Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense
et de la sécurité nationale

Direction Protection et Sécurité de l'Etat

Paris, le 12 JUIL. 2013
N° 2102/SGDSN/PSE/PSD

PRM	D	1	3	1	8	6	2	8	J

INSTRUCTION GÉNÉRALE INTERMINISTÉRIELLE N° 2102

SUR LA PROTECTION EN FRANCE DES INFORMATIONS CLASSIFIÉES DE L'UNION EUROPEENNE

SOMMAIRE

TITRE PREMIER : **3**

PRINCIPES ET ORGANISATION DE LA PROTECTION DES INFORMATIONS CLASSIFIÉES DE L'UNION EUROPEENNE **3**

CHAPITRE PREMIER : 3
PRINCIPES GÉNÉRAUX ET DÉFINITIONS 3
CHAPITRE II : 6
ORGANISATION DU SYSTÈME DE SÉCURITÉ DE L'UE 6
Section 1 : L'organisation de la sécurité au sein de l'UE *6*
Section 2 : L'organisation française *7*

TITRE II : **11**

MESURES DE SÉCURITÉ RELATIVES AUX PERSONNES AYANT VOCATION Á ACCÉDER AUX INFORMATIONS CLASSIFIÉES DE L'UNION EUROPEENNE **11**

CHAPITRE PREMIER : 11
L'ACCÈS AUX ICUE 11
CHAPITRE II : 12
SÉCURITÉ DU PERSONNEL : L'HABILITATION UE 12
CHAPITRE III : 14
LES CAS PARTICULIERS 14

TITRE III : **16**

MESURES DE SÉCURITÉ RELATIVES AUX INFORMATIONS CLASSIFIÉES DE L'UNION EUROPEENNE **16**

CHAPITRE PREMIER : 16
GESTION DES INFORMATIONS CLASSIFIÉES DE L'UNION EUROPÉENNE 16
Section 1 : Élaboration des informations classifiées *16*
Section 2 : Circulation des ICUE *17*
Section 3 : Gestion des ICUE *19*
CHAPITRE II : 21
LA COMPROMISSION D'INFORMATIONS CLASSIFIÉES DE L'UNION EUROPÉENNE 21
Section 1 : La compromission des ICUE *21*
Section 2 : Les sanctions *22*

TITRE IV : **23**

MESURES DE SÉCURITÉ RELATIVES A LA PROTECTION DES LIEUX DANS LESQUELS SONT CONSERVEES DES INFORMATIONS CLASSIFIEES DE L'UNION EUROPEENNE **23**

TITRE V : **25**

MESURES DE SÉCURITÉ RELATIVES AUX SYSTEMES D'INFORMATION **25**

CHAPITRE PREMIER 25
L'ORGANISATION DES RESPONSABILITÉS RELATIVES AUX SYSTÈMES D'INFORMATION 25
CHAPITRE II 28
LA PROTECTION DES SYSTÈMES D'INFORMATION 28

TITRE VI : **30**

LA PROTECTION DES INFORMATIONS CLASSIFIEES DE L'UE DANS LES CONTRATS **30**

GLOSSAIRE **33**

ANNEXES **35**

TITRE PREMIER :

PRINCIPES ET ORGANISATION DE LA PROTECTION DES INFORMATIONS CLASSIFIÉES DE L'UNION EUROPEENNE

→ La protection du secret UE concerne tous les domaines d'activité relevant de l'Union européenne (UE) : politique, militaire, diplomatique, scientifique, économique, industriel…
→ Sont classifiées les informations dont la divulgation est de nature à porter atteinte aux intérêts de l'UE ou à ceux d'un ou plusieurs de ses Etats membres ;
→ La protection des secrets de l'UE est assurée par une chaîne de responsabilité qui s'applique, de manière équivalente, aux niveaux européen et national, ainsi qu'aux domaines public et privé ;
→ Le Secrétariat général de la défense et de la sécurité nationale (SGDSN) tient, pour ce qui concerne la France, les fonctions d'autorité nationale de sécurité prévues par la réglementation de sécurité de l'UE ; il peut déléguer certaines de ses responsabilités.

Chapitre premier :

Principes généraux et définitions

ART. 1er : But de l'instruction

Aux termes de la Décision du Conseil n°2011/292/UE du 31 mars 2011[1] (ci-après dénommée « Décision 2011/292/UE ») et de l'Accord entre les Etats membres de l'Union européenne (UE) relatif à la protection des informations classifiées signé à Bruxelles le 4 mai 2011[2] (ci-après dénommé « Accord intergouvernemental »), les Etats membres prennent toutes les mesures appropriées, conformément à leurs dispositions législatives et réglementaires nationales respectives, pour que le niveau de protection accordé aux informations classifiées de l'UE (ICUE) soit équivalent à celui qui est accordé par la Décision 2011/292/UE.

La présente instruction a pour objet de définir les modalités particulières selon lesquelles est organisée la protection des ICUE dans le cadre de la réglementation française.

Les présentes dispositions ne font pas obstacle aux règles énoncées à l'article 346.1.a du Traité sur le fonctionnement de l'UE[3].

---

[1] Décision du Conseil 2011/292/UE du 31 mars 2011 concernant les règles de sécurité aux fins de la protection des ICUE.
[2] Accord entre les Etats membres de l'UE, réunis au sein du Conseil, relatif à la protection des informations classifiées échangées dans l'intérêt de l'UE (2011/C 202/05), signé le 4 mai 2011 et publié au *Journal officiel* de l'Union européenne le 8 juillet 2011.
[3] *« Aucun Etat membre n'est tenu de fournir des renseignements dont il estimerait la divulgation contraire aux intérêts essentiels de sa sécurité ».*

ART. 2 : Champ d'application

Les dispositions de la présente instruction sont applicables dans toutes les administrations centrales, tous les services déconcentrés de l'Etat et établissements publics nationaux placés sous l'autorité d'un ministre, dans toutes les entités, publiques ou privées, concernées par la protection et la sauvegarde des ICUE produites par ou confiées à la France, ainsi qu'à toute personne dépositaire, même à titre provisoire, d'une telle information, y compris dans le cadre de la passation et de l'exécution d'un contrat.

Les présentes dispositions doivent être connues de l'ensemble du personnel appelé à prendre connaissance, à acheminer ou à traiter toute ICUE.

Elles s'appliquent aux informations classifiées portant un marquage de classification de l'UE, tel que défini à l'article 4 de la présente instruction, confiées à la France ou produites par elle.

ART. 3 : Principes de sécurité de l'UE

Aux termes de la Décision 2011/292/UE et de l'Accord intergouvernemental, chaque Etat membre s'engage à assurer la sécurité des ICUE et veille à ce que ces informations ne soient pas :

- déclassées ou déclassifiées sans le consentement préalable écrit de l'autorité d'origine;
- utilisées à d'autres fins que celles qui sont fixées par l'autorité d'origine;
- divulguées à un pays tiers ou à une organisation internationale en l'absence d'un accord ou d'un arrangement approprié de protection des informations classifiées conclu entre l'UE et le pays tiers ou l'organisation internationale en question et sans le consentement préalable écrit de l'autorité d'origine.

ART. 4 : Typologie des classifications applicables aux informations de l'UE et tableau d'équivalence

Les niveaux de classification de l'UE, définis dans la Décision 2011/292/UE et l'Accord intergouvernemental, sont établis comme suit :

- TRÈS SECRET UE/EU TOP SECRET : ce niveau de classification s'applique aux informations et matériels dont la divulgation non autorisée pourrait causer un préjudice exceptionnellement grave aux intérêts de l'UE ou d'un ou de plusieurs de ses Etats membres ;
- SECRET UE/EU SECRET : ce niveau de classification s'applique aux informations et matériels dont la divulgation non autorisée pourrait nuire gravement aux intérêts essentiels de l'UE ou d'un ou de plusieurs de ses Etats membres ;
- CONFIDENTIEL UE/EU CONFIDENTIAL : ce niveau de classification s'applique aux informations et matériels dont la divulgation non autorisée pourrait nuire aux intérêts essentiels de l'UE ou d'un ou de plusieurs de ses Etats membres ;
- RESTREINT UE/EU RESTRICTED : cette classification s'applique aux informations et matériels dont la divulgation non autorisée pourrait être défavorable aux intérêts de l'UE ou d'un ou de plusieurs de ses Etats membres.

La présente instruction définit les mesures spécifiques qui s'appliquent aux ICUE par rapport aux informations classifiées nationales de niveau équivalent. En l'absence de dispositions spécifiques, les ICUE sont traitées conformément aux dispositions de l'IGI n°1300, suivant le tableau d'équivalence ci-après :

UE[4]	FRANCE
TRES SECRET UE/EU TOP SECRET	TRÈS SECRET DÉFENSE
SECRET UE/EU SECRET	SECRET DÉFENSE
CONFIDENTIEL UE/EU CONFIDENTIAL	CONFIDENTIEL DÉFENSE
RESTREINT UE/EU RESTRICTED	(1)

Nota (1) : La République française traite et protège les informations portant la mention de classification RESTREINT UE/EU RESTRICTED selon les règles de protection des informations ou supports portant la mention de protection Diffusion Restreinte, énoncées en annexe 3 de l'IGI n°1300.

Certaines informations non classifiées, dont la diffusion est interne aux Institutions et Etats membres de l'UE, portent la mention *LIMITE*. Cette mention indique que l'information ne doit pas être rendue publique. Les agents, titulaires ou non, de l'État sont tenus en ce qui les concerne au devoir général de discrétion professionnelle et doivent être avertis des règles afférentes à la manipulation de telles informations et des conséquences de toute négligence, conformément aux consignes relatives au traitement des documents internes du Conseil[5].

ART. 5 : Définitions

La présente instruction emploiera les expressions suivantes :

- ***Autorité nationale de sécurité (ANS)*** : Organisme gouvernemental chargé des relations avec les autres Etats et les structures internationales en matière d'habilitation de personnes et de protection des informations classifiées. En France, l'ANS est le secrétaire général de la défense et de la sécurité nationale.

