

Subcontracting in classified contracts

15. The conditions under which a contractor awarded a GSC prime contract may subcontract should be defined in the invitation to tender and in the prime contract documentation. If subcontracting is permitted, then a contractor must obtain written consent from the GSC before subcontracting any parts of a classified contract. No classified subcontract may be awarded to industrial or other entities registered in a non-EU Member State which has not concluded a security of information agreement with the EU or entered into an administrative arrangement with the GSC.

[5] Other forms used may differ from the example provided in these guidelines in their design. However, they must not differ in their content.

IV. LETTING GSC CLASSIFIED CONTRACTS

16. Upon letting the prime contract, the GSC Security Office will ensure that the obligations of the contractor regarding the protection of EUCI provided to the contractor or generated in the performance of the contract are an integral part of the contract. Contract-specific security requirements may take the form of a Security Aspects Letter (hereinafter 'SAL') (an example of a SAL is provided in Annex II to these guidelines) or of Programme/Project Security Instructions (hereinafter 'PSI').

17. To ensure appropriate security oversight of the contractor, the GSC Security Office will notify and provide a copy of the contract-specific security provisions to the contractor's or subcontractor's NSA/DSA. NSAs/DSAs or any other competent security authority requiring notification about the security provisions of classified contracts at RESTREINT UE/EU RESTRICTED level only are listed in Annex III to these guidelines.

18. Contracts involving classified information at RESTREINT UE/EU RESTRICTED level will include a contract security clause making the provisions specified in Annex II, Appendix E to these guidelines binding upon the contractor. For such purpose contracts involving RESTREINT UE/EU RESTRICTED information will include a SAL detailing, as a minimum, the requirements for handling RESTREINT UE/EU RESTRICTED information including information assurance aspects and specific provisions to be satisfied by a contractor under delegation from the contracting authority for the accreditation of the contractor's CIS handling RESTREINT UE/EU RESTRICTED information.

19. When RESTREINT UE/EU RESTRICTED information is provided to bidders or potential contractors such minimum requirements will also be included in tenders or relevant non-disclosure arrangements concluded at the tender stage.

20. Where required by Member States' national laws and regulations, NSAs/DSAs will be responsible for ensuring that contractors or subcontractors under their jurisdiction comply with the applicable security provisions for the protection of RESTREINT UE/EU

RESTRICTED information and should conduct verification visits on contractors' facilities located in their territory. If an NSA/DSA does not have such an obligation, it is the responsibility of the contracting authority to ensure that the required security provisions detailed in Annex II are implemented by the contractor.

Access to EUCI by contractor and subcontractor personnel

21. The GSC, as contracting authority, will make sure that the classified contract includes provisions indicating that personnel of a contractor or subcontractor who, for the performance of the classified contract or subcontract, require access to EUCI may be granted such access only if:

    a) their need-to-know has been determined;
    b) they have been granted a PSC at the relevant level for information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET by the respective NSA/DSA or any other competent security authority; and
    c) they have been briefed on the applicable security rules for protecting EUCI, and have acknowledged their responsibilities with regard to protecting such information.

22. If a contractor or subcontractor wishes to employ a national of a non-EU country in a position that requires access to EUCI classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET, it is the responsibility of the NSA/DSA or any other competent security authority under whose jurisdiction the contractor or subcontractor falls to begin the security clearance procedure in accordance with national laws and regulations.

V. VISITS IN CONNECTION WITH CLASSIFIED CONTRACTS

23. Where the GSC, contractors or subcontractors require access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET in each other's premises for the performance of a classified contract, visits will be arranged in liaison with the NSAs/DSAs or any other competent security authority concerned.

24. Those visits are subject to the following conditions:
    a) the visit must have an official purpose related to a classified contract let by the GSC;
    b) all visitors must hold a PSC at the required level and have a need-to-know in order to access EUCI provided or generated in the performance of a classified contract let by the GSC.

Requests for Visits

25. Visits by contractors to other contractors' facilities, or to GSC premises, that involve access to EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET level are authorised by the following procedure:

    a) the Security Officer of the visitor(s) must complete all the relevant parts of the Request for Visit (RFV) form (an example of the form is provided in Annex II, Appendix C) and submit that request to its NSA/DSA;
    b) the visitor's NSA/DSA will confirm the PSC of the visitor(s) before submitting the RFV to the host facility's NSA/DSA (or the GSC Security Office if the visit is to GSC premises);
    c) the host facility's NSA/DSA (or the GSC Security Office) will reply to the request either authorising or denying the RFV;
    d) an RFV can be considered as approved unless objections are raised five working days prior to the date of the visit.

26. Visits by GSC officials to contractor facilities that involve access to EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET level are authorised by the following process:

a) the visitor(s) must complete all the relevant parts of the RFV form (an example of the form is provided in Annex II, Appendix C), and submit that request to the GSC Security Office;
b) the GSC Security Office will confirm the PSC of the visitor(s) before submitting the RFV to the host facility's NSA/DSA;
c) the host facility's NSA/DSA will reply to the request either authorising or denying the RFV;
d) an RFV can be considered as approved unless objections are raised five working days prior to the date of the visit.

27. An RFV may cover either a single visit or recurring visits. In the case of recurring visits, the RFV can only be valid for up to one year from the start date requested.

28. The validity of any RFV must not exceed the validity of the PSC of the visitor(s).

29. As a general rule an RFV should be submitted to the host facility's competent security authority at least 15 working days prior to the date of the visit.

Visit procedures

30. Before permitting the visitor(s) to have access to EUCI, the host facility must have received authorisation from its NSA/DSA or other competent security authority.

31. Visitors must prove their identity upon arrival at the host facility by presenting a valid ID card or passport as indicated in the RFV.

32. The facility hosting the visit must ensure that records are kept of all visitors, including their names, the organisation they represent, the date of expiry of the PSC, the date of the visit and the name(s) of the person(s) visited. Without prejudice to European data-protection rules, such records are to be retained for a period of no less than three years or in accordance with national rules and regulations, as appropriate.

Visits arranged directly

33. In the context of specific projects, the relevant NSAs/DSAs and the GSC may agree on a procedure whereby visits for a specific classified contract can be arranged directly between the visitor's Security Officer and the Security Officer of the facility to be visited (an example of the form is provided in Annex II, Appendix C). Such an exceptional procedure will be set out in the PSI or other specific arrangements. In such cases, the procedures in paragraphs 25 to 30 do not apply.

34. Visits involving access or potential access to EUCI at RESTREINT UE/EU RESTRICTED level will be arranged directly between the sending and receiving entity without the need to follow the procedure described in paragraphs 25 to 30.

VI. TRANSMISSION AND CARRIAGE OF EUCI

35. The contracting authority must ensure that all transfer and carriage decisions are in accordance with the CSR and with the terms of the classified contract, including the consent of the originator.

Electronic handling

36. Electronic handling and transmission of EUCI must be done in accordance with the provisions laid down in Article 10 of and Annexes IV and V to the CSR. These include, *inter alia,* that Communication and Information Systems owned by a contractor and used for handling EUCI for the performance of the contract (hereinafter 'contractor CIS') will be subject to accreditation by the responsible Security Accreditation Authority, that any electronic transmission of EUCI must be protected by cryptographic products approved in accordance with Article 10(6) of the CSR, and that TEMPEST measures must be implemented in accordance with Article 10(5) of the CSR.

37. The security accreditation of contractor CIS handling EUCI at RESTREINT UE/EU RESTRICTED level and any interconnection thereof may be delegated to the Security Officer of a contractor if permitted by national laws and regulations. Where that task is delegated, it is the responsibility of the contractor to implement the minimum security requirements described in the SAL when handling RESTREINT UE/EU RESTRICTED information on its CIS. However, the relevant NSAs/DSAs/SAAs must retain responsibility for the protection of RESTREINT UE/EU RESTRICTED information handled by the contractor and the right to inspect the security measures taken by the contractors. In addition, the contractor will provide to the contracting authority and, where nationally required the competent national SAA, a statement of compliance certifying that the contractor CIS and respective interconnections have been accredited for handling EUCI at RESTREINT UE/EU RESTRICTED level[6].

[6] Minimum requirements for CIS handling EUCI at R-UE/EU-R level are laid down in Annex II, Appendix E.

Carriage by commercial couriers

38. Carriage of EUCI by commercial couriers, where necessary for the performance of the contract, must be in accordance with the 'Guidelines on the carriage of EUCI by commercial couriers'[7].

Hand carriage of EUCI

39. Hand carriage of EUCI at RESTREINT UE/EU RESTRICTED level by contractor personnel is permitted provided that contractors comply with the following instructions:

    a) the envelope/package used must be opaque and bear no indication of the classification of its contents;
    b) EUCI must not leave the possession of the bearer; and
    c) the envelope/package must not be opened *en route* and the EUCI must not be read in public places.

40. Hand carriage of EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET level by contractor personnel will be arranged between the sending and receiving entities and must comply with the following minimum standards:

    a) the EUCI must be carried in a double envelope/package;
    b) the outer envelope/package must be secured and bear no indication of the classification of its contents, while the inner envelope must bear the level of classification;
    c) EUCI must not leave the possession of the bearer;

[7] 5385/13.

d) the envelope/package must not be opened *en route* and the EUCI must not be read in public places;

e) a lockable briefcase or similar approved container must be of such size and weight that it can be retained at all times in the personal possession of the bearer and not be consigned to a baggage hold;

f) the courier must carry a courier certificate issued by his/her competent security authority authorising the courier to carry the classified consignment as identified.

41. Additional precautions must be taken when CONFIDENTIEL UE/EU CONFIDENTIAL information is carried internationally by contractor personnel:

a) the courier must be responsible for the safe custody of the classified material carried until such time as it has been handed over to the consignee. In the event of a breach of security, the consignor's NSA/DSA may request that the authorities in the country in which the breach occurred carry out an investigation, report their findings and take legal or other action as appropriate;

b) the courier must be briefed on all the security obligations to be observed during carriage and must sign a relevant acknowledgement;

c) the instructions for the courier must be attached to the courier certificate;

d) the courier must also be provided with a description of the consignment and an itinerary;

e) the documents must be returned to the issuing NSA/DSA upon completion of the journey(s) or be kept available at the company for monitoring purposes;
if customs, immigration authorities or border police ask to examine and inspect the consignment, they must be permitted to open and observe sufficient parts of the consignment so as to determine that it does not contain material other than that which is declared;

f) customs authorities may be advised by the appropriate national authorities of the impending consignment and should be urged to honour the official authority of the shipping documents and of the authorisation documents carried by the courier;

g) if a consignment is opened by customs, this should be done out of sight of unauthorised persons and in the presence of the courier where possible. The consignment must be repacked and the authorities conducting the inspection should be asked to reseal the consignment and confirm in writing that it was opened by them.

42. The dispatching authority/facility must inform the receiving authority/facility of the details (e.g. reference, classification, expected time of arrival, name of courier) prior to the hand carriage taking place.

VII. BUSINESS CONTINUITY PLANNING

43. The GSC, as contracting authority, will ensure that the classified contract obliges the contractor to set out contingency plans for protecting EUCI handled in connection with the performance of the classified contract in emergency situations, as well as to put in place preventive and recovery measures in the context of business continuity planning (hereinafter 'BCP') to minimise the impact of incidents in relation to the handling and storage of EUCI. The contractor must inform the GSC of its BCP.

ANNEX I

ARTICLE ON SECURITY IN THE FRAMEWORK CONTRACT
for contracts involving EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET level

21.2 The contractor or subcontractor, and their personnel, must be security cleared to the appropriate level where:

a) the contract or subcontract involves or entails access to, or handling and/or storage of information classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET, for which a Facility Security Clearance is required;

b) for the performance of a classified contract, contractor or subcontractor personnel require access to information classified CONFIDENTIEL UE/EU CONFIDENTIEL or SECRET UE/EU SECRET, for which a Personnel Security Clearance is required;

c) for the performance of a contract, contractor or subcontractor personnel are employed in circumstances where they may have access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above, for which a Personnel Security Clearance is required;

d) for the performance of the contract, contractor or subcontractor personnel have access to secured areas or are involved in the technical operation or maintenance of communications and information systems containing information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above, for which a Personnel Security Clearance is required.

21.3 The contractor or his personnel and, where applicable their subcontractors, must comply with Council Decision 2013/488/EU of 23 September 2013 on the security rules for protecting EU classified information[8]; with the security requirements provided for in the Security Aspects Letter (hereinafter 'SAL'); and with any additional instructions from the Council's Security Office. Should the contractor fail to comply with any of those rules, requirements or instructions, the GSC may, without prejudice to any indemnity due by the contractor to the GSC, terminate the specific contract with immediate effect to the contractor. In those circumstances, no costs or compensation relating to such termination will be due by the GSC to the contractor.

[8] OJ L 274, 15.10.2013, p. 1.

ARTICLE ON SECURITY IN THE FRAMEWORK CONTRACT
for contracts involving EUCI at RESTREINT UE /EU RESTRICTED level only

[21.2] The contractor must handle and protect information classified RESTREINT UE/EU RESTRICTED in accordance with the requirements stated in the SAL.

[21.3] The GSC or competent national security authorities, where required by national laws and regulations, must be entitled to conduct verification visits on the contractor's facilities to ensure compliance with these requirements.

ANNEX II

[Annex 4 (to the Framework Contract)]

SECURITY ASPECTS LETTER (SAL)

[Model]

APPENDIX A

SECURITY REQUIREMENTS

The contracting authority must include the following security requirements in the SAL. Some clauses may not be applicable to the contract and are indicated by brackets.

The clauses listed are not an exhaustive list, and additional clauses may be added depending on the nature of the classified contract.

GENERAL CONDITIONS [*note: applicable to all classified contracts*]

1. This Security Aspects Letter (SAL) is an integral part of the classified contract [or subcontract] and describes contract-specific security requirements. Non-compliance with these requirements may constitute sufficient grounds for termination of the contract.

2. Classified information generated for the performance of the contract must be marked as EU classified information (EUCI) as determined in the Security Classification Guide (SCG) in Appendix B to this letter.

3. Regarding EUCI created and handled for the performance of the classified contract, the rights incumbent on the originator are exercised by the GSC, as the contracting authority.

4. Without the written consent of the contracting authority, the contractor or subcontractor must not make use of any information or material furnished by the contracting authority or produced on behalf of the contracting authority other than for the purpose of the contract.

5. All security breaches related to EUCI must be investigated. Security breaches are to be reported to the contracting authority as soon as is practicable. The contractor or subcontractor must immediately report to his responsible NSA/DSA and, where permitted by its national laws and regulations, to the GSC Security Office all cases in which it is known or there is reason to suspect that EUCI provided or generated pursuant to the contract has been lost or disclosed to unauthorised persons.

6. Upon termination of the contract, the contractor or subcontractor must return any EUCI held by him to the contracting authority as soon as possible. Where practicable, in accordance with national laws and regulations, and with the prior agreement of and under instruction from the GSC Security Office, EUCI may be destroyed by the contractor or subcontractor instead of being returned. EUCI must be destroyed in such a way that it cannot be reconstructed in whole or in part.

7. Where the contractor or subcontractor is authorised to retain EUCI after termination or conclusion of the contract, the EUCI must continue to be protected in accordance with the Council security rules[9].