- ***Autorité de sécurité désignée (ASD)*** : Conformément à l'article R.2311-10-1 du code de la défense, le SGDSN peut, en sa qualité d'ANS pour le secret de la défense nationale, nommer dans des domaines particuliers, notamment dans le domaine industriel, sur proposition du ou des ministres intéressés, une autorité de sécurité déléguée. Dans un cadre européen, cette autorité est plus particulièrement chargée de faire connaître aux entreprises privées ou publiques la politique de sécurité industrielle

[4] Les informations portant un marquage de classification EURATOM, tel que prévu par le Règlement n°3 du Conseil de la Communauté européenne de l'énergie atomique (CEEA) du 31 juillet 1958 (EURA-TRES SECRET, EURA-SECRET, EURA-CONFIDENTIEL et EURA-DIFFUSION RESTREINTE), reçoivent la même protection que les ICUE de niveau équivalent.
[5] Document n°1136/11 du 9 juin 2011.

de l'UE et de fournir des orientations et une aide pour sa mise en œuvre. Elle est alors nommée "autorité de sécurité désignée".

- ***Bureau d'ordre*** : Bureau créé au sein de chaque organisme ou service dans lequel des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau supérieur sont traitées. Il est chargé de veiller à ce que ces informations soient traitées conformément à la présente instruction.

- ***Information classifiée de l'UE*** (ICUE) : Toute information ou support classifié, tel que défini dans l'IGI n°1300, dont la divulgation non autorisée pourrait porter atteinte à des degrés divers aux intérêts de l'UE, ou à ceux d'un ou de plusieurs de ses Etats membres, et identifié comme tel par une classification de sécurité de l'UE.

- ***Sécurité industrielle de l'UE*** : La sécurité industrielle consiste à appliquer des mesures visant à assurer la protection des ICUE dès la phase de négociations précontractuelles ou de l'avis d'appel public à la concurrence et, par la suite, tout au long du cycle de vie des contrats classifiés. De tels contrats ne doivent pas concerner l'accès à des informations classifiées TRES SECRET UE/EU TOP SECRET.

- ***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.

Chapitre II :

Organisation du système de sécurité de l'UE

Section 1 : L'organisation de la sécurité au sein de l'UE

ART. 6 : Les Institutions et autres organes de l'UE

Afin de favoriser la mise en place d'un système global et cohérent, au sein de l'UE, en matière de protection des informations classifiées, les institutions de l'UE et les agences, organes ou organismes institués par elles (ci-après « Institutions et autres organes de l'UE ») se sont engagés à appliquer des normes équivalentes de sécurité.

Le Conseil, la Commission européenne, le Service européen pour l'action extérieure (SEAE) et le Parlement européen disposent néanmoins de leur propre organisation interne de sécurité et de leurs propres règles de sécurité[6].

---

[6] Il s'agit de la Décision du Conseil 2011/292/UE du 31 mars 2011 concernant les règles de sécurité aux fins de la protection des ICUE, de la Décision 2011/844/CE, CECA, Euratom du 29 novembre 2001 relative aux dispositions de la Commission en matière de sécurité, de la Décision 2011/C 304/05 du 15 juin 2011 sur les règles de sécurité pour le service européen pour l'action extérieure et de la Décision 2011/C 190/2 du 6 juin 2011 concernant les règles applicables au traitement des informations confidentielles par le Parlement européen.

Toutes les informations reçues des Institutions et autres organes de l'UE portant un marquage de classification de l'UE tel que défini à l'article 4 sont protégées conformément aux dispositions de la présente instruction.

ART. 7 : Les organisations nationales de sécurité UE

Chaque Etat membre de l'UE est dans l'obligation de protéger les ICUE et de mettre en place un système de sécurité adapté et efficace. A cet effet, il confie à une autorité nationale de sécurité (ANS) la responsabilité de la sécurité des ICUE ; ces autorités agissent de manière coordonnée.

Section 2 : L'organisation française

ART. 8 : L'autorité nationale de sécurité

En France, la fonction d'ANS est exercée, sous l'autorité du Premier ministre, par le Secrétaire général de la défense et de la sécurité nationale (SGDSN), conformément aux articles R.2311-10 et R.2311-11 du code de la défense.

En tant qu'ANS, le SGDSN :

- assure la sécurité des ICUE confiées à la France ou produites par elle, conformément aux dispositions adoptées en commun par les Etats membres ;
- organise le fonctionnement interne du réseau UE, notamment en prenant les décisions de création, de rattachement, de transfert ou de dissolution des bureaux d'ordre TS-UE ;
- mène ou fait effectuer des inspections périodiques afin de vérifier l'application pratique des mesures de protection des ICUE ;
- définit la procédure d'habilitation de sécurité à mettre en œuvre pour les ressortissants français appelés à connaître des ICUE ;
- veille à ce que tout le personnel national, de même que les ressortissants étrangers employés dans des entités publiques ou privées nationales, susceptibles d'avoir accès aux informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL et d'un niveau de classification supérieur, soient dûment habilités au niveau requis ;
- décide de l'admission au TRES SECRET UE/EU TOP SECRET du personnel ayant à connaître des informations de ce niveau ;
- se charge de l'établissement et de la gestion des décisions d'habilitation, quel que soit le niveau de confidentialité concerné, pour les personnes de nationalité française employées directement par des Institutions ou autres organes de l'UE ;

Par ailleurs, il a la faculté de soumettre aux autorités de sécurité des Institutions et autres organes de l'UE des propositions tendant à la modification des procédures de sécurité, ainsi que des questions impliquant une coordination entre les services de sécurité des États membres et les Institutions et autres organes de l'UE. Il participe aux différents comités de sécurité. Il bénéficie de l'expertise de l'ANSSI pour les questions relatives à la sécurité des systèmes d'information, et des autorités de sécurité désignées.

ART. 9 : Les ministres

Chaque ministre s'assure, dans le département dont il a la charge, de la mise en œuvre des dispositions relatives à la sécurité des ICUE détenus par tout service ou toute entité publique ou privée relevant de ses attributions. Il est assisté par un haut fonctionnaire de défense et de sécurité (HFDS).

Chaque ministre prend les décisions d'habilitation pour les niveaux SECRET UE/EU SECRET et CONFIDENTIEL UE/EU CONFIDENTIAL et peut déléguer cette compétence conformément aux dispositions du Titre I de l'IGI n°1300.

Pour l'exercice de leurs responsabilités en matière de défense et de sécurité, la Présidence de la République et le Premier Ministre disposent, respectivement, d'un correspondant de défense et de sécurité de la Présidence de la République (CDSPR) et d'un HFDS auprès du Premier Ministre.
Dans la suite de l'instruction, le terme HFDS sera utilisé de façon générique.

ART. 10 : Les autorités de sécurité désignées

En fonction des besoins, des autorités de sécurité désignées (ASD), responsables devant l'ANS, peuvent être mises en place pour mettre en œuvre la politique de protection des ICUE, dans le domaine industriel, en particulier dans le cadre d'un programme ou projet européen.

Les ASD sont notamment chargées du traitement des habilitations de personnes morales et physiques dans le cas d'entreprises exécutant des contrats classifiés de l'UE et sont autorisées à communiquer avec les autorités de sécurité étrangères.

La Direction générale de l'armement (DGA) du ministère de la défense est reconnue comme ASD pour les entreprises exécutant un contrat classifié de l'UE dans le domaine de la défense, y compris en phase précontractuelle.

Une ASD peut également être appelée à agir dans le domaine de la sécurité nationale et pour tout contrat classifié de l'UE dans le domaine de la sécurité.

ART. 11 : Le réseau UE

Le réseau UE, dont un organigramme réduit est reproduit en annexe, est l'organisation française de sécurité responsable du traitement des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau supérieur.

1. Organisation

Le réseau UE comprend :
- un Bureau central UE (ci-après « bureau central UE »);
- des bureaux TRES SECRET UE/EU TOP SECRET (ci-après « bureaux TS-UE »), principaux, isolés ou subordonnés, chargés du traitement des informations classifiées TRES SECRET UE/EU TOP SECRET ;

- des bureaux de protection des ICUE (ci-après « bureaux ICUE ») pour le traitement des informations classifiées SECRET UE/EU SECRET et CONFIDENTIEL UE/EU CONFIDENTIAL.

Le SGDSN, en tant qu'ANS, est responsable de l'organisation et du fonctionnement du réseau UE. Il fait office d'autorité centrale de réception et de diffusion des informations classifiées TRES SECRET UE/EU TOP SECRET tel que prévu par la Décision 2011/292/UE et dispose, pour l'accomplissement de sa mission, du bureau central UE.

Chaque ministère est chargé de proposer au SGDSN l'organisation des bureaux TS-UE et des bureaux ICUE qui relèvent de son autorité. Cette organisation peut prendre la forme d'un sous-réseau, constitué d'un bureau principal et de plusieurs bureaux subordonnés, selon le schéma présenté en Annexe I.

Les personnes qui mettent en œuvre le réseau UE peuvent être les mêmes que celles qui mettent en œuvre les réseaux de gestion des secrets de la défense nationale ou ceux de l'OTAN. Toutefois, le principe de cloisonnement exige que les ICUE soient détenues séparément et enregistrées sur des supports spécifiques.

2. Fonctionnement

Le fonctionnement interne du réseau UE français, notamment les décisions de création, de rattachement, de transfert, de changement d'appellation, de fusion ou de suppression de bureaux TS-UE, est organisé par le SGDSN en tant qu'ANS.

La demande de création d'un bureau TS-UE principal ou subordonné doit être adressée au bureau central UE et réunir les éléments suivants :
- la demande de création émise par le bureau d'ordre de niveau supérieur ;
- la demande de création émise par l'autorité de la structure d'accueil ;
- un catalogue des emplois ;
- une attestation de garanties matérielles de sécurité, établie au vu de l'avis technique délivré par les services enquêteurs[7]. Un modèle d'attestation de garanties matérielles de sécurité figure en annexe 2 ;
- une copie de l'avis technique de sécurité ;
- les notices 94A pour chacune des personnes appelées à exercer des fonctions au sein du bureau d'ordre, impliquant l'accès à des ICUE ;
- un état des signatures du chef du bureau, du suppléant et des personnels habilités à signer les accusés de réception. Un modèle d'état de signature figure en annexe 3.