8. Electronic handling, processing and transmission of EUCI must be done in accordance with the provisions laid down in Article 10 of and Annexes IV and V to the Council security rules (hereinafter 'CSR'). These include, *inter alia*, that Communication and Information Systems (hereinafter 'CIS') owned by the contractor and used for handling EUCI for the purpose of the contract (hereinafter 'contractor CIS') must be subject to accreditation[10]; that any electronic transmission of EUCI must be protected by cryptographic products approved in accordance with Article 10(6) CSR; and that TEMPEST measures must be implemented in accordance with Article 10(5) CSR.

---

[9] Council Decision 2013/488/EU of 23 September 2013 on the security rules for protecting EU classified information (OJ L 274, 15.10.2013, p. 1).

[10] The party undertaking the accreditation will have to provide a statement of compliance to the contracting authority (the GSC Security Office) in co-ordination with the relevant national Security Accreditation Authority.

9. The contractor or subcontractor will inform the GSC of Business Contingency Plans (BCP) for protecting EUCI handled in the performance of the classified contract in emergency situations and will put in place preventive and recovery measures in the context of BCP to minimise the impact of incidents in relation to the handling and storage of EUCI.

CONTRACTS REQUIRING ACCESS TO INFORMATION CLASSIFIED RESTREINT UE/EU RESTRICTED

10. A Personnel Security Clearance (PSC) is not required. However, RESTREINT UE/EU RESTRICTED information or material must only be accessible to contractor personnel requiring such information for the performance of the contract (need-to-know principle), who have been briefed by the contractor's Security Officer on their responsibilities and on the consequences of any compromise or breach of security of such information, and have acknowledged in writing the consequences of a failure to protect EUCI.

11. Except where the contracting authority has given its written consent, the contractor or subcontractor must not provide access to RESTREINT UE/EU RESTRICTED information or material to any entity or person other than those of his personnel who have a need-to-know.

12. The contractor or subcontractor must maintain the security classification markings of classified information generated by or provided during the performance of a contract and must not declassify information without the written consent of the contracting authority.

13. Information or material classified RESTREINT UE/EU RESTRICTED must be stored in locked office furniture when not in use. When in transit documents must be carried inside an opaque envelope. The documents must not leave the possession of the bearer and they must not be opened *en route* or read in public places.

14. The contractor or subcontractor may transmit documents classified RESTREINT UE/EU RESTRICTED to the GSC using commercial courier companies, postal services, hand carriage or electronic means. To this end, the contractor or subcontractor must follow the Programme Security Instructions (PSI) issued by the GSC.

15. When no longer required, documents classified RESTREINT UE/EU RESTRICTED must be destroyed in such a way that it cannot be reconstructed in whole or in part.

16. The security accreditation of contractor CIS handling EUCI at RESTREINT UE/EU RESTRICTED level and any interconnection thereof may be delegated to the Security Officer of a contractor if permitted by national laws and regulations. Where that delegation is exercised, the NSAs/DSAs/SAAs must retain responsibility for the protection of RESTREINT UE/EU RESTRICTED information handled by the contractor and the right to inspect the security measures taken by the contractor. In addition, the contractor will provide to the contracting authority and, where nationally required, the competent national SAA a statement of compliance certifying that the contractor CIS and respective interconnections have been accredited for handling EUCI at RESTREINT UE/EU RESTRICTED level.

HANDLING OF INFORMATION CLASSIFIED RESTREINT UE/EU RESTRICTED

IN COMMUNICATION AND INFORMATION SYSTEMS (CIS)

17. Minimum requirements for CIS handling EUCI at RESTREINT UE/EU RESTRICTED level are laid down in Appendix E to this SAL.

CONDITIONS UNDER WHICH THE CONTRACTOR MAY SUBCONTRACT

18. The contractor must obtain permission from the GSC, as contracting authority, before subcontracting any parts of a classified contract.

19. No subcontract may be awarded to companies registered in a non-EU Member State which has not concluded a security of information agreement with the EU or an administrative arrangement with the GSC.

20. Where the contractor has let a subcontract, the security provisions of the contract will apply *mutatis* mutandis to the subcontractor(s) and their personnel. In such case, it is the responsibility of the contractor to ensure that all subcontractors apply these principles to their own subcontracting arrangements.

21. The contractor may not release any EUCI to a subcontractor without the prior written approval of the contracting authority. If transmission of EUCI to subcontractors will be frequent or routine, then the contracting authority may issue an approval to cover a specified length of time (e.g. 12 months) or the duration of the subcontract.

VISITS

If the standard RFV procedure is to be applied for visits involving EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET level, then the contracting authority must include paragraphs 22, 23 and 24 and delete paragraph 25. If visits involving EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET level are arranged directly between the sending and receiving establishments, then the contracting authority must delete paragraphs 23 and 24 and only include paragraph 25.

22. Visits involving access or potential access to EUCI at RESTREINT UE/EU RESTRICTED level will be arranged directly between the sending and receiving establishments without the need to follow the procedure described in paragraphs 23 to 25 hereafter.

[23. Visits involving access or potential access to EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET level must be subject to the following procedure:

a) the Security Officer of the visitor(s) must complete all the relevant parts of the RFV form (Appendix C) and submit that request to its NSA/DSA;
b) the NSA/DSA of the visitor(s) will confirm the PSC of the visitor(s) before submitting the RFV to the host facility's NSA/DSA (or the GSC Security Office if the visit is to GSC premises);
c) the host facility's NSA/DSA (or the GSC Security Office) will reply either authorising or denying the RFV;
d) an RFV can be deemed approved unless objections are raised five working days prior to the date of the visit.]

[24. Before permitting the visitor(s) to have access to EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET level, the host facility must have received authorisation from its NSA/DSA.]

[25. Visits involving access or potential access to EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET level will be arranged directly between the sending and receiving establishments (an example of the form that may be used for this purpose is provided in Appendix C).]

26. Visitors must prove their identity upon arrival at the host facility by presenting a valid ID card or passport.

27. The facility hosting the visit must ensure that records are kept of all visitors, including their names, the organisation they represent, the date of expiry of the PSC (if applicable), the date of the visit and the name(s) of the person(s) visited. Without prejudice to European data-protection rules, such records are to be retained for a period of no less than three years or in accordance with national rules and regulations, as appropriate.

ASSESSMENT VISITS

28. The GSC Security Office may, in cooperation with the relevant NSA/DSA, conduct visits at contractors' or subcontractors' facilities to verify proper implementation of the security requirements for handling EUCI.

SECURITY CLASSIFICATION GUIDE

29. A list of all the items in the contract which are classified or to be classified in the course of the performance of the contract and the rules for so doing are contained in the Security Classification Guide (hereinafter 'SCG'). The SCG is an integral part of this contract and can be found in Appendix B to this Annex.

APPENDIX B

SECURITY CLASSIFICATION GUIDE

[specific text to be adjusted depending on the object of the contract]

APPENDIX C

REQUEST FOR VISIT

(MODEL)

DETAILED INSTRUCTIONS FOR COMPLETION OF REQUEST FOR VISIT

(The application must be submitted in English only)

HEADING	Check boxes for visit type, information type, and indicate how many sites are to be visited and the number of visitors.
4. ADMINISTRATIVE DATA	To be completed by requesting NSA/DSA).
5. REQUESTING ORGANISATION OR INDUSTRIAL FACILITY	Give full name and postal address. Include city, state and post code as applicable.
6. ORGANISATION OR INDUSTRIAL FACILITY TO BE VISITED	Give full name and postal address. Include city, state, post code, telex or fax number (if applicable), telephone number and e-mail. Give the name and telephone/fax numbers and e-mail of your main point of contact or the person with whom you have made the appointment for the visit. Remarks: 1) Giving the correct post code (zip code) is important because a company may have various different facilities. 2) When applying manually, Annex 1 can be used when two or more facilities have to be visited in connection with the same subject. When an Annex is used, item 3 should state: "SEE ANNEX 1, NUMBER OF FAC.:.." (state number of facilities).

7. DATES OF VISIT	Give the actual date or period (date-to-date) of the visit in the format 'day - month - year'. Where applicable, give an alternate date or period in brackets.
8. TYPE OF INITIATIVE	Specify whether the visit has been initiated by the requesting organisation or facility or by invitation of the facility to be visited.
9. THE VISIT RELATES TO:	Specify the full name of the project, contract or call for tender using commonly used abbreviations only.
10. SUBJECT TO BE DISCUSSED/ JUSTIFICATION	Give a brief description of the reason(s) for the visit. Do not use unexplained abbreviations. <u>Remarks</u>: In the case of recurring visits this item should state 'Recurring visits' as the first words in the data element (e.g. Recurring visits to discuss_____)
11. ANTICIPATED LEVEL OF CLASSIFIED INFORMATION TO BE INVOLVED	State SECRET UE/EU SECRET (S-UE/EU-S) or CONFIDENTIEL UE/EU CONFIDENTIAL (C-UE/EU-C) as appropriate.
12. PARTICULARS OF VISITOR	<u>Remark</u>: when more than two visitors are involved in the visit, Annex 2 should be used.
13. THE SECURITY OFFICER OF THE REQUESTING ENTITY	This item requires the name, telephone number, fax number and e-mail of the requesting facility's Security Officer.

14. CERTIFICATION OF SECURITY CLEARANCE	This field is to be completed by the certifying authority. Notes for the certifying authority: a. Give name, address, telephone number, fax number and e-mail (can be pre-printed). b. This item should be signed and stamped (if applicable).
15. REQUESTING SECURITY AUTHORITY	This field is to be completed by the NSA/DSA. Note for the NSA/DSA: a. Give name, address, telephone number, fax number and e-mail (can be pre-printed). b. This item should be signed and stamped (if applicable).

All fields must be completed and the form submitted via Government-to-Government channels[11]

REQUEST FOR VISIT

(MODEL)

TO: _____

1. TYPE OF VISIT REQUEST	**2. TYPE OF INFORMATION**	**3. SUMMARY**
☐ Single ☐ Recurring ☐ Emergency ☐ Amendment ☐ Dates ☐ Visitors ☐ Facility For an amendment, insert the NSA/DSA original RFV Reference No_____	☐ C-UE/EU-C ☐ S-UE/EU-S	No of sites: _____ No of visitors: _____
4. ADMINISTRATIVE DATA:		

[11] If it has been agreed that visits involving access or potential access to EUCI at CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET level can be arranged directly, the completed form can be submitted directly to the Security Officer of the establishment to be visited.

Requester: To:	NSA/DSA RFV Reference No_____ Date *(dd/mm/yyyy)*: _____/_____/_____

5. REQUESTING ORGANISATION OR INDUSTRIAL FACILITY:

NAME:

POSTAL ADDRESS:

E-MAIL ADDRESS:

FAX NO: TELEPHONE NO:

6. ORGANISATION(S) OR INDUSTRIAL FACILITY(IES) TO BE VISITED *(Annex 1 to be completed)*

7. DATE OF VISIT *(dd/mm/yyyy)*: FROM _____/_____/_____ TO _____/_____/_____

8. TYPE OF INITIATIVE:

☐ Initiated by requesting organisation or facility

☐ By invitation of the facility to be visited

9. THE VISIT RELATES TO CONTRACT:

10. SUBJECT TO BE DISCUSSED/REASONS/PURPOSE (Include details of host entity and any other relevant information. Abbreviations should be avoided):

11. ANTICIPATED HIGHEST CLASSIFICATION LEVEL OF INFORMATION/MATERIAL OR SITE ACCESS TO BE INVOLVED:
12. PARTICULARS OF VISITOR(S) ***(Annex 2 to be completed)***
13. THE SECURITY OFFICER OF THE REQUESTING ORGANISATION OR INDUSTRIAL FACILITY: NAME: TELEPHONE NO: E-MAIL ADDRESS: SIGNATURE:

14. CERTIFICATION OF SECURITY CLEARANCE LEVEL:

NAME:

ADDRESS:

STAMP

TELEPHONE NO:

E-MAIL ADDRESS:

SIGNATURE: DATE *(dd/mm/yyyy)*: _____/_____/_____

15. REQUESTING NATIONAL SECURITY AUTHORITY/DESIGNATED SECURITY AUTHORITY:

NAME:

ADDRESS:

STAMP

TELEPHONE NO:

E-MAIL ADDRESS:

SIGNATURE: DATE *(dd/mm/yyyy)*: _____/_____/_____

16. REMARKS *(Mandatory justification required in the case of an emergency visit)*:

ORGANISATION(S) OR INDUSTRIAL FACILITY(IES) TO BE VISITED
1. NAME: ADDRESS: TELEPHONE NO: FAX NO: NAME OF POINT OF CONTACT: E-MAIL: TELEPHONE NO: NAME OF SECURITY OFFICER OR SECONDARY POINT OF CONTACT: E-MAIL: TELEPHONE NO:
2. NAME: ADDRESS: TELEPHONE NO: FAX NO:

NAME OF POINT OF CONTACT: E-MAIL: TELEPHONE NO: NAME OF SECURITY OFFICER OR SECONDARY POINT OF CONTACT: E-MAIL: TELEPHONE NO:
3. NAME: ADDRESS: TELEPHONE NO: FAX NO: NAME OF POINT OF CONTACT: E-MAIL: TELEPHONE NO: NAME OF SECURITY OFFICER OR SECONDARY POINT OF CONTACT: E-MAIL: TELEPHONE NO:
4. NAME:

ADDRESS:

TELEPHONE NO:

FAX NO:

NAME OF POINT OF CONTACT:

E-MAIL:

TELEPHONE NO:

NAME OF SECURITY OFFICER OR

SECONDARY POINT OF CONTACT:

E-MAIL:

TELEPHONE NO:

(Continue as required)

PARTICULARS OF VISITOR(S)

1.

SURNAME:

FIRST NAMES *(as per passport)*:

DATE OF BIRTH *(dd/mm/yyyy)*:____/____/____

PLACE OF BIRTH:

NATIONALITY:

SECURITY CLEARANCE LEVEL:

PP/ID NUMBER:

POSITION:

COMPANY/ORGANISATION:

2.

SURNAME:

FIRST NAMES *(as per passport)*:

DATE OF BIRTH *(dd/mm/yyyy)*:____/____/____

PLACE OF BIRTH:

NATIONALITY:

SECURITY CLEARANCE LEVEL: PP/ID NUMBER: POSITION: COMPANY/ORGANISATION:
3. SURNAME: FIRST NAMES *(as per passport)*: DATE OF BIRTH *(dd/mm/yyyy)*:____/____/____ PLACE OF BIRTH: NATIONALITY: SECURITY CLEARANCE LEVEL: PP/ID NUMBER: POSITION: COMPANY/ORGANISATION:

4.

SURNAME:

FIRST NAMES *(as per passport)*:

DATE OF BIRTH *(dd/mm/yyyy)*:____/____/____

PLACE OF BIRTH:

NATIONALITY:

SECURITY CLEARANCE LEVEL:

PP/ID NUMBER:

POSITION:

COMPANY/ORGANISATION:

(Continue as required)

APPENDIX D

FACILITY SECURITY CLEARANCE INFORMATION SHEET (FSCIS)
(MODEL)

1. INTRODUCTION

1.1 Attached is a sample Facility Security Clearance Information Sheet (hereinafter 'FSCIS') for the rapid exchange of information between the National Security Authority or Designated Security Authority (hereinafter 'NSA/DSA'), other competent national security authorities and the GSC (as contracting authority) with regard to the Facility Security Clearance (hereinafter 'FSC') of a facility involved in classified tenders, contracts or subcontracts.