La demande de dissolution d'un bureau TS-UE ou de fusion de différents bureaux TS-UE doit être justifiée par des éléments d'ordre géographique et/ou de gestion et de rationalisation. Sur proposition d'un chef de bureau TS-UE principal, le chef du Bureau central UE décide de la destination de l'ensemble des documents détenus jusqu'alors par le bureau dissous.
Les bureaux ICUE sont établis dans les conditions prévues par l'IGI n°1300 pour les bureaux de protection du secret. Ils sont obligatoirement rattachés au réseau UE par l'intermédiaire d'un bureau TS-UE principal ou subordonné, selon le schéma présenté en Annexe 1.

---

[7] Direction centrale du renseignement intérieur (DCRI), Direction de la protection de la sécurité et de la défense (DPSD) ou Direction générale de la sécurité extérieure (DGSE) le cas échéant.

La création et la dissolution des bureaux ICUE sont de la responsabilité des bureaux TS-UE principaux, qui en avisent systématiquement le bureau central UE.

S'il n'existe qu'un besoin de consultation occasionnel de documents classifiés de niveau CONFIDENTIEL UE/EU CONFIDENTIAL, ces documents peuvent être communiqués sans création d'un bureau d'ordre subordonné, sous réserve que les règles établies garantissent qu'ils resteront sous le contrôle d'un bureau d'ordre ICUE ou TS-UE, et sous réserve du respect de toutes les mesures de sécurité physique, conformément au titre IV de la présente instruction, et concernant le personnel.

3. Attributions générales des bureaux d'ordre

Le chef d'un bureau d'ordre est responsable de la sécurité des ICUE dans l'organisme auquel il appartient. Il est plus particulièrement chargé de la réception, la comptabilisation, la manipulation, la distribution et la destruction des informations classifiées TRÈS SECRET UE/EU TOP SECRET, SECRET UE/EU SECRET et CONFIDENTIEL UE/EU CONFIDENTIAL, à l'exclusion de celles comportant les mentions *CRYPTO* ou *CCI*[8], dont la gestion est définie au Titre V de la présente instruction.

Il est désigné par le chef de cet organisme, qui notifie cette décision au chef du Bureau central UE par la voie hiérarchique du réseau, et doit faire l'objet d'une décision d'habilitation en cours de validité. Il est assisté par un suppléant.
Il applique les règles de sécurité relatives au personnel, aux informations et aux lieux et veille à leur mise en œuvre effective.

Le chef du bureau central UE effectue le suivi de l'organigramme du réseau UE français, en liaison avec les chefs des bureaux TS-UE principaux. Il mène des inspections périodiques dans les bureaux d'ordre principaux et isolés du réseau et peut participer à l'inspection des sous-réseaux.

Le chef d'un bureau principal mène, ou fait mener, des inspections périodiques dans les bureaux d'ordre de son sous-réseau.
Chaque année, avant le 1er mars, il adresse au Bureau central UE un organigramme actualisé de son sous-réseau, comprenant l'ensemble des bureaux TS-UE subordonnés et des bureaux ICUE.

---

[8] *Cryptographic controlled item.*

TITRE II :

MESURES DE SÉCURITÉ RELATIVES AUX PERSONNES AYANT VOCATION Á ACCÉDER AUX INFORMATIONS CLASSIFIÉES DE L'UNION EUROPEENNE

→ Ne peuvent accéder aux ICUE que les personnes dûment habilitées (pour les informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau supérieur) et ayant le besoin d'en connaître ;
→ L'habilitation UE de sécurité du personnel est une procédure lourde, qui ne doit être engagée que lorsqu'elle est strictement nécessaire et conforme au catalogue des emplois ;
→ Les décisions relatives aux habilitations sont notifiées aux intéressés.

Chapitre premier :

L'accès aux ICUE

ART. 12 : Principes généraux

L'accès aux informations de niveaux TRES SECRET UE/EU TOP SECRET, SECRET UE/EU SECRET et CONFIDENTIEL UE/EU CONFIDENTIAL n'est autorisé qu'aux personnes :

- en possession de l'habilitation de sécurité du niveau UE correspondant ou supérieur ;
- et ayant besoin d'en connaître pour l'exercice de leurs fonctions ou l'accomplissement de leur mission.

Les décisions d'habilitation permettant l'accès aux ICUE sont distinctes de celles permettant l'accès aux informations classifiées du domaine national ; néanmoins, toute décision d'habilitation permettant l'accès aux informations classifiées du domaine national peut en soi, à défaut d'une habilitation spécifique et sous réserve du besoin d'en connaître, donner accès aux ICUE du niveau correspondant et des niveaux inférieurs, conformément au tableau d'équivalence de l'article 4 de la présente instruction. Une décision d'habilitation permettant l'accès aux ICUE ne donne pas accès aux informations classifiées du domaine national.

L'accès aux informations de niveau RESTREINT UE/EU RESTRICTED ne requiert pas d'habilitation de sécurité mais n'est autorisé qu'aux personnes ayant besoin d'en connaître pour l'exercice de leurs fonctions ou l'accomplissement de leur mission.

ART. 13 : Catalogues des emplois

L'autorité hiérarchique compétente assume, pour tout organisme ou service traitant d'ICUE, la pleine responsabilité de la désignation des fonctions ou emplois nécessitant l'accès à de telles informations.

Elle fait établir par son bureau d'ordre, pour les niveaux de classification TRÈS SECRET UE/EU TOP SECRET, SECRET UE/EU SECRET et CONFIDENTIEL UE/EU CONFIDENTIAL, un catalogue des emplois nécessitant la connaissance d'informations classifiées, dans les conditions prévues par l'IGI n°1300.

Elle s'efforce de limiter à ce qui est strictement nécessaire les demandes d'habilitation qui en résultent.

Chaque bureau TS-UE principal adresse le catalogue des emplois de son sous-réseau aux niveaux TRÈS SECRET UE/EU TOP SECRET au SGDSN/PSE/PSD.

Chapitre II :

Sécurité du personnel : l'habilitation UE

ART. 14 : Procédure d'habilitation

Le dossier d'habilitation est constitué et instruit selon les modalités définies dans l'IGI n°1300 pour les habilitations nationales de niveau équivalent.

Chaque bureau d'ordre principal adresse les dossiers d'habilitation des personnels relevant de son sous-réseau à l'autorité d'habilitation compétente (SGDSN pour le niveau TRES SECRET UE/EU TOP SECRET, ministre concerné (ou son délégataire) pour les niveaux inférieurs). L'autorité d'habilitation, après avoir vérifié que le dossier est complet, saisit pour enquête les services compétents, conformément aux dispositions de l'IGI n°1300.

ART. 15 : Modalités de délivrance des décisions d'habilitation

Les décisions d'habilitation sont liées au catalogue des emplois. Elles sont notifiées et délivrées dans les conditions prévues par l'IGI n°1300 et selon les équivalences définies à l'article 4 de la présente instruction.

Les décisions d'habilitation permettant l'accès aux informations TRES SECRET UE/EU TOP SECRET sont matérialisées par la délivrance d'un document revêtu du « *cachet sec* » de la sous-direction Protection du secret du SGDSN. Ces décisions sont transmises aux bureaux d'ordre TS-UE.

Pendant leur durée de validité, les décisions d'habilitation sont conservées par le bureau d'ordre du service employeur ou, le cas échéant, peuvent être centralisées par les services du HFDS. Elles ne sont pas remises aux intéressés. Le bureau d'ordre compétent peut cependant être amené, en cas de nécessité, à leur délivrer un certificat de sécurité délivré pour une mission déterminée et une période limitée, dans les conditions prévues par l'IGI n°1300.

Les experts nationaux détachés auprès des Institutions et autres organes de l'UE pour occuper un poste nécessitant une habilitation UE de sécurité doivent présenter à l'autorité de sécurité de l'Institution ou organe concerné, avant de prendre leurs fonctions, un certificat de sécurité leur donnant accès aux ICUE.

ART. 16 : Répertoire des habilitations

Le SGDSN tient à jour le répertoire central des habilitations de niveau TRÈS SECRET UE/EU TOP SECRET.

Dans chaque département ministériel, il est tenu pour chaque niveau un répertoire :

- Des dossiers d'habilitation UE en cours d'instruction ;
- Des habilitations UE en cours de validité.

Pour permettre au SGDSN d'évaluer le nombre total d'habilitations UE délivrées et de personnes ayant accès aux ICUE, le HFDS de chaque ministère lui adresse chaque année, dans le cadre du rapport annuel d'évaluation prévu par l'IGI n°1300, un état des personnes relevant de son département ministériel habilitées aux niveaux SECRET UE/EU SECRET et CONFIDENTIEL UE/EU CONFIDENTIAL.

ART. 17 : Fin de l'habilitation

Les décisions de refus, de renouvellement et de retrait d'habilitation sont prises dans les conditions prévues par l'IGI n°1300 pour les habilitations nationales de niveau équivalent.

Tout retrait d'habilitation concernant une personne détachée auprès d'une Institution ou organe de l'UE ou directement employée par celui-ci doit être notifié à cette Institution ou organe par l'ANS.

ART. 18: Sensibilisation et instruction du personnel en matière de sécurité

Toute personne ayant accès à des ICUE fait l'objet d'une instruction de base, dispensée par le bureau d'ordre compétent, qui a pour but, non seulement de lui donner une connaissance des règles de sécurité, mais encore de lui faire comprendre que ces documents sont toujours l'objet de recherches sous des formes variées contre lesquelles il faut se prémunir. Les intéressés doivent notamment être informés sur les dangers que présentent, pour la sécurité, les conversations indiscrètes avec des personnes n'ayant pas besoin d'en connaître, les relations avec les médias et les activités des services de renseignement ayant pris pour cible l'UE et ses Etats membres.

Les personnes ayant fait l'objet d'une décision d'habilitation permettant l'accès aux ICUE doivent être instruites périodiquement des règles de sécurité en vigueur au sein de l'UE et des conséquences que peut entraîner leur violation.