1.2 The FSCIS is valid only if stamped by the relevant NSA/DSA or other competent authority.

1.3 The FSCIS is divided into a request and reply section and can be used for the purposes identified above or for any other purposes for which the FSC status of a particular facility is required. The reason for the enquiry must be identified by the requesting NSA/DSA in field 7 of the request section.

1.4 The details contained in the FSCIS are not normally classified; accordingly, when an FSCIS is to be sent between the respective NSAs/DSAs/GSC this should preferably be done by electronic means.

1.5 NSAs/DSAs should make every effort to respond to an FSCIS request within ten working days.

1.6 Should any classified information be transferred or a contract awarded in relation to this assurance, the issuing NSA/DSA must be informed.

Procedures and Instructions for the

use of the Facility Security Clearance Information Sheet (FSCIS)

These detailed instructions are for the NSA/DSA or GSC contracting authority that completes the FSCIS. The request should preferably be typed in capital letters

HEADER	The requester inserts full NSA/DSA and country name.
1. REQUEST TYPE	The requesting contracting authority selects the appropriate checkbox for the type of FSCIS request. Include the level of security clearance requested. The following abbreviations should be used: SECRET UE/EU SECRET = S-UE/EU-S CONFIDENTIEL UE/EU CONFIDENTIAL = C-UE/EU-C CIS = Communication and information systems for processing classified information
2. SUBJECT DETAILS	Fields 1 to 6 are self-evident. In field 4 the standard two-letter country code should be used. Field 5 is optional.
3. REASON FOR REQUEST	Give the specific reason for the request, provide project indicators, number of contract or invitation to tender. Please specify the need for storage capability, CIS classification level, etc. Any deadline/expiry/award dates which may have a bearing on the completion of an FSC should be included.
4. REQUESTING NSA/DSA	State the name of the actual requester (on behalf of the NSA/DSA) and the date of the request in number format (dd/mm/yyyy).
5. REPLY SECTION	Fields 1-5: select appropriate fields. Field 2: if an FSC is in progress, it is recommended to give the requester an

	indication of the required processing time (if known). Field 6: a) Although validation differs by country or even by facility, it is recommended that the expiry date of the FSC be given. b) In cases where the expiry date of the FSC assurance is indefinite, this field may be crossed out. c) The requester is responsible for applying for a renewal of the FSC.
6. REMARKS	May be used for additional information with regard to the FSC, the facility or the foregoing items.
7. ISSUING NSA/DSA	State the name of the providing authority (on behalf of the NSA/DSA) and the date of the reply in number format (dd/mm/yyyy).

FACILITY SECURITY CLEARANCE INFORMATION SHEET (FSCIS)

(MODEL)

All fields must be completed and the form communicated via Government-to-Government or Government-to-international organisation channels

REQUEST FOR A FACILITY SECURITY CLEARANCE ASSURANCE

TO: _____

(NSA/DSA Country name)

Please complete the reply boxes, where applicable:

[ ] Provide an FSC assurance at the level of: [ ] S-UE/EU-S [ ] C-UE/EU-C

for the facility listed below

[ ] Including safeguarding of classified material/information

[ ] Including Communication and Information Systems (CIS) for processing classified information

[ ] Initiate the process of obtaining an FSC up to and including the level of .....… with …….level of safeguarding and ……level of CIS, if the facility does not currently hold these levels of capabilities.

Confirm accuracy of the details of the facility listed below and provide corrections/additions as required.

1. Full facility name: Corrections/Additions:

…….. ……..…….

2. Full facility address:

…….. …….

3. Postal address(if different from 2)

…….. …….

4. Zip/post code/city/country

……... …….…….

5. Name of the Security Officer

…….....
...…….……..….

6. Telephone/Fax/E-mail of the Security Officer

…….. …….…….

7. This request is made for the following reason(s): (provide details of the pre-contractual stage, contract, subcontract, programme/project, etc.)

…….....……

Requesting NSA/DSA/EU contracting authority: Name: …… Date:(dd/mm/yyyy) ……

REPLY (within ten working days)

This is to certify that:

1. [ ] the abovementioned facility holds an FSC up to and including the level of [ ] S-UE/EU-S

[ ] C-UE/EU-C.

2. The abovementioned facility has the capability to safeguard classified information/material:

[ ] yes, level: ……. [ ] no.

3. the abovementioned facility has accredited/authorised CIS:

[ ] yes, level: ……. [ ] no.

4. [ ] in relation to the abovementioned request, the FSC process has been initiated. You will be informed

when the FSC has been established or refused.

5. [ ] the abovementioned facility does not hold an FSC.

6. This FSC assurance expires on: ……. (*dd/mm/yyyy*), or as advised otherwise by the NSA/DSA. In the case of earlier invalidation or any changes to the information listed above, you will be informed.

7. Remarks:

.....…….....……
…

Issuing NSA/DSA Name: …… Date:(dd/mm/yyyy)……

APPENDIX E

Minimum requirements for protection of EUCI in electronic form at RESTREINT UE/EU RESTRICTED level handled in the contractor's CIS

General

1. The contractor must be responsible for ensuring that the protection of RESTREINT UE/EU RESTRICTED classified information is in compliance with the minimum security requirements as stated within this security clause and any other additional requirements advised by the Contracting Authority or, if applicable, with the National Security Authority (NSA) or Designated Security Authority (DSA).

2. It is the responsibility of the contractor to implement the security requirements identified in this document.

3. For the purpose of this document a communication and information system (CIS) covers all equipment used to handle, store and transmit EUCI, including workstations, printers, copiers, fax, servers, network management system, network controllers and communications controllers, laptops, notebooks, tablet PCs, smart phones and removable storage devices like USB-sticks, CDs, SD-cards, etc.

4. Special equipment like cryptographic products must be protected in accordance with its dedicated Security Operating Procedures (SecOPs).

5. Contractors must establish a structure responsible for the security management of the CIS handling information classified RESTREINT UE/EU RESTRICTED and appoint a responsible Security Officer of the facility.

6. The use of privately-owned equipment of contractor’s personnel (hardware and software) or processing RESTREINT UE/EU RESTRICTED classified information is not permitted.

7. Accreditation of the contractor's CIS handling information classified RESTREINT UE/EU RESTRICTED must be approved by the Member State's Security Accreditation Authority (SAA) or delegated to the Security Officer of the contractor as permitted by national laws and regulations.

8. Only information classified RESTREINT UE/EU RESTRICTED encrypted using approved cryptographic products may be handled, stored or transmitted (wired or wireless) like any other unclassified information under the contract. These cryptographic products must be approved by the EU or a Member State.

9. External facilities involved in the maintenance/repair work must be obliged, on a contractual basis, to comply with the applicable provisions for handling of information classified RESTREINT UE/EU RESTRICTED as set out in this document.

10. At the request of the contracting authority or relevant NSA/DSA/SAA, the contractor must provide evidence of compliance with the Contract Security Clause. If also requested, contractors will permit an audit and inspection of the contractor's processes and facilities by representatives of the contracting authority, the NSA/DSA/SAA, or the relevant EU security authority in order to ensure compliance with these requirements.

Physical Security

11. Areas in which CIS are used to display, store, process or transmit RESTREINT UE/EU RESTRICTED information or areas housing servers, network management system, network controllers and communications controllers for such CIS should be established as separate and controlled areas with an appropriate access control system. Access to these separate and controlled areas should be limited to only specifically authorised persons. Without prejudice to paragraph 8 equipment as described in paragraph 3 has to be stored in such separate and controlled areas.

12. Security mechanisms and/or procedures must be implemented to regulate the introduction or connection of removable computer storage media (for example, USB, mass storage devices, CD-RWs) to components on the CIS.

Access to CIS

13. Access to contractor's CIS handling EUCI is based on a strict need to know principle and authorisation of personnel.

14. All CIS must have up to date lists of authorised users and an authentication of all users at the start of each processing session.

15. Passwords, which are part of most identification and authentication security measures must be a minimum of 9 characters long and must include numeric and "special" characters (if permitted by the system) as well as alphabetic characters. Passwords must be changed at least every 180 days. Passwords must be changed as soon as possible if they have or are suspected to have been compromised or disclosed to an unauthorised person.

16. All CIS must have internal access controls to prevent unauthorised users from accessing or modifying information classified RESTREINT UE/EU RESTRICTED and from modifying system and security controls. Users are to be automatically logged off the CIS if their terminals have been inactive for some predetermined period of time, or CIS must activate a password protected screen saver after 15 minutes of inactivity.

17. Each user of the CIS is allocated a unique user account and ID. User accounts will be automatically locked after at least 5 successive incorrect login attempts.

18. All users of the CIS must be made aware of their responsibilities and the procedures to be followed to protect information classified RESTREINT UE/EU RESTRICTED on the CIS. The responsibilities and procedures to be followed must be documented and acknowledged by users in writing.

19. Security Operating Procedures are available for the Users and Administrators and include security roles descriptions and associated list of tasks, instructions and plans.

Accounting, Audit and Incident Response

20. Any access to the CIS are logged.

21. The following events must be recorded:

    a) all log on attempts whether successful or failed;
    b) log off (including time out where applicable);
    c) creation, deletion or alteration of access rights and privileges; and
    d) creation, deletion or alteration of passwords.

22. For all of the events listed above at least the following information must be communicated:

    a) type of event;
    b) user ID;
    c) date and time; and
    d) device ID.

23. The accounting records should support the capability to be examined by a Security Officer for potential security incidents and that they can be used to support any legal investigations in the event of a security incident. All security records should be regularly checked to identify potential security incidents. The accounting records must be protected from unauthorised deletion or modification.

24. The contractor has established a response strategy to deal with security incidents. Users and Administrators are instructed how to react to incidents, how to report incidents and what to do in case of emergencies.

25. The compromise or suspected compromise of information classified RESTREINT UE/EU RESTRICTED must be reported to the Contracting Authority. The report must contain a description of the information involved and a description of the circumstances of the (suspected) compromise. All users of the CIS must be made aware of how to report any actual or suspected security incident to the Security Officer.

Networking & Interconnection

26. When a contractor CIS that handles information classified RESTREINT UE/EU RESTRICTED is interconnected to a CIS that is not accredited, this leads to a significant increase in threat to both the security of the CIS and the RESTREINT UE/EU RESTRICTED classified information handled by that CIS. This includes the internet, other public or private CIS such as other CIS owned by the contractor or its subcontractors. In this case, the contractor must perform a risk assessment to identify the additional security requirements that need to be implemented as part of the security accreditation process. The contractor will provide to the contracting authority and where nationally required, the competent SAA a statement of compliance certifying that the contractor CIS and respective interconnection have been accredited for handling EUCI at RESTREINT UE/EU RESTRICTED.

27. Remote access from others systems to LAN services (e.g., remote access to e-mail and remote SYSTEM support) are prohibited unless special security measures are implemented and agreed by the Contracting Authority and where nationally required, approved by the competent SAA.

Configuration Management

28. A detailed hardware and software configuration, as reflected in the accreditation/approval documentation (including system and network diagrams) is available and regularly maintained.

29. Configuration checks are carried out by the Security Officer of the Contractor on hardware and software to ensure that unauthorised hardware and software has not been introduced.

30. Changes to the contractor CIS configuration are assessed for their security implications and must be approved by the Security Officer and where nationally required, the SAA.

31. The system is scanned for the presence of security vulnerabilities at least quarterly. Software must be implemented allowing detection of malware. Such software must be kept up-to-date. If possible, the software should have a national or recognised international approval, otherwise it should be a widely accepted industry standard.

32. The contractor must develop a Business Continuity Plan. Back-up procedures are established addressing the following:

    a) frequency of back-ups;
    b) storage requirements on-site (fireproof containers) or off-site;
    c) control of authorised access to back-up copies.

Sanitisation and Destruction

33. For CIS or data storage media that at any time held RESTREINT UE/EU RESTRICTED classified information the following sanitisation must be performed to the entire system or storage media prior to its disposal:

    a) Random data in flash memory (e.g. USB sticks, SD cards, solid state drives, hybrid hard drives) must overwrite at least three times then verify storage content matches the random data or using approved deletion software;
    b) Magnetic media (e.g. hard disks) must be overwritten or degaussed;
    c) Optical media (e.g. CDs and DVDs) must be shredded or disintegrated; and
    d) concerning other storage media the contracting authority, or if appropriate the NSA/DSA/SAA, should be consulted for the security requirements that need to be met.

34. Information classified RESTREINT UE/EU RESTRICTED must be sanitised on any data storage media before it is given to an entity not authorised to access RESTREINT UE/EU RESTRICTED (e.g. for maintenance work).

ANNEX III

Facility and Personnel Security Clearance for contractors involving RESTREINT UE/EU RESTRICTED information and NSAs/DSAs requiring notification of the security provisions of classified contracts at RESTREINT UE/EU RESTRICTED level[12]

Member State	**FSC**		**Notification of contract/subcontract involving R-UE/EU-R information to NSA/DSA**		**PSC**	
	YES	**NO**	**YES**	**NO**	**YES**	**NO**
Belgium		**X**		**X**		**X**
Bulgaria		**X**		**X**		**X**
Czech Republic		**X**		**X**		**X**
Denmark	**X**		**X**		**X**	
Germany		**X**		**X**		**X**
Estonia	**X**		**X**			**X**
Ireland						
Greece	**X**			**X**	**X**	
Spain		**X**	**X**			**X**
France		**X**		**X**		**X**

[12] These national requirements for FSC/PSC and notifications for contracts involving RESTREINT UE/EU RESTRICTED classified information must not place additional obligations on other Member States or contractors under their jurisdiction.

Croatia		**X**	**X**			**X**
Italy		**X**	**X**			**X**
Cyprus		**X**	**X**			**X**
Latvia		**X**		**X**		**X**
Lithuania	**X**		**X**			**X**
Luxembourg	**X**				**X**	
Hungary		**X**		**X**		**X**
Malta		**X**		**X**		**X**
Netherlands	**X** (for defence-related contracts only)		**X** (for defence-related contracts only)			**X**
Austria						
Poland		**X**		**X**		**X**
Portugal		**X**		**X**		**X**
Romania		**X**		**X**		**X**
Slovenia	**X**		**X**			**X**
Slovakia	**X**		**X**			**X**
Finland		**X**		**X**		**X**

Sweden	**X** (for defence-related contracts only)		**X** (for defence-related contracts only)		**X** (for defence-related contracts only)	
United Kingdom		**X**		**X**		**X**

ANNEX IV

LIST OF NSA/DSA DEPARTMENTS RESPONSIBLE FOR HANDLING INDUSTRIAL SECURITY-RELATED PROCEDURES

BELGIUM

National Security Authority

FPS Foreign Affairs

Rue des Petits Carmes 15

1000 Brussels

Tel.: +32 25014542 (Secretariat)

Fax: +32 25014596

E-mail: nvo-ans@diplobel.fed.be

BULGARIA

1. State Commission on Information Security - National Security Authority

Cherkovna Str. 90

1505 Sofia

Bulgaria

Tel.: +3592 9333 600

Fax: +3592 9873 750

E-mail: dksi@government.bg

2. Military Information Service of the Ministry of Defence (Security Service)

3 Dyakon Ignatiy Str. the Secu

1092 Sofia

Bulgaria

Tel.: +3592 8551 042; +3592 9220 922; +3592 9227 526

E-mail: presscntr@md.government.bg

3. State Agency Intelligence (Security Service)

12 Haidushka Polyana Str.

1612 Sofia

Bulgaria

Tel.: +3592 9813 221

E-mail: headoffice@nrs.bg

4. State Agency for Technical Operations (Security Service)

29 Shesti Septemvri Str.

1000 Sofia

Bulgaria

Tel.: +3592 9877 121, +3592 9824 110

Conduct the vetting procedures for issuing FSC and PSC to legal entities and individuals that apply for concluding a classified contract or who fulfil a classified contract for the needs of these authorities.