Le bureau d'ordre de chaque organisme est, en outre, chargé de l'organisation de l'instruction permanente, en matière de sécurité, des personnes habilitées lors de leur entrée en fonction, puis à intervalles réguliers et à chaque renouvellement de l'habilitation.

Chapitre III :

Les cas particuliers

ART.19 : L'habilitation provisoire

En cas d'urgence, lorsque cela est dûment justifié dans l'intérêt du service et sous réserve des résultats des vérifications préliminaires pour s'assurer de l'absence d'informations défavorables, une habilitation provisoire peut être accordée pour une période ne dépassant pas six mois.
Cette habilitation provisoire est accordée dans les conditions prévues par l'IGI n°1300 pour la procédure d'urgence.
La décision d'habilitation provisoire est notifiée à l'intéressé qui signe un engagement de responsabilité.

ART 20 : L'habilitation des ressortissants étrangers

1. L'habilitation des ressortissants d'un Etat membre de l'UE

Les ressortissants d'un Etat membre de l'UE occupant un emploi en France peuvent avoir accès aux ICUE jusqu'au niveau TRES SECRET UE/EU TOP SECRET dans les mêmes conditions que les ressortissants nationaux et selon la procédure relative à l'habilitation des ressortissants étrangers définie dans l'IGI n°1300.

La procédure d'habilitation est engagée par le ministre concerné, son délégataire ou l'ASD, pour les niveaux CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET, et par le SGDSN pour le niveau TRES SECRET UE/EU TOP SECRET. La décision est prise par la même autorité. Le SGDSN, en sa qualité d'ANS, assure la liaison avec les ANS étrangères pour obtenir les éléments permettant l'instruction du dossier d'habilitation de l'intéressé. Le SGDSN peut autoriser des échanges directs entre les ASD et leurs homologues étrangers.

2. L'habilitation des ressortissants d'Etats non membres de l'UE

Les ressortissants de pays non membres de l'UE occupant un emploi en France peuvent accéder à des ICUE dès lors que les éléments suivants sont réunis :

- la réalisation d'un programme, d'un projet, d'un contrat, d'une opération ou d'une tâche liés à l'UE justifie leur besoin d'en connaître ;
- une habilitation UE de sécurité a été délivrée aux intéressés selon la procédure relative à l'habilitation des ressortissants étrangers définie dans l'IGI n°1300, à moins qu'il ne s'agisse d'informations de niveau RESTREINT UE/EU RESTRICTED ;
- le consentement préalable écrit de l'autorité dont émanent les ICUE a été obtenu.

Aucune habilitation ne doit être délivrée en l'absence d'un accord de sécurité entre la France et l'Etat dont l'intéressé est ressortissant, sauf cas exceptionnel prévu par l'IGI n°1300.

ART. 21: Moyens d'accès des magistrats aux ICUE

Le dispositif défini au Titre III de l'IGI n°1300 fixant les conditions dans lesquelles un magistrat peut accéder à une information classifiée dans le cadre de ses investigations s'applique exclusivement aux informations classifiées nationales.

Aussi, pour obtenir communication d'ICUE intéressant la procédure qu'il diligente, le magistrat doit en demander la déclassification à l'autorité étrangère ou à l'organisme international ayant procédé à la classification. Il peut, s'il le souhaite, s'informer des procédures auprès du SGDSN, en tant qu'ANS.

TITRE III :

MESURES DE SÉCURITÉ RELATIVES AUX INFORMATIONS CLASSIFIÉES DE L'UNION EUROPEENNE

→ La décision de classifier une information de l'UE a pour objectif de restreindre leur accès aux personnes préalablement habilitées (pour les informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau supérieur) et justifiant du besoin d'en connaître ;
→ Cette décision doit être précédée d'une appréciation rigoureuse de son opportunité ;
→ Elle place cette ICUE sous la protection de dispositions pénales spécifiques ;
→ La compromission peut résulter d'un acte de malveillance comme d'une simple négligence.

Chapitre premier :

Gestion des informations classifiées de l'Union européenne

Section 1 : Élaboration des informations classifiées

ART 22 : Généralités

D'une manière générale, lorsqu'une information classifiée destinée à l'UE est produite par une entité française, le document porte l'une des mentions de classification UE définies à l'article 4 de la présente instruction et est établi et enregistré conformément à la présente instruction.

Dans l'hypothèse où certains exemplaires d'un document national sont destinés à l'UE :
- le document est établi et enregistré conformément à la réglementation nationale,
- les exemplaires adressés à l'UE comportent, en plus du marquage national de sécurité, l'identification UE équivalente, conformément au tableau d'équivalence établi à l'article 4 de la présente instruction.

ART. 23 : Responsabilité de la décision de classification, de déclassement ou de déclassification

Les règles de classification des ICUE répondent aux mêmes impératifs que celles des documents nationaux.
La responsabilité du choix de classification incombe à l'autorité d'origine après évaluation aussi précise que possible de la sensibilité de l'information. La révision du besoin et du

niveau de classification des ICUE doit être effectuée rigoureusement selon une périodicité inférieure ou égale à dix (10) ans.

Une ICUE ne peut en aucun cas être déclassée ou déclassifiée sans le consentement préalable écrit de l'autorité d'origine.

ART. 24 : Identification de la classification UE et marquage

Le marquage des ICUE est effectué dans les conditions prévues par l'IGI n° 1300 pour les informations classifiées nationales.

Outre les mentions de classification prévues à l'article 4 de la présente instruction, les ICUE peuvent porter des marquages complémentaires destinés à préciser l'autorité d'origine, à limiter le champ de diffusion, ou à indiquer, le cas échéant, la date ou l'évènement particulier à partir desquels elles peuvent être déclassées ou déclassifiées.

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 classification en toutes lettres. Les abréviations admises sont les suivantes :

- TRES 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

ART. 25 : Enregistrement des ICUE

Les informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau de classification supérieur sont enregistrées par chaque bureau d'ordre dans un système d'enregistrement dédié avant leur diffusion et lors de leur réception, dans les conditions prévues par l'IGI n°1300 pour l'enregistrement des informations classifiées nationales. L'enregistrement doit permettre de garder la trace du cycle de vie d'une information classifiée, y compris de sa diffusion et de sa destruction.

La mention de l'objet du document, si cet objet est lui-même classifié, ne doit pas figurer dans le système d'enregistrement, à moins que ce système ne soit classifié. Cette obligation de classifier le système d'enregistrement lui-même s'impose aux niveaux SECRET UE/EU SECRET et TRES SECRET UE/EU TOP SECRET.

Section 2 : Circulation des ICUE

ART. 26 : Principes généraux de l'acheminement

L'acheminement des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL et d'un niveau de classification supérieur s'opère de bureau d'ordre à bureau d'ordre.

Les informations de niveau RESTREINT UE/EU RESTRICTED ne sont pas comptabilisées dans le réseau UE. Leur acheminement sur le territoire national ou vers l'étranger obéit aux règles de protection des documents marqués « *diffusion restreinte* » au niveau national, telles qu'énoncées à l'annexe 3 de l'IGI n°1300.

1. Acheminement des informations TRES SECRET UE/EU TOP SECRET

Le Bureau central UE est l'autorité centrale de réception et de diffusion des informations classifiées TRES SECRET UE/EU TOP SECRET entrant ou sortant du réseau français. Pour ce faire, il s'appuie sur le bureau TS-UE principal du SGDSN.

Exceptionnellement, et sous réserve de l'autorisation préalable écrite du Bureau central UE, une information TRES SECRET UE/EU TOP SECRET entrant ou sortant du réseau français peut passer par un bureau TS-UE principal ou isolé. Le cas échéant, un compte-rendu de prise en compte ou de transmission doit immédiatement être transmis au Bureau central UE.

A l'intérieur du réseau français, une information TRES SECRET UE/EU TOP SECRET circulant entre deux bureaux TS-UE principaux ou isolés doit faire l'objet d'un compte-rendu adressé au bureau central UE.

Une information TRES SECRET UE/EU TOP SECRET entrant dans un sous-réseau ou en sortant doit passer par le bureau TS-UE principal de ce sous-réseau ; une information circulant entre deux bureaux TS-UE subordonnés d'un même sous-réseau doit passer par l'intermédiaire du bureau TS-UE principal de rattachement.

2. Acheminement des informations SECRET UE/EU SECRET et CONFIDENTIEL UE/EU CONFIDENTIAL

L'acheminement des informations SECRET UE/EU SECRET et CONFIDENTIEL UE/EU CONFIDENTIAL sur le territoire national et depuis ou vers l'étranger relève de la responsabilité du bureau d'ordre expéditeur.

Avant toute expédition d'une ICUE, le bureau d'ordre expéditeur s'assure auprès de son bureau d'ordre principal de rattachement que la structure destinataire dispose d'un bureau d'ordre du réseau UE, qui est seul autorisé à réceptionner le document et à le transmettre au destinataire.

Toute information SECRET UE/EU SECRET entrant ou sortant d'un sous-réseau doit faire l'objet d'un compte-rendu adressé au bureau d'ordre principal de rattachement. Ce compte-rendu peut prendre la forme d'une mise à jour de l'inventaire annuel prévu à l'article 30 de la présente instruction.

ART. 27 : Modalités de diffusion, d'expédition et d'acheminement des ICUE

La diffusion, l'expédition et l'acheminement des informations ou matériels classifiés de l'UE, sur le territoire national et depuis ou vers l'étranger, sont effectués dans les conditions prévues par l'IGI n°1300 pour les informations nationales de niveau équivalent.

Aucune ICUE ne peut être communiquée à un Etat tiers à l'UE ou à une organisation internationale en l'absence d'un accord ou arrangement de sécurité entre l'UE et l'Etat tiers ou organisation internationale en question et sans le consentement préalable écrit de l'autorité d'origine.

Section 3 : Gestion des ICUE

ART. 28 : Conditions matérielles de conservation

En dehors des périodes d'utilisation, les documents classifiés de l'UE sont conservés dans des coffres-forts, des armoires-fortes ou chambres fortes selon les normes et les conditions fixées dans l'IGI n°1300 pour les informations classifiées nationales de niveau équivalent.

Afin de respecter le principe du besoin d'en connaître, les documents classifiés de l'UE sont conservés de manière distincte et séparée sans qu'il puisse y avoir ni confusion ni amalgame avec d'autres informations classifiées d'origines nationales et/ou étrangères différentes. Un tel cloisonnement doit permettre d'empêcher l'accès aux documents classifiés de l'UE à une personne n'ayant pas l'habilitation requise ou n'ayant pas le besoin d'en connaître. Cette mesure peut nécessiter l'emploi d'armoires fortes ou de coffres distincts ou l'utilisation de meubles de sécurité à compartiments différents.

La conservation des documents classifiés SECRET UE/EU SECRET et TRES SECRET UE/EU TOP SECRET doit être centralisée par chaque bureau d'ordre afin de faciliter la mise en œuvre des mesures de protection. De manière exceptionnelle, les documents classifiés SECRET UE/EU SECRET peuvent être détenus en dehors d'un bureau d'ordre, à condition que les mesures de sécurité physique soient conformes aux exigences définies au Titre IV de la présente instruction, et sous réserve du strict respect du principe de cloisonnement des informations.

ART. 29 : Reproduction et traduction

Chaque autorité responsable doit être consciente que la généralisation et la diversité des moyens de reproduction accroissent les risques de diffusion incontrôlée des documents classifiés de l'UE.

Les documents classifiées TRES SECRET UE/EU TOP SECRET ne doivent pas être dupliqués ou traduits sans le consentement écrit préalable de l'autorité d'origine.
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, dans le strict respect du principe du besoin d'en connaître. Si l'autorité d'origine veut impérativement en garder le contrôle exclusif, en particulier au niveau SECRET UE/EU SECRET, la mention suivante peut être apposée sur le document : « *La reproduction totale ou partielle du présent document est interdite, sauf autorisation préalable de l'autorité d'origine* ».

Les mesures de sécurité applicables au document original le sont aussi à ses copies et à ses traductions. Pour les documents classifiés CONFIDENTIEL UE/EU CONFIDENTIAL ou

d'un niveau supérieur, le nombre et les destinataires des exemplaires reproduits ou traduits doivent être dûment consignés dans le système d'enregistrement visé à l'article 25.

ART. 30 : Procédure d'inventaire

L'établissement d'un inventaire des ICUE obéit à des règles différentes selon le niveau de classification de ces documents.

1. Documents TRÈS SECRET UE/EU TOP SECRET

Chaque bureau d'ordre TS-UE procède, tous les ans, à l'inventaire physique de tous les documents TRÈS SECRET UE/EU TOP SECRET qu'il détient réellement. Un inventaire est effectué également sous forme contradictoire à chaque mutation de personnel du bureau d'ordre, l'ancien détenteur et le nouveau apposant tous deux leur signature sur le procès-verbal.

Un document est considéré comme inventorié si le bureau d'ordre s'est assuré de la présence :
- du document lui-même, dont la pagination doit être vérifiée après chaque mise à jour et changement de détenteur ;
- ou d'un récépissé de transmission à un autre bureau d'ordre TS-UE ;
- ou d'un procès-verbal de destruction ;
- ou d'un ordre de déclassement ou déclassification.

Les bureaux TS-UE subordonnés adressent leurs inventaires de documents TRÈS SECRET UE/EU TOP SECRET à leur bureau TS-UE principal de rattachement.

Les résultats des inventaires annuels détaillés doivent parvenir au bureau central UE, et ce au plus tard le 1er mars de chaque année, terme de rigueur, pour l'année précédente.

2. Documents SECRET UE/EU SECRET

Cet inventaire est fait à l'échelon du bureau TS-UE principal selon une procédure analogue à celle des documents TRÈS SECRET UE/EU TOP SECRET.

Seul le total numérique des documents SECRET UE/EU SECRET réellement détenus par les bureaux d'ordre, classés par bureaux d'ordre de rattachement au bureau TS-UE principal, sera transmis annuellement au bureau central UE, au plus tard le 1er mars de chaque année pour l'année précédente.

3. Documents CONFIDENTIEL UE/EU CONFIDENTIAL

Un inventaire des documents CONFIDENTIEL UE/EU CONFIDENTIAL est effectué annuellement par chaque bureau d'ordre du réseau UE.

ART. 31 : Destruction et archivage des ICUE

Lorsque des ICUE sont périmées ou devenues inutiles, il peut être procédé à leur destruction, dans les conditions prévues par l'IGI n°1300 pour les informations classifiées nationales et avec, pour le document original, l'accord de l'administration des archives.

La destruction des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL et d'un niveau de classification supérieur est effectuée sous la responsabilité du bureau d'ordre compétent, en présence d'un témoin habilité au niveau requis et fait l'objet d'un procès-verbal de destruction.
Les procès-verbaux de destruction des documents TRES SECRET UE/EU TOP SECRET sont conservés pendant une période de dix (10) ans au minimum, ceux des documents CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET pendant cinq (5) ans au minimum.
La destruction des informations RESTREINT UE/EU RESTRICTED ne fait pas l'objet de procès-verbal de destruction.

Chaque bureau d'ordre établit un plan d'évacuation et de destruction d'urgence des ICUE détenues, dans les conditions prévues par l'IGI n°1300 pour les informations classifiées nationales.

Le versement des ICUE aux archives se fait dans les conditions prévues par l'IGI n°1300 pour les informations classifiées nationales.

Chapitre II :

La compromission d'informations classifiées de l'Union européenne

Section 1 : La compromission des ICUE

ART. 32 : Compromission

Les atteintes au secret de la défense nationale définies aux articles 413-10 à 413-12 du code pénal constituent le délit de compromission.

En application de l'article 414-9 du code pénal, les dispositions des articles 411-6 à 411-11 relatives à la livraison d'informations à une puissance étrangère et des articles 413-9 à 413-12 du code pénal relatives aux atteintes au secret de la défense nationale sont applicables aux informations échangées entre la France et une institution ou un organe de l'Union européenne et classifiées en vertu des règlements de sécurité de ces derniers qui ont fait l'objet d'une publication au Journal officiel de l'Union européenne.

ART. 33 : Procédure à suivre en cas de compromission supposée ou avérée

Il est rendu compte immédiatement de toute découverte de compromission possible d'ICUE à l'autorité hiérarchique et au responsable du bureau d'ordre de l'organisme concerné. Ce dernier en informe directement et dans les plus brefs délais les autorités compétentes, dans les conditions prévues par l'IGI n°1300.

L'ANS est seule habilitée à porter l'incident à la connaissance de l'autorité de sécurité européenne concernée.

Section 2 : Les sanctions

ART. 34 : Les sanctions pénales

Conformément au tableau d'équivalence défini à l'article 4 de la présente instruction, les atteintes aux informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL et de niveau supérieur sont réprimées dans les conditions prévues aux articles 413-10 et 413-11 du Code pénal[9].

ART. 35 : Les sanctions disciplinaires

Outre les sanctions pénales, l'auteur d'un acte, commis délibérément ou non, qui compromet un secret de l'UE encourt le retrait de son habilitation et des sanctions disciplinaires ou professionnelles[10].

---

[9] Lorsqu'elles sont commises en temps de guerre, les atteintes au secret de la défense nationale sont punies dans les conditions prévues à l'article L332-2 du Code de justice militaire.

[10] Article L.4121-2 du code de la défense pour les militaires, article 26 de la loi 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires et article 1.1 du décret n°86-83 du 17 janvier 1986 pour les agents non titulaires de l'Etat.

TITRE IV :

MESURES DE SÉCURITÉ RELATIVES A LA PROTECTION DES LIEUX DANS LESQUELS SONT CONSERVEES DES INFORMATIONS CLASSIFIEES DE L'UNION EUROPEENNE

→ Les mesures de protection physique appliquées à une information de l'UE dépendent de son niveau de classification ;
→ Tout système de protection physique doit s'appuyer sur une analyse des risques ;
→Un dispositif de protection est satisfaisant lorsqu'il retarde suffisamment l'intrusion pour permettre la mise en œuvre des moyens d'intervention avant que les ICUE ne soient compromises ;
→ Les contrôles élémentaires de personnes physiques ou morales sont prévus pour l'exécution de contrats sensibles – le recours aux gardes notamment – dans des lieux dans lesquels sont conservées des ICUE.

ART. 36 : Les modalités matérielles de protection

Les informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau supérieur doivent être traitées et conservées dans les conditions prévues au Titre IV de l'IGI n°1300 pour les informations classifiées nationales de niveau équivalent.

Les informations classifiées de niveau RESTREINT UE/EU RESTRICTED sont conservées dans un meuble de bureau fermant à clés, dans une zone délimitée de façon visible, permettant de contrôler les personnes et les véhicules et où des mesures d'accompagnement des visiteurs sont prises.

ART. 37 : La protection des réunions de travail et des salles de conférence

Les mesures de protection des salles de réunion et de conférence dans lesquelles peuvent être échangées des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau supérieur doivent répondre aux exigences prévues par l'IGI n°1300 pour les informations classifiées nationales de niveau équivalent.
En particulier, l'autorité organisatrice doit veiller à ce que le local prévu à cet effet :

- soit à l'abri des interceptions par écoute directe ou indirecte et des prises de vue non autorisées ;
- ne soit accessible qu'aux personnes autorisées ;
- fasse l'objet de contrôles techniques réguliers par le service chargé de la sécurité.

ART. 38 : Accès des personnes non qualifiées

L'accès des personnes non qualifiées, c'est-à-dire non titulaires de l'habilitation appropriée ou n'ayant pas le besoin d'en connaître, à des lieux dans lesquels sont conservées des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau

supérieur, que ce soit dans le cadre d'une prestation de service, d'une intervention d'urgence ou d'une mission de contrôle, est autorisé dans les conditions prévues par l'IGI n°1300.

En particulier, le convoyage d'ICUE, le gardiennage des lieux dans lesquels sont conservées des ICUE et l'entretien ou la maintenance dans de tels lieux font l'objet d'un contrat sensible au sens de l'IGI n°1300. Ont seules le droit d'exécuter ce contrat les personnes appartenant à l'entreprise concernée qui ont fait l'objet au préalable d'un contrôle élémentaire tel que défini dans l'IGI n°1300. Les contrats de travail des personnes exécutant un contrat sensible comportent une clause de protection du secret.

TITRE V :

MESURES DE SÉCURITÉ RELATIVES AUX SYSTEMES D'INFORMATION

→ Le SGDSN met en œuvre la politique d'assurance de l'information (ou SSI[11]) de l'UE ;
→ L'ANSSI exerce les fonctions d'autorité nationale chargée de l'assurance de l'information, d'autorité nationale d'homologation de sécurité, d'autorité d'agrément cryptographique;
→ Les systèmes d'information traitant d'ICUE déployés dans une entité française et mis en œuvre par l'UE ou spécifiquement déployés entre Etats membres dans le cadre d'un programme européen sont régis par les politiques de sécurité de l'UE et le cas échéant par les instructions de sécurité du programme ;
→ Les principaux textes de référence de l'UE imposant une adaptation des exigences nationales sont accessibles auprès de l'ANSSI, sous réserve de satisfaire aux exigences de sécurité et du besoin d'en connaître ;
→ Outre les règles de la présente instruction, il convient de prendre en compte les instructions spécifiques détaillées d'application émises par l'UE en matière de sécurité des systèmes d'information, en particulier :
- Annexe IV de la Décision 2011/292/UE ;
- TECH-P-02-01 Policy on computers and LAN;
- TECH-P-05 Interconnection of CIS;
- TECH-P-02-03 Policy on Protective Monitoring;
- TECH-G-01-04 General Security Governance Requirements for CIS processing RESTREINT UE.

ART. 39 : Champ d'application

Les mesures définies dans la présente instruction sont applicables à tout système d'information national ayant vocation à traiter des ICUE.

Chapitre premier

L'organisation des responsabilités relatives aux systèmes d'information

ART. 40 : Les instances interministérielles chargées de la sécurité des systèmes d'information

1. Le Secrétariat général de la défense et de la sécurité nationale (SGDSN)

Le SGDSN, en tant qu'ANS, est responsable de la mise en œuvre dans les entités françaises de la politique de l'UE en matière de sécurité des systèmes d'information.

[11] Sécurité des systèmes d'information.

Il dispose à cette fin d'un service à compétence nationale, l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

2. L'Agence nationale de la sécurité des systèmes d'information (ANSSI)

L'ANSSI exerce les fonctions d'autorité nationale chargée de l'assurance de l'information prévues par les règles de sécurité du Conseil[12].
L'autorité nationale chargée de l'assurance de l'information s'acquitte des tâches suivantes:

a) définir les politiques et les lignes directrices de sécurité en matière d'assurance de l'information (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.

L'ANSSI exerce au profit du SGDSN la fonction d'autorité nationale d'homologation de sécurité. A ce titre :

- elle est responsable de la décision d'homologation des systèmes nationaux traitant des ICUE du niveau RESTREINT UE/EU RESTRICTED jusqu'au niveau TRES SECRET UE/EU TOP SECRET ou des implantations nationales des systèmes de l'UE manipulant des ICUE jusqu'au niveau TRES SECRET UE/EU TOP SECRET ;
- elle participe ou se fait représenter aux panels ou comités d'homologation de sécurité des institutions ou autres organes de l'UE.

L'ANSSI exerce les fonctions d'autorité d'agrément cryptographique prévues par les règles de sécurité du Conseil[13].
A ce titre, elle agréé les produits cryptographiques pour la protection d'informations classifiées jusqu'à un certain niveau de classification dans leur environnement opérationnel. Elle est en outre chargée de l'évaluation des produits cryptographiques.

L'autorité nationale de distribution assure les fonctions d'autorité de distribution cryptologique prévues par les règles de sécurité du Conseil[14].

[12] Décision 2011/292/UE, ANNEXE IV, Art 43.
[13] Décision 2011/292/UE, ANNEXE IV, Art 45.
[14] Décision 2011/292/UE, ANNEXE IV, Art 46.

ART. 41 : Les départements ministériels

Chaque ministre est responsable, dans le département et les organismes dont il a la charge, de la sécurité des systèmes d'information traitant d'ICUE, dans les conditions prévues par l'IGI n°1300 pour les systèmes d'information traitant d'informations classifiées nationales. Il peut désigner des autorités qualifiées responsables de la sécurité des systèmes d'information au niveau d'un service, d'une direction d'un ministère, au niveau d'un organisme ou d'un établissement relevant d'un ministère. Les autorités qualifiées peuvent se faire assister par un ou plusieurs agents de sécurité des systèmes d'information.

L'ANSSI, en tant qu'autorité nationale d'homologation, peut désigner une autorité d'homologation au sein d'un ministère pour les systèmes d'information nationaux traitant des ICUE du niveau RESTREINT UE/EU RESTRICTED jusqu'au niveau SECRET UE/EU SECRET.

Cette délégation a pour effet de transférer la responsabilité d'autorité nationale d'homologation de sécurité. Elle sera formalisée[15] et l'UE sera officiellement informée.

ART. 42 : L'administrateur de la sécurité d'un système

Un administrateur de la sécurité est désigné pour mettre en œuvre les mesures opérationnelles de sécurité relatives à chaque système d'information traitant d'ICUE, dans les conditions définies par l'IGI n°1300 pour les systèmes d'information traitant d'informations classifiées nationales.

L'administrateur de la sécurité d'un système exerce, en lien avec l'agent de sécurité des systèmes d'information concerné, la fonction d'autorité opérationnelle chargée de l'assurance de l'information prévue par les règles de sécurité du Conseil[16].

Conformément à la politique du Conseil relative aux ordinateurs et réseaux locaux (LAN) [17], les administrateurs de la sécurité doivent être habilités au niveau de classification immédiatement supérieur à celui des informations traitées par le système. Lorsqu'une habilitation TRES SECRET UE/EU TOP SECRET est requise, l'autorité d'homologation peut décider, dans des circonstances particulières et au cas par cas, qu'une habilitation SECRET UE/EU SECRET est suffisante.

---

[15] la formalisation de cette délégation peut prendre la forme d'une note de délégation, d'une instruction ou d'une note de stratégie d'homologation.
[16] Décision 2011/292/UE, Annexe IV, article 51.
[17] TECH-P-02-01

Chapitre II

La protection des systèmes d'information

ART. 43 : Principes généraux de protection des systèmes d'information

L'objectif général de la protection d'un système d'information est de garantir l'intégrité, l'authenticité, la confidentialité, la non-répudiation et la disponibilité des informations traitées par ce système. La protection d'un système d'information s'appuie sur des principes portant sur l'organisation et sur les moyens techniques, auxquels s'ajoutent des principes de défense en profondeur. Ces principes doivent être respectés strictement, dès lors que le système est susceptible de traiter des informations classifiées, selon les dispositions de l'IGI n°1300.

ART. 44 : Agrément des dispositifs de sécurité

Au sein d'un système national, lorsque la protection de la confidentialité des informations classifiées au niveau SECRET UE/EU SECRET ou d'un niveau supérieur est assurée par un produit cryptographique, celui-ci doit satisfaire aux conditions suivantes :

- dans tous les cas, il doit être agréé par le Conseil de l'UE[18] en tant qu'autorité d'agrément cryptographique, sur recommandation du comité de sécurité ;
- il doit en outre être agréé par l'ANSSI[19] au niveau de classification national équivalent ;
- en l'absence de produit disponible agréé par l'ANSSI, une dérogation exceptionnelle peut être accordée par l'ANSSI en fonction notamment des caractéristiques techniques et des conditions d'emploi du produit proposé par l'autorité responsable du système.

Au sein d'un système national, lorsque la protection de la confidentialité des informations classifiées au niveau CONFIDENTIEL UE/EU CONFIDENTIAL et RESTREINT UE/EU RESTRICTED est assurée par un produit cryptographique, celui-ci doit satisfaire aux conditions suivantes :

- il doit être agréé par l'ANSSI au niveau de classification national équivalent ;
- en l'absence de produit disponible agréé par l'ANSSI, une dérogation exceptionnelle peut être accordée par l'ANSSI en fonction notamment des caractéristiques techniques et des conditions d'emploi du produit proposé et sous réserve que ce produit ait été agréé par le secrétaire général du Conseil de l'UE (voire par le Conseil de l'UE) pour la protection d'ICUE de ce niveau ou d'un niveau supérieur.

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.
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:

---

[18] L'article 10 de la Décision du Conseil n° 2011/292/UE du 31 mars 2011 fixe les conditions d'agrément par l'UE des produits cryptographiques. La liste des produits agréés par l'UE est disponible sur www.consilium.europa.eu/policies/information-assurance.
[19] Au sens de l'article 89 de l'IGI 1300 du 30 novembre 2011.

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.
Les informations classifiées transmises dans les conditions d'urgence définies au présent paragraphe 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.
Lorsque des informations sont transmises dans les conditions d'urgence définies dans le présent paragraphe, un rapport est par la suite adressé à ce sujet au SGDSN en tant qu'ANS.

ART. 45 : L'homologation de sécurité

Les dispositions de l'IGI n°1300 relatives à l'homologation de sécurité sont applicables avec les précisions suivantes :

- tous les systèmes d'information traitant d'ICUE font l'objet d'un processus d'homologation, y compris au niveau RESTREINT UE/EU RESTRICTED.
- l'ANSSI exerce les fonctions d'autorité nationale d'homologation de sécurité pour les systèmes d'information nationaux traitant d'informations classifiés de l'UE jusqu'au niveau TRES SECRET UE/EU TOP SECRET (cf. article 40 de la présente instruction) ;
- dans le cas d'une interconnexion entre un système national traitant des ICUE et un système de l'UE, les responsabilités d'autorité nationale d'homologation de sécurité pour le nœud d'interconnexion sont exercées par un comité conjoint d'homologation.[20]

ART. 46 : Matériel cryptographique

En matière de gestion, de protection et de contrôle du matériel cryptographique UE[21], s'appliquent les règles définies par le Conseil de l'UE.
Les adaptations nécessaires de la réglementation nationale relative aux Articles contrôlés de la sécurité des systèmes d'information (ACSSI) pour le traitement du matériel cryptographique de l'UE sont précisées par l'ANSSI dans une instruction interministérielle[22].

ART. 47 : Systèmes d'information particuliers

Les systèmes d'information nationaux traitant des ICUE susceptibles de traiter des informations portant la mention «Spécial France[23] » doivent faire l'objet de mesures de sécurité particulières pour garantir que les utilisateurs étrangers qui auraient un besoin d'accès légitime au système ne puissent accéder aux informations dont l'accès n'est autorisé qu'aux seuls utilisateurs français.[24]

---

[20] Les règles concernant le comité conjoint d'homologation sont définies dans la Décision 2011/292/UE, ANNEXE IV, Art. 50.
[21] CCI (Crypto Controlled Item)
[22] Instruction interministérielle 910/DISSI/SCSSI/DR du 19 décembre 1994, en cours de révision au jour de la publication de la présente instruction.
[23] Conformément à l'article R. 2311-4 du code de la défense.
[24] Art 92- 1° de l'IGI 1300.

TITRE VI :

LA PROTECTION DES INFORMATIONS CLASSIFIEES DE L'UE DANS LES CONTRATS

→ Les personnes morales, de la même façon que les personnes physiques, ayant besoin de connaître des ICUE de niveau CONFIDENTIEL UE/EU CONFIDENTIAL ou d'un niveau supérieur pour l'exécution de travaux, doivent être habilitées par l'ANS/ASD du pays dans lequel elles sont implantées.
→ La détention par un contractant de telles ICUE est notamment conditionnée par l'aptitude physique des locaux et, le cas échéant, l'aptitude informatique des systèmes d'information, à accueillir de telles informations.

ART. 48 : Principes généraux de sécurité

Un Etat membre, une Institution ou autre organe de l'UE peut, par voie contractuelle, confier à des entreprises immatriculées et officiellement constituées dans un Etat membre ou dans un pays tiers ayant conclu un accord de sécurité avec l'UE des tâches qui impliquent ou nécessitent l'accès, le traitement ou le stockage d'ICUE. De tels contrats ne doivent pas concerner l'accès à des informations classifiées TRES SECRET UE/EU TOP SECRET.

Les dispositions prévues au Titre VI de l'IGI n°1300 pour les informations classifiées nationales sont applicables, en France, à toute entité publique ou privée impliquée dans un contrat dont l'exécution requiert l'accès, le traitement ou le stockage d'ICUE. Le présent titre définit les mesures additionnelles spécifiques applicables aux contrats classifiés de l'UE.

ART 49 : La procédure d'habilitation UE

1. Cas des entreprises françaises

La procédure d'habilitation UE pour les personnes morales et le dossier d'aptitude sont conformes à ceux décrits dans l'IGI n°1300 pour les contrats traitant d'informations couvertes par le secret de la défense nationale.

L'habilitation des entreprises françaises candidates à un contrat, contrat de sous-traitance[25] ou sous-contrat[26] impliquant l'accès, le traitement ou le stockage d'informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou SECRET UE/EU SECRET relève de chaque ministère, en fonction de son domaine de compétence.

Lorsqu'elles ne sont pas déjà titulaires d'une habilitation, les entreprises françaises qui soumissionnent à un tel contrat dans un cadre international peuvent adresser leur dossier d'habilitation soit au SGDSN, en tant qu'ANS, soit à l'ASD compétente, conformément à l'article 10 de la présente instruction. L'ANS ou l'ASD peut, le cas échéant, transmettre le

[25] Au sens de la loi no 75-1334 du 31 décembre 1975 relative à la sous-traitance.
[26] Au sens de l'article 275 du code des marchés publics.

dossier d'habilitation au ministère compétent, en fonction du domaine d'activité de l'entreprise.

Une entreprise déjà habilitée s'adresse à son autorité d'habilitation pour une extension éventuelle du domaine d'habilitation. L'autorité d'habilitation transmet, le cas échéant, les éléments à l'ANS ou l'ASD compétente pour la délivrance d'une attestation d'habilitation appropriée.

2. Cas des entreprises étrangères

Toute entreprise immatriculée dans un Etat membre de l'UE peut candidater à un contrat, contrat de sous-traitance ou sous-contrat impliquant l'accès, le traitement ou le stockage d'ICUE passé par un pouvoir adjudicateur ou un contractant français.

Aucun contrat, contrat de sous-traitance ou sous-contrat impliquant l'accès, le traitement ou le stockage d'ICUE ne peut être attribué à des entreprises immatriculées dans un Etat non membre de l'UE n'ayant pas conclu avec l'UE un accord sur la sécurité des informations classifiées.

Toute entreprise de droit étranger candidate à un tel contrat est tenue, à l'appui de sa candidature, de produire une attestation justifiant de son habilitation ou de la procédure en cours engagée à cette fin. Cette attestation est délivrée par une autorité d'habilitation de l'Etat dont elle relève lorsque cet Etat a conclu un accord de sécurité bilatéral ou multilatéral avec la France.

L'autorité d'habilitation peut saisir le SGDSN, en tant qu'ANS, ou l'ASD compétente, aux fins de requérir l'ANS ou l'ASD de l'Etat de nationalité de l'entreprise candidate en vue de procéder à l'habilitation appropriée de cette entreprise. Le modèle de demande d'attestation reproduit en annexe 4 peut être utilisé à cette fin.

ART. 50 : Aspects liés à la sécurité dans un contrat classifié de l'UE

Tout contrat nécessitant l'accès, le traitement ou le stockage d'ICUE comporte à minima une annexe de sécurité qui énumère les impératifs de sécurité propres au contrat. Le non-respect de ces impératifs peut constituer un motif suffisant de résiliation du contrat.
La liste des ICUE à protéger dans le cadre du contrat est consignée dans un guide de classification, partie intégrante de l'annexe de sécurité, élaboré par l'autorité contractante et utilisé aux fins de l'exécution dudit contrat.

En fonction de la portée des programmes ou des projets impliquant l'accès à des ICUE, l'autorité contractante chargée de gérer le projet ou le programme considéré peut élaborer des instructions de sécurité relatives à un programme/un projet (ISP). Les ISP sont approuvées par les ANS/ASD ou toute autre autorité de sécurité compétente des États membres associées au programme/projet.

Un guide de classification lié à l'ISP peut également être défini dès l'origine par l'autorité contractante. Ce guide de classification est alors décliné dans chaque contrat selon son périmètre à travers son annexe de sécurité.

ART. 51 : Mesures particulières pour les contrats RESTREINT UE/EU RESTRICTED

Une habilitation de sécurité n'est pas nécessaire pour l'accès à des informations de niveau RESTREINT UE/EU RESTRICTED; les intéressés doivent néanmoins justifier du besoin d'en connaître et être informés de leurs responsabilités quant à la protection de ces informations.

Conformément à la Décision 2011/292/UE, l'autorité de sécurité compétente est habilitée à effectuer des visites dans les installations des contractants ou sous-traitants, en vertu de stipulations contractuelles, afin de vérifier que les mesures de sécurité adaptées pour la protection des informations de niveau RESTREINT UE/EU RESTRICTED ont été mises en place.

Lorsqu'un contrat prévoit le traitement d'informations de niveau RESTREINT UE/EU RESTRICTED dans un système d'information exploité par un contractant, l'autorité contractante veille à ce que les exigences techniques et administratives à remplir concernant les moyens de transmission électronique et l'homologation des systèmes d'information soient précisées dans le contrat ou tout contrat de sous-traitance.

ART. 52 : Mise en application

La présente instruction entre en vigueur le

Fait à Paris, le 12 JUIL 2013

Pour le Premier ministre et par délégation,

le Secrétaire général de la défense et de la sécurité nationale,

Francis DELON

GLOSSAIRE

« Accord de sécurité » : Accord intergouvernemental conclu entre gouvernements ou avec une organisation internationale et ayant pour objet la protection d'informations classifiées. Ces accords comprennent l'identification et la reconnaissance mutuelle des autorités nationales de sécurité, la correspondance des niveaux de classification, la reconnaissance mutuelle des habilitations de personnes, les modalités de transmission et de protection des informations classifiées.

« Articles contrôlés de la sécurité des systèmes d'information » (ACSSI) : Moyens, tels que les dispositifs de sécurité ou leurs composants, et certaines informations relatives à ces moyens (spécifications algorithmiques, documents de conception, clés de chiffrement, rapports d'évaluation, etc.) qui nécessitent la mise en œuvre d'une gestion spécifique visant à assurer leur traçabilité tout au long de leur cycle de vie. Il s'agit des moyens et des informations, qu'ils soient eux-mêmes classifiés ou non, qu'il est essentiel de pouvoir localiser à tout moment et en particulier en cas de compromission suspectée ou avérée.

« Assurance de l'information » (AI ou SSI[27]): Certitude que les systèmes d'information protégeront les informations qu'ils traitent et fonctionneront comme ils le doivent, quand ils le doivent, sous le contrôle d'utilisateurs légitimes. Une assurance de l'information efficace garantit des niveaux appropriés de confidentialité, d'intégrité, de disponibilité, de non-répudiation et d'authenticité. L'assurance de l'information est fondée sur un processus de gestion des risques.

Autorité nationale de sécurité (ANS) : Organisme gouvernemental chargé des relations avec les autres Etats et les structures internationales en matière d'habilitation de personnes et de protection des informations classifiées. En France, l'autorité nationale de sécurité est le secrétaire général de la défense et de la sécurité nationale.

Autorité d'habilitation : Autorité compétente pour solliciter une enquête d'habilitation et émettre la décision.

Autorité de sécurité désignée (ASD) : Conformément à l'article R.2311-10-1 du code de la défense, le SGDSN peut, en sa qualité d'ANS pour le secret de la défense nationale, nommer dans des domaines particuliers, notamment dans le domaine industriel, sur proposition du ou des ministres intéressés, une autorité de sécurité déléguée. Dans un cadre européen, cette autorité est plus particulièrement chargée de faire connaître aux entreprises privées ou publiques la politique de sécurité industrielle de l'UE et de fournir des orientations et une aide pour sa mise en œuvre. Elle est alors nommée "autorité de sécurité désignée".

Besoin d'en connaître : nécessité impérieuse de prendre connaissance d'une information dans le cadre d'une fonction déterminée, pour la bonne exécution d'une mission précise.

---

[27] Sécurité des systèmes d'information.

Bureau d'ordre : Bureau créé au sein de chaque organisme ou service dans lequel des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL et de niveau supérieur sont traitées. Il est chargé de veiller à ce que ces informations soient traitées conformément à la présente instruction.

Contrat classifié de l'UE : contrat 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.

Habilitation UE de sécurité du personnel : Etablissement du fait qu'une personne a le droit d'accéder à des informations classifiées de l'UE. Cette habilitation désigne la décision explicite, permettant à une personne, en fonction de son besoin d'en connaître, d'avoir accès aux informations classifiées de l'UE au niveau précisé dans la décision ainsi qu'au(x) niveau(x) inférieur(s).

Haut fonctionnaire de défense et de sécurité (HFDS) : Personne chargée d'assister le un ministre, le Premier ministre ou le Président de la République dans l'exercice de ses leurs attributions de sécurité, de défense et de protection du secret. Il est, dans certains ministères, appelé haut fonctionnaire correspondant de sécurité et de défense (HFCDS) ou haut fonctionnaire de défense (HFD).

Information classifiée de l'UE (ICUE) : Toute information ou support classifié, tel que défini dans l'IGI n°1300, 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 Etats membres, et identifié comme tel par une classification de sécurité de l'UE.

Instruction de sécurité de programme (ISP) : 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.

Sécurité industrielle de l'UE : la sécurité industrielle consiste à appliquer des mesures visant à assurer la protection des informations classifiées de l'UE dès la phase de négociations précontractuelles ou de l'avis d'appel public à la concurrence et, par la suite, tout au long du cycle de vie des contrats classifiés. De tels contrats ne doivent pas concerner l'accès à des informations classifiées TRES SECRET UE/EU TOP SECRET.

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. La présente instruction s'applique aux systèmes d'information et de communication traitant d'informations classifiées de l'UE.

ANNEXES

- Schéma d'organisation du réseau UE..... *36*

- Attestation de garantie matérielle de sécurité..... *37*

- Modèle d'état des signatures *38*

- Modèle de demande d'attestation d'habilitation internationale *39*

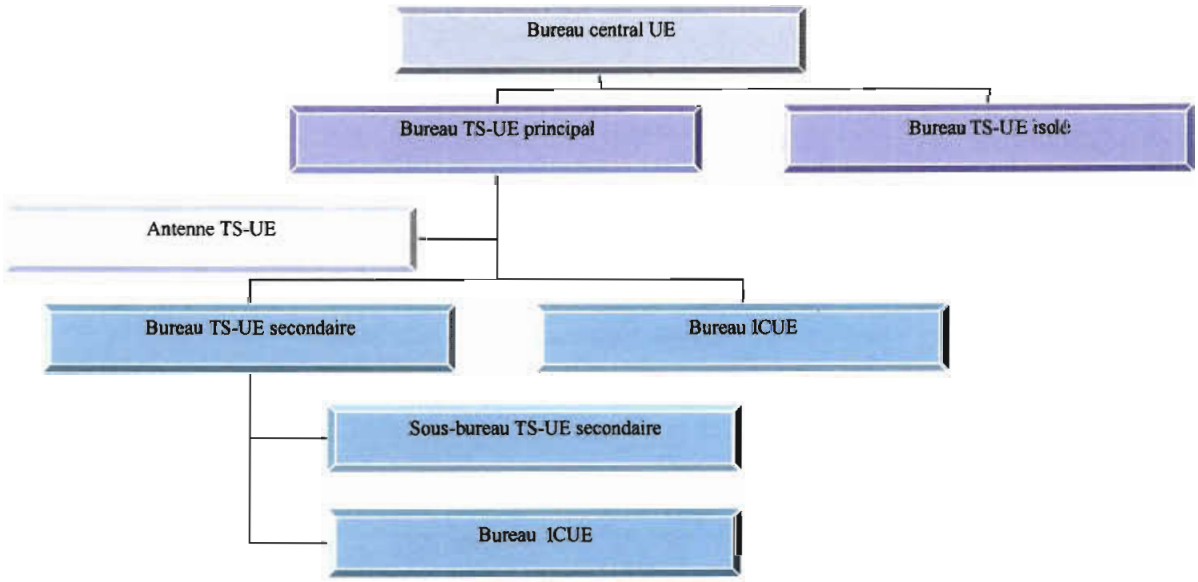
Annexe 1

SCHEMA D'ORGANISATION DU RESEAU UE

Ayant à sa tête le chef du Bureau central UE, le réseau UE est articulé en plusieurs sous-réseaux pouvant grouper chacun, sous le contrôle du chef d'un bureau TS-UE principal, plusieurs bureaux TS-UE secondaires et bureaux ICUE. Ces sous-réseaux sont d'une manière générale adaptés aux grands ensembles civils ou militaires.

Le réseau UE comprend :

- un bureau central TRES SECRET UE/EU TOP SECRET (« bureau central UE »);
- des bureaux TRES SECRET UE/EU TOP SECRET principaux ;
    - o des antennes TRES SECRET UE/EU TOP SECRET (« antennes TS-UE »), implantées dans la même enceinte que le bureau TS-UE principal dont elles dépendent et qui les gère directement ;
- des bureaux TRES SECRET UE/EU TOP SECRET secondaires (« bureaux TS-UE secondaires ») ;
    - o des sous-bureaux TRES SECRET UE/EU TOP SECRET secondaires (« sous-bureaux TS-UE secondaires »), créés à titre exceptionnel avec l'accord du Bureau central UE, dépendants d'un bureau TS-UE secondaire et implantés dans une aire géographique différente (ex. : bases aériennes ou maritimes) ;
- Des bureaux TRES SECRET UE/EU TOP SECRET isolés (« bureaux TS-UE isolés »), directement rattachés au Bureau central UE ;
- Des bureaux de protection des ICUE (« bureaux ICUE »), pour le traitement des informations classifiées SECRET UE/EU SECRET et CONFIDENTIEL UE/EU CONFIDENTIAL.



Annexe 2

Ministère
Organisme demandeur
(timbre)
N° . . . . . /

ATTESTATION DE GARANTIES MATERIELLES DE SECURITE

Concernant :

Le bureau : (1)

Localisation du bureau d'ordre : (2)

Référence : - Article 11 de l'instruction interministérielle n° 2102/SGDSN/PSE/PSD du .../.../...
- Avis technique n° ....

Je soussigné, atteste que les conditions matérielles de sécurité définies par l'instruction susvisée sont réalisées dans les locaux prévus pour l'installation du (3) précité. Elles ont été contrôlées par le (4).

A....., le.....
Grade ou titre, fonction et signature
du chef de l'organisme abritant le bureau d'ordre

(1) : Désignation complète du bureau d'ordre (B. TS-UE P., B. TS-UE I., B.TS-UE S., S-B TSUE S., antennes TS-UE, B-ICUE) avec adresse postale.
(2) : Pièce(s), étage, nom ou numéro du bâtiment.
(3) : Désignation du bureau d'ordre.
(4) : Service enquêteur ayant délivré l'avis technique de sécurité.

Annexe 3

MINISTERE DE …
…..
……..

N° …/…
du

ETAT DES SIGNATURES

Du personnel du bureau d'ordre ayant des responsabilités dans la production des certificats de sécurité ou la réception des documents classifiés

U.E

Bureau : Bureau TS-UE principal (par exemple)
Adresse :

FONCTIONS	GRADE,NOMS ET PRENOMS	SPECIMEN DE SIGNATURE	N° DE TELEPHONE	REFERENCE DE L'HABILITATION TS.UE OU S.UE	DATE LIMITE DE VALIDITE
Chef bureau TS-UE principal					
Suppléant Chef bureau TS-UE principal					

PERSONNELS HABILITES A SIGNER LES ACCUSES DE RECEPTION

FONCTIONS	GRADE,NOMS ET PRENOMS	SPECIMEN DE SIGNATURE	N° DE TELEPHONE	REFERENCE DE L'HABILITATION TS.UE OU S.UE	DATE LIMITE DE VALIDITE
Chef de secrétariat					

Cet Etat annule et remplace l'état n°…. du……

FACILITY SECURITY CLEARANCE INFORMATION SHEET (FIS)

REQUEST

Please [ ] provide a FSC assurance of the facility listed below.
[ ] start initiating a FSC up to and including the level of... if the facility does not hold acurrent FSC.
[ ] confirm the FSC up to and including the level of ... as provided on .....(ddmmyy).
[ ] provide the correct and complete information, if applicable.

	corrections/completions:
1. Full facility name:	
2. Full facility address:	
3. Mailing address (if different from 2):	
4. Zip code/city/country:	
5. Name/phone/fax/e-mail of the security officer:	

6. This request is made for the following reason(s):
(indicate particulars of the precontractual stage, contract, sub-contract, programme/project)

REQUESTING NSA/DSA or SA: Name:.....Date:.....

REPLY

1. This is to inform you that the above mentioned facility:

[ ] holds a FSC up to and including the level of [ ] S [ ] C
[ ] does not hold a FSC.
[ ] does not hold a FSC but, on your above mentioned request, the FSC is in progress. You will be informed when the FSC has been established. Expected date: .../...(mm/yy). (if known).

2. Safeguarding of classified documents: [ ] yes, level: ... [ ] no.
Safeguarding of classified material : [ ] yes, level: ... [ ] no.

3. This FSC certification expires on:.....(ddmmyy).
You will be informed in case of an earlier invalidation or significant change to any information listed above.

4. Should any contract be let or classified information be transferred in relation to this certification, please inform us of all relevant data including security classification.

5. REMARKS:
.....
.....
.....

PROVIDING NSA/DSA: Name:..... Date:.....