5. State Agency 'National Security' (Security Service)

45 Cherni Vrah Blvd

1407 Sofia

Bulgaria

Tel.: +3592 8147 109; +3592 8147 108

Fax: +3592 9632 188; +3592 8147 441

E-mail: dans@dans.bg

Conducts the vetting procedures for issuing FSC and PSC to all other legal entities and individuals in the country that apply for concluding a classified contract or who fulfil a classified contract.

CZECH REPUBLIC

National Security Authority

Industrial Security Department

Ms Lenka Ivincova, Head of INDUSEC unit

Tel.: +420 257 283 388

E-mail: l.ivincova@nbu.cz

PO BOX 49

150 06 Praha 56

Czech Republic

DENMARK

1. Politiets Efterretningstjeneste

(Danish Security Intelligence Service)

Klausdalsbrovej 1

2860 Søborg

Tel.: +45 33148888

Fax: +45 33430190

2. Forsvarets Efterretningstjeneste

(Danish Defence Intelligence Service)

Kastellet 30

2100 Copenhagen Ø

Tel.: +45 33325566

Fax: +45 33931320

GERMANY

1. For industrial security policy matters, FSCs, Transportation Plans (except for crypto /CCI):

Federal Ministry of Economic Affairs and Energy

Industrial Security Division - ZB3

Villemombler Str. 76

53123 Bonn

Germany

E-mail: dsagermany-zb3@bmwi.bund.de (office e-mail address)

Tel.: +49 228 99615 4028

Fax: +49 228 99615 2676

2. For standard visit requests from/to German companies:

Federal Ministry of Economic Affairs and Energy

Industrial Security Division – ZB2

Villemombler Str. 76

53123 Bonn

Germany

Tel.: +49 228 99615 2401

Fax: +49 228 99615 2603

E-mail: zb2-international@bmwi.bund.de (office e-mail address)

3. Transportation Plans for crypto material:

Federal Office for Information Security (BSI)

National Distribution Agency/NDA-EU DEU

Mainzer Str. 84

53179 Bonn

Tel.: +49 (0)228 99 9582 6052

Fax: +49 (0)228 99 10 9582 6052

E-mail: NDAEU@bsi.bund.de

ESTONIA

National Security Authority Department

Estonian Information Board

Rahumäe tee 4B

11316 Tallinn

Tel.: +372 693 9211

Fax: +372 6935001

E-mail: nsa@teabeamet.ee

IRELAND

Ray Walker

National Security Authority

Department of Foreign Affairs and Trade

76-78 Harcourt Street

Dublin 2

Ireland

Official direct line: +353 1 4082123

Mobile phone: +353 87 829 1918

E-mail address: Raymond.Walker@dfa.ie

GREECE

POC Lieutenant Commander (Ltcdr) Spyridon Mexias, Hellenic Navy

Hellenic National Defence General Staff

F' Branch

Security & Counter-Intelligence Directorate

Industrial Security Office

Mesogeion Avenue 227-231

15561 Holargos, Athens Hellas

Tel.: +30 2106572022

Fax: +30 2106527612

E-mail: daa.industrial@hndgs.mil.gr

SPAIN

Autoridad Nacional de Seguridad

Oficina Nacional de Seguridad

Calle Argentona 2028023 Madrid

Tel.: +34 913725000

Fax: +34 913725808

E-mail: nsa-sp@areatec.com

asip@areatec.com

FRANCE

1. Secrétariat général de la défense et de la sécurité nationale

Sous-direction Protection du secret (SGDSN/PSD)

51 boulevard de la Tour-Maubourg

75700 Paris 07 SP

France

Tel.: +33 171758177

Fax: +33 171758200

2. DSA: Direction Générale de l'Armement

Service de la Sécurité de Défense et des systèmes d'Information (DGA/SSDI)

60 boulevard du général Martial Valin

CS 21623

75509 Paris CEDEX 15

France

Tel.: +33 9 8867 0418

E-mail: dga.fax-ssdi.fct@intradef.gouv.fr

CROATIA

Office of the National Security Council

Croatian NSA

Jurjevska 34

10000 Zagreb

Croatia

Tel.: +385 14681222

Fax: +385 14686049

www.uvns.hr

ITALY

Presidenza del Consiglio dei Ministri

D.I.S. - U.C.Se.

Via di Santa Susanna 15

00187 Roma

Tel.: +39 0661174266

Fax: +39 064885273

CYPRUS

ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ

ΣΤΡΑΤΙΩΤΙΚΟ ΕΠΙΤΕΛΕΙΟ ΤΟΥ ΥΠΟΥΡΓΟΥ

Εθνική Αρχή Ασφάλειας (ΕΑΑ)

Υπουργείο Άμυνας

Λεωφόρος Εμμανουήλ Ροΐδη 4

1432 Λευκωσία, Κύπρος

Τηλέφωνα: +357 22807569; +357 22807643; +357 22807764

Τηλεομοιότυπο: +357 22302351

Ministry of Defence

Minister's Military Staff

National Security Authority (NSA)

Industrial Security Department

Emanuel Roidi Street 4

1432 Nicosia

Tel.: +357 22807569; +357 22807669; +357 22807764

Fax: +357 22302351

E-mail: cynsa@mod.gov.cy

LATVIA

National Security Authority

Constitution Protection Bureau of the Republic of Latvia

P.O. Box 286

Riga LV-1001

Tel.: +371 67025418 or +371 67 025 463

Fax: +371 67025454

E-mail: ndi@sab.gov.lv or ndi@zd.gov.lv

LITHUANIA

Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija

(The Commission for Secrets Protection Coordination of the Republic of Lithuania

National Security Authority)

Gedimino 40/1

LT-01110 Vilnius

Tel.: +370 706 66 703, +370 706 66 701

Fax: +370 706 66 700

E-mail: nsa@vsd.lt

LUXEMBOURG

Autorité Nationale de Sécurité

POC: Mr Carlo Mreches

207, route d'Esch

L-1471 Luxembourg

Tel.: +352 24782210

E-mail: ans@me.etat.lu

HUNGARY

National Security Authority of Hungary

POC: Ms Erika Némethné Stadler

Szilágyi Erzsébet fasor 11/B

H-1024 Budapest

Tel.: +36 17952303

Fax: +36-1-795-0345

E-mail: nbf@nbf.hu

postal address: P.O. Box 314, H-1903 Budapest

MALTA

Francis Farrugia

Director

Designated Security Authority for Industrial Security

Standards & Metrology Institute

Malta Competition and Consumer Affairs Authority

Mizzi House,

National Road,

Blata I-Bajda HMR9010

Tel.:+356 2395 2000

Fax: +356 2124 2406

E-mail: francis.p.farrugia@mccaa.org.mt

NETHERLANDS

1. Ministry of the Interior and Kingdom Relations

PO Box 20010

2500 EA The Hague

Tel.: +31 703204400

Fax: +31 703200733

E-mail: nsa-nl-industry@minbzk.nl

2. Ministry of Defence

Industrial Security Department

PO Box 20701

2500 ES The Hague

Tel.: +31 704419407

Fax: +31 703459189

E-mail: indussec@mindef.nl

AUSTRIA

1. Federal Chancellery of Austria,

Department I/12, Office for Information Security

Ballhausplatz 2

1014 Vienna

Austria

Tel.: +43 1 53115 202594

E-mail: isk@bka.gv.at

2. DSA in the military sphere:

BMLVS/Abwehramt

Postfach 2000

1030 Vienna

Austria

E-mail: abwa@bmlvs.gv.at

POLAND

Internal Security Agency

Department for the Protection of Classified Information

Rakowiecka 2A

00-993 Warsaw

Tel: +48 22 58 57 944

Fax: +48 22 58 57 443

E-mail: nsa@abw.gov.pl

PORTUGAL

Gabinete Nacional de Segurança

Serviço de Segurança Industrial

Rua da Junqueira nº 69

1300-342 Lisbon

Tel.: +351 21 303 17 10

Fax: +351 21 303 17 11

E-mail: sind@gns.gov.pt; franco@gns.gov.pt

ROMANIA

Oficiul Registrului Național al Informațiilor Secrete de Stat

(Romanian NSA – ORNISS

National Registry Office for Classified Information)

PoC Prof. dr. Marius Petrescu

Secretary of State

Director General

Tel./Fax: +40 21 224 58 30

E-mail: relatii.publice@orniss.ro

Mr Ion Mihai

Head of Industrial Security and Access Control to Classified Information Department

Tel.: +40 21 20 75 133

Fax: +40 21 224 58 33

E-mail: relatii.publice@orniss.ro; ion.mihai@orniss.ro

Ms Monica Nidelea

Director of Industrial Security Agency

Tel.: +40 21 20 75 132

Fax: +40 21 224 58 33

E-mail: relatii.publice@orniss.ro; monica.nidelea@orniss.ro

SLOVENIA

Urad Vlade RS za varovanje tajnih podatkov

Tel.: +386 1 478 1390 Fax: +386 1 4781399

E-mail: gp.uvtp@gov.si

SLOVAKIA

Národný bezpečnostný úrad

(National Security Authority)

Security Clearance Department

Budatinska 30

850 07 Bratislava 57

Tel.: +421 2 6869 2627 (secretariat), +421 2 6869 2629

Fax: +421 2 6869 1706

E-mail: podatelna@nbusr.sk

FINLAND

National Security Authority

Ministry for Foreign Affairs

P.O. Box 453

FI-00023 Government

E-mail: NSA@formin.fi

E-mail: DSA@defmin.fi

SWEDEN

1. National Security Authority

Utrikesdepartementet (Ministry for Foreign Affairs)

UD SÄK

SE-103 39 Stockholm

Tel.: +46 84051000

Fax: +46 87231176

E-mail: ud-nsa@gov.se

2. DSA

Försvarets Materielverk (Swedish Defence Materiel Administration)

FMV Säkerhetsskydd

SE-115 88 Stockholm

Tel.: +46 8 782 40 00

Fax: +46 8 782 69 00

E-mail: registrator@fmv.se

UNITED KINGDOM

UK National Security Authority

Room 335, 3rd Floor

70 Whitehall

London

SW1A 2AS

Tel. 1: +44 2072765497

Tel. 2: +44 2072765645

Fax: +44 2072765651

E-mail: UK-NSA@cabinet-office.x.gsi.gov.uk

Projet de loi n°6961

portant

1. création de l'Autorité nationale de sécurité et

2. modification

1) de la loi modifiée du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité ;

2) du Code pénal.

Situation actuelle : loi modifiée du 15 juin 2004 relative à la classification des pieces et aux habilitations de sécurité

Elle determine les règles de base relatives :

- à la procedure de classification, de déclassement et de declassification des pieces;
- aux mesures de protection matérielle et physique des pièces;
- à l'émission d'habilitations de sécurité aux personnes appelées à avoir accès aux pièces classifies dans le cadre de l'exercice de leurs missions.

➢ **Elle s'applique seulement aux personnes physiques et morales appelées, de par leur fonctions, à avoir accès aux pièces classifiées.**

Situation actuelle : loi modifiée du 15 juin 2004 relative à la classification des pieces et aux habilitations de sécurité

Désuétude de certaines de ses dispositions :

- ne tient pas compte de la montée en puissance des systèmes d'informations dans l'élaboration, le traitement, la transmission et le stockage d'informations classifiées
- prise en compte insuffisante de l'utilisation croissante d'informations classifiées par le secteur privé
- le rôle de l'ANS doit être adapté face à l'accroissement du volume d'informations classifiées et à l'évolution technologique
- déphasé par rapport au cadre juridique international devenu plus contraignant et aux standards en matière de protection des pièces appliqués par nos partenaires

Situation actuelle : loi modifiée du 15 juin 2004 relative à la classification des pieces et aux habilitations de sécurité

Absence de dispositions détaillées en matière de protection de la vie privée :

- la loi de 2004 reste largement muette par rapport à l'ampleur de l'enquête de sécurité et
- en l'absence de dispositions nationales applicables l'ANS s'inspire largement du cadre de référence international pour effectuer les verifications requises en vue de la délivrance d'une habilitation de sécurité

Traitement des données :

- renvoi aux dispositions législatives nationales applicables en matière d'accès aux données personnelles et de protection de ces dernières

Cadre de référence international

- **UE** – decision 2013/488/UE du Conseil du 23 septembre 2013 : force de loi au Luxembourg depuis la loi du 18 juillet 2014 portant approbation de l'Accord entre les Etats membres de l'UE, réunis au Conseil, relatif à la protection des informations classifiées échangées dans l'intérêt de l'UE, signé à Bruxelles, le 25 mai 2011.

- **OTAN** – document C-M(2002)49 "La sécurité dans l'OTAN" et directive de sécurité n°1 "sécurité dans le domaine du personnel" : l'accord de sécurité a été approuvé par une loi du 15 juin 2004.

Cadre de référence international

- Harmonisation des critères et règles applicables en matière d'enquêtes de sécurité au niveau de l'UE et de l'OTAN.
- Il s'agit de standards minimaux que les Etats membres de l'UE et de l'OTAN s'engagent à accomplir pour garantir un même degré de protection des informations classifiées.
- Préoccupation partagée de veiller à la sécurité et à la protection des pièces classifiées, propriété légale d'organisations internationales ou d'Etats tiers, dont la circulation s'est accrue pour diverses raisons.
- Pour toutes ces raisons il est nécessaire que le Luxembourg s'aligne sur ce cadre de référence international.

Projet de loi n°6961

Objectif affiché :

- Renforcer la sécurité juridique de la protection des pièces classifiées nationales et internationals.
- Nécessité de préciser certains éléments du dispositif et notamment en ce qui concerne l'enquête de sécurité.
- Compléter le dispositif de protection des pièces classifiées, notamment à l'égard du secteur privé.
- Replacer l'ANS au coeur du dispositif de la protection des pièces classifiées en clarifiant son rôle et en complétant son autorité.
- Tenir compte du rôle grandissant des systèmes d'informations classifiées.
- Tenir compte des évolutions du cadre de référence international.

Projet de loi n°6961 – Enquête de sécurité

- Introduction du concept de “critères d’appréciation” (introduit par l’ancien article 21, devenant l’article 26 – définis par l’article 31)

- La procédure de l’enquête de sécurité est davantage détaillée (article 27)

- Les “critères d’appréciation” de l’article 31 découlent du cadre de référence de l’UE et de l’OTAN sans y ajouter de critère supplémentaire.

Projet de loi n°6961 – traitement des données

- Il n'est désormais plus seulement renvoyé à la loi SRE pour ce qui est de l'accès aux traitement de données – l'ancien article 22, devant l'article 28, détaille dorénavant cet accès.
- Les modalités de collecte de certaines données sont précisées (§2-§4 de l'article 28).
- L'accès à ces traitements de données est soumis à la surveillance de la CNPD.
- L'article 29 précise le traitement des données recueillies en application de la loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale.