COMMISSION DECISION (EU, Euratom) 2015/444

of 13 March 2015

on the security rules for protecting EU classified information

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 249 thereof,

Having regard to the Treaty establishing the European Atomic Energy Community, and in particular Article 106 thereof,

Having regard to the Protocol No 7 on the Privileges and Immunities of the European Union annexed to the Treaties, and in particular Article 18 thereof,

Whereas:

(1) The Commission's security provisions regarding the protection of European Union Classified Information (EUCI) need to be reviewed and updated, taking into account institutional, organisational, operational and technological developments.

(2) The European Commission has entered into instruments on security matters for its principal sites with the governments of Belgium, Luxembourg and Italy ([1])

(3) The Commission, the Council and the European External Action Service are committed to applying equivalent security standards for protecting EUCI.

(4) It is important that, where appropriate, the European Parliament and other Union institutions, agencies, bodies or offices, are associated with the principles, standards and rules for protecting classified information which are necessary in order to protect the interests of the Union and its Member States.

(5) Risk to EUCI shall be managed as a process. This process shall be aimed at determining known security risks, defining security measures to reduce such risks to an acceptable level in accordance with the basic principles and minimum standards set out in this Decision and at applying these measures in line with the concept of defence in depth. The effectiveness of such measures shall be continuously evaluated.

(6) Within the Commission, physical security aimed at protecting classified information is the application of physical and technical protective measures intended to prevent unauthorised access to EUCI.

(7) The management of EUCI is the application of administrative measures for controlling EUCI throughout its life-cycle to supplement the measures provided for in Chapters 2, 3 and 5 of this Decision and thereby help deter, detect and recover from deliberate or accidental compromise or loss of such information. Such measures relate in particular to the creation, storage, registration, copying, translation, downgrading, declassification, carriage and destruction of EUCI and they supplement the general rules on document management of the Commission (Decisions 2002/47/EC ([2]), ECSC, Euratom and 2004/563/EC, Euratom ([3])).

([1]) Cf. the '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' of 31 December 2004, the 'Accord de sécurité signé entre la Commission et le Gouvernement luxembourgeois' of 20 January 2007, and the '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' of 22 July 1959.

([2]) Commission Decision 2002/47/EC, ECSC, Euratom of 23 January 2002 amending its rules of procedure (OJ L 21, 24.1.2002, p. 23).

([3]) Commission Decision 2004/563/EC, Euratom of 7 July 2004 amending its Rules of Procedure (OJ L 251, 27.7.2004, p. 9).

(8) The provision of this Decision shall be without prejudice to:

(a) Regulation (Euratom) No 3 ([1]);

(b) Regulation (EC) No 1049/2001 of the European Parliament and of the Council ([2]);

(c) Regulation (EC) No 45/2001 of the European Parliament and of the Council ([3]);

(d) Council Regulation (EEC, Euratom) No 354/83 ([4]),

HAS ADOPTED THIS DECISION:

CHAPTER 1

BASIC PRINCIPLES AND MINIMUM STANDARDS

Article 1

Definitions

For the purpose of this Decision, the following definitions shall apply:

(1) 'Commission department' means any Commission Directorate-General or service, or any Cabinet of a Member of the Commission;

(2) 'cryptographic (Crypto) material' means cryptographic algorithms, cryptographic hardware and software modules, and products including implementation details and associated documentation and keying material;

(3) 'declassification' means the removal of any security classification;

(4) 'defence in depth' means the application of a range of security measures organised as multiple layers of defence;

(5) 'document' means any recorded information regardless of its physical form or characteristics;

(6) 'downgrading' means a reduction in the level of security classification;

(7) 'handling' of EUCI means all possible actions to which EUCI may be subject throughout its life-cycle. It comprises its creation, registration, processing, carriage, downgrading, declassification and destruction. In relation to Communication and Information Systems (CIS) it also comprises its collection, display, transmission and storage;

(8) 'holder' means a duly authorised individual with an established need-to-know who is in possession of an item of EUCI and is accordingly responsible for protecting it;

(9) 'implementing rules' means any set of rules or security notices adopted in accordance with Chapter 5 of Commission Decision (EU, Euratom) 2015/443 ([5]);

(10) 'material' means any medium, data carrier or item of machinery or equipment, either manufactured or in the process of manufacture;

(11) 'originator' means the Union institution, agency or body, Member State, third state or international organisation under whose authority classified information has been created and/or introduced into the Union's structures;

(12) 'premises' means any immovable or assimilated property and possessions of the Commission;

([1]) Regulation (Euratom) No 3 of 31 July 1958 implementing Article 24 of the Treaty establishing the European Atomic Energy Community (OJ 17, 6.10.1958, p. 406/58).
([2]) Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (OJ L 145, 31.5.2001, p. 43).
([3]) Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1).
([4]) Council Regulation (EEC, Euratom) No 354/83 of 1 February 1983 concerning the opening to the public of the historical archives of the European Economic Community and the European Atomic Energy Community (OJ L 43, 15.2.1983, p. 1).
([5]) Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on Security in the Commission (See page 41 of this Official Journal).

(13) 'security risk management process' means the entire process of identifying, controlling and minimising uncertain events that may affect the security of an organisation or of any of the systems it uses. It covers the entirety of risk-related activities, including assessment, treatment, acceptance and communication;

(14) 'Staff Regulations' means the Staff Regulations of officials of the European Union and the Conditions of Employment of other servants of the European Union, as laid down by Regulation (EEC, Euratom, ECSC) No 259/68 of the Council [1];

(15) 'threat' means a potential cause of an unwanted incident which may result in harm to an organisation or any of the systems it uses; such threats may be accidental or deliberate (malicious) and are characterised by threatening elements, potential targets and attack methods;

(16) 'vulnerability' means a weakness of any nature that can be exploited by one or more threats. A vulnerability may be an omission or it may relate to a weakness in controls in terms of their strength, completeness or consistency and may be of a technical, procedural, physical, organisational or operational nature.

Article 2

Subject matter and scope

1. This Decision lays down the basic principles and minimum standards of security for protecting EUCI.

2. This Decision shall apply to all Commission departments and in all premises of the Commission.

3. Notwithstanding any specific indications concerning particular groups of staff, this Decision shall apply to the Members of the Commission, to Commission staff under the scope of the Staff Regulations and of the Conditions of Employment of other servants of the European Communities to national experts seconded to the Commission (SNEs), to service providers and their staff, to trainees and to any individual with access to Commission buildings or other assets, or to information handled by the Commission.

4. The provisions of this Decision shall be without prejudice to Decision 2002/47/EC, ECSC, Euratom and Decision 2004/563/EC, Euratom.

Article 3

Definition of EUCI, security classifications and markings

1. 'European Union classified information' (EUCI) means any information or material designated by an EU security classification, the unauthorised disclosure of which could cause varying degrees of prejudice to the interests of the European Union or of one or more of the Member States.

2. EUCI shall be classified at one of the following levels:

(a) TRES SECRET UE/EU TOP SECRET: information and material the unauthorised disclosure of which could cause exceptionally grave prejudice to the essential interests of the European Union or of one or more of the Member States;

(b) SECRET UE/EU SECRET: information and material the unauthorised disclosure of which could seriously harm the essential interests of the European Union or of one or more of the Member States;

(c) CONFIDENTIEL UE/EU CONFIDENTIAL: information and material the unauthorised disclosure of which could harm the essential interests of the European Union or of one or more of the Member States;

(d) RESTREINT UE/EU RESTRICTED: information and material the unauthorised disclosure of which could be disadvantageous to the interests of the European Union or of one or more of the Member States.

3. EUCI shall bear a security classification marking in accordance with paragraph 2. It may bear additional markings, which are not classification markings, but are intended to designate the field of activity to which it relates, identify the originator, limit distribution, restrict use or indicate releasability.

---

[1] Regulation (EEC, Euratom, ECSC) No 259/68 of the Council of 29 February 1968 laying down the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Communities and instituting special measures temporarily applicable to officials of the Commission (Conditions of Employment of Other Servants) (OJ L 56, 4.3.1968, p. 1).

Article 4

Classification management

1. Each Member of the Commission or Commission department shall ensure that EUCI it creates, is appropriately classified, clearly identified as EUCI and retains its classification level for only as long as necessary.

2. Without prejudice to Article 26 below, EUCI shall not be downgraded or declassified nor shall any of the security classification markings referred to in Article 3(2) be modified or removed without the prior written consent of the originator.

3. Where appropriate, implementing rules on handling EUCI, including a practical classification guide, shall be adopted in accordance with Article 60 below.

Article 5

Protection of classified information

1. EUCI shall be protected in accordance with this Decision and its implementing rules.

2. The holder of any item of EUCI shall be responsible for protecting it, in accordance with this Decision and its implementing rules, according to the rules laid out in Chapter 4 below.

3. Where Member States introduce classified information bearing a national security classification marking into the structures or networks of the Commission, the Commission shall protect that information in accordance with the requirements applicable to EUCI at the equivalent level, as set out in the table of equivalence of security classifications contained in Annex I.

4. An aggregate of EUCI may warrant a level of protection corresponding to a higher classification than that of its individual components.

Article 6

Security risk management

1. Security measures for protecting EUCI throughout its life-cycle shall be commensurate in particular with its security classification, the form and the volume of the information or material, the location and construction of facilities housing EUCI and the locally assessed threat of malicious and/or criminal activities, including espionage, sabotage and terrorism.

2. Contingency plans shall take account of the need to protect EUCI during emergency situations in order to prevent unauthorised access, disclosure or loss of integrity or availability.

3. Preventive and recovery measures to minimise the impact of major failures or incidents on the handling and storage of EUCI shall be included in all services' business continuity plans.

Article 7

Implementation of this Decision

1. Where necessary, implementing rules to supplement or support this Decision shall be adopted in accordance with Article 60 below.

2. The Commission departments shall take all necessary measures falling under their responsibility in order to ensure that, when handling or storing EUCI or any other classified information, this Decision and the relevant implementing rules are applied.

3. The security measures taken in implementation of this Decision shall be compliant with the principles for security in the Commission laid down in Article 3 of Decision (EU, Euratom) 2015/443.

4. The Director-General for Human Resources and Security shall set up the Commission Security Authority within the Directorate-General for Human Resources and Security. The Commission Security Authority shall have the responsibilities assigned to it by this Decision and its implementing rules.

5. Within each Commission department, the Local Security Officer (LSO), as referred to in Article 20 of Decision (EU, Euratom) 2015/443, shall have the following overall responsibilities for protecting EUCI in accordance with this Decision, in close cooperation with the Directorate-General for Human Resources and Security:

(a) managing requests for security authorisations for staff;

(b) contributing to security training and awareness briefings;

(c) supervising the department's Registry Control Officer (RCO);

(d) reporting on breaches of security and compromise of EUCI;

(e) holding spare keys and a written record of each combination setting;

(f) assuming other tasks related to the protection of EUCI or defined by implementing rules.

Article 8

Breaches of security and compromise of EUCI

1. A breach of security occurs as the result of an act or omission by an individual which is contrary to the security rules laid down in this Decision and its implementing rules.

2. Compromise of EUCI occurs when, as a result of a breach of security, it has wholly or in part been disclosed to unauthorised persons.

3. Any breach or suspected breach of security shall be reported immediately to the Commission Security Authority.

4. Where it is known or where there are reasonable grounds to assume that EUCI has been compromised or lost, a security inquiry shall be conducted in accordance with Article 13 of Decision (EU, Euratom) 2015/443.

5. All appropriate measures shall be taken to:

(a) inform the originator;

(b) ensure that the case is investigated by personnel not immediately concerned with the breach in order to establish the facts;

(c) assess the potential damage caused to the interests of the Union or of the Member States;

(d) take appropriate measures to prevent a recurrence; and

(e) notify the appropriate authorities of the action taken.

6. Any individual who is responsible for a breach of the security rules laid down in this Decision may be liable to disciplinary action in accordance with the Staff regulations. Any individual who is responsible for compromising or losing EUCI shall be liable to disciplinary and/or legal action in accordance with the applicable laws, rules and regulations.

CHAPTER 2

PERSONNEL SECURITY

Article 9

Definitions

For the purpose of this Chapter, the following definitions apply:

(1) 'authorisation for access to EUCI' means a decision by the Commission Security Authority taken on the basis of an assurance given by a competent authority of a Member State that a Commission official, other servant or seconded national expert may, provided his 'need-to-know' has been determined and he has been appropriately briefed on his responsibilities, be granted access to EUCI up to a specified level (CONFIDENTIEL UE/EU CONFIDENTIAL or above) until a specified date; the individual thus described is said to be 'security authorised'.

(2) 'personnel security authorisation' is the application of measures to ensure that access to EUCI is granted only to individuals who have:

(a) a need-to-know;

(b) been security authorised to the relevant level, where appropriate; and

(c) been briefed on their responsibilities.

(3) 'Personnel Security Clearance' (PSC) means a statement by a competent authority of a Member State which is made following completion of a security investigation conducted by the competent authorities of a Member State and which certifies that an individual may, provided his 'need-to-know' has been determined and he has been appropriately briefed on his responsibilities, be granted access to EUCI up to a specified level (CONFIDENTIEL UE/EU CONFIDENTIAL or above) until a specified date;

(4) 'Personnel Security Clearance Certificate' (PSCC) means a certificate issued by a competent authority establishing that an individual holds a valid security clearance or a security authorisation issued by the Commission Security Authority and which shows the level of EUCI to which that individual may be granted access (CONFIDENTIEL UE/EU CONFIDENTIAL or above), the period of validity of the relevant security clearance or authorisation and the date of expiry of the certificate itself.

(5) 'security investigation' means the investigative procedures conducted by the competent authority of a Member State in accordance with its national laws and regulations in order to obtain an assurance that nothing adverse is known which would prevent an individual from being granted a security clearance up to a specified level (CONFIDENTIEL UE/EU CONFIDENTIAL or above).

Article 10

Basic Principles

1. An individual shall only be granted access to EUCI after

(1) his need-to-know has been determined;

(2) he has been briefed on the security rules for protecting EUCI and the relevant security standards and guidelines, and has acknowledged his responsibilities with regard to protecting such information;

(3) for information classified CONFIDENTIEL UE/EU CONFIDENTIAL and above, he has been security authorised to the relevant level or is otherwise duly authorised by virtue of his functions in accordance with national laws and regulations.

2. All individuals whose duties may require them to have access to EUCI classified CONFIDENTIEL UE/EU CONFIDENTIAL or above shall be security authorised to the relevant level before being granted access to such EUCI. The individual concerned shall consent in writing to being submitted to the personnel security clearance procedure. Failure to do so shall mean that the individual cannot be assigned to a post, function or task which involves access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above.

3. Personnel security clearance procedures shall be designed to determine whether an individual, taking into account his loyalty, trustworthiness and reliability, may be authorised to access EUCI.

4. The loyalty, trustworthiness and reliability of an individual for the purposes of being security cleared for access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above shall be determined by means of a security investigation conducted by the competent authorities of a Member State in accordance with its national laws and regulations.

5. The Commission Security Authority shall be solely responsible for liaising with the national security authorities ('NSAs') or other competent national authorities in the context of all security clearance issues. All contacts between Commission services and their staff and the NSAs and other competent authorities shall be conducted through the Commission Security Authority.

Article 11

Security authorisation procedure

1. Each Director-General or head of service within the Commission shall identify the positions within his department for which the holders need to access information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above to perform their duties and so need to be security authorised.

2. As soon as it is known that an individual will be appointed to a position requiring access to information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above, the LSO of the Commission department concerned shall inform the Commission Security Authority, which shall transmit to the individual the security clearance questionnaire issued by the NSA of the Member State under whose nationality the individual has been appointed as a staff member of the European institutions. The individual shall consent in writing to being submitted to the security clearance procedure and return the completed questionnaire within the shortest deadline to the Commission Security Authority.

3. The Commission Security Authority shall forward the completed security clearance questionnaire to the NSA of the Member State under whose nationality the individual has been appointed as a staff member of the European institutions, requesting that a security investigation be undertaken for the level of EUCI to which the individual will require access.

4. Where information relevant to a security investigation is known to the Commission Security Authority concerning an individual who has applied for a security clearance, the Commission Security Authority, acting in accordance with the relevant rules and regulations, shall notify the competent NSA thereof.

5. Following completion of the security investigation, and as soon as possible after having been notified by the relevant NSA of its overall assessment of the findings of the security investigation, the Commission Security Authority:

(a) may grant an authorisation for access to EUCI to the individual concerned and authorise access to EUCI up to the relevant level until a date specified by him but for a maximum of 5 years, where the security investigation results in an assurance that nothing adverse is known which would call into question the loyalty, trustworthiness and reliability of the individual;

(b) shall, where the security investigation does not result in such an assurance, in accordance with the relevant rules and regulations, notify the individual concerned, who may ask to be heard by the Commission Security Authority, who in turn may ask the competent NSA for any further clarification it can provide according to its national laws and regulations. If the outcome of the security investigation is confirmed, the authorisation for access to EUCI shall not be issued.

6. The security investigation together with the results obtained shall be subject to the relevant laws and regulations in force in the Member State concerned, including those concerning appeals. Decisions by the Commission Security Authority shall be subject to appeals in accordance with the Staff Regulations.

7. The Commission shall accept the authorisation for access to EUCI granted by any other Union institution, body or agency provided it remains valid. Authorisations shall cover any assignment by the individual concerned within the Commission. The Union institution, body or agency in which the individual is taking up employment will notify the relevant NSA of the change of employer.

8. If an individual's period of service does not commence within 12 months of the notification of the outcome of the security investigation to the Commission Security Authority, or if there is a break of 12 months in an individual's service, during which time he has not been employed by the Commission or by any other Union Institution, body or agency, or in a position with a national administration of a Member State, the Commission Security Authority shall refer the matter to the relevant NSA for confirmation that the security clearance remains valid and appropriate.

9. Where information becomes known to the Commission Security Authority concerning a security risk posed by an individual who holds a valid security authorisation, the Security Authority, acting in accordance with the relevant rules and regulations, shall notify the competent NSA thereof.

10. Where an NSA notifies the Commission Security Authority of the withdrawal of an assurance given in accordance with paragraph 5(a) for an individual who holds a valid authorisation for access to EUCI, the Commission Security Authority may ask for any clarification the NSA can provide according to its national laws and regulations. If the adverse information is confirmed by the relevant NSA, the security authorisation shall be withdrawn and the individual shall be excluded from access to EUCI and from positions where such access is possible or where he might endanger security.

11. Any decision to withdraw or suspend an authorisation for access to EUCI from any individual falling under the scope of this Decision, and, where appropriate, the reasons for doing so, shall be notified to the individual concerned, who may ask to be heard by the Commission Security Authority. Information provided by an NSA shall be subject to the relevant laws and regulations in force in the Member State concerned. Decisions made in this context by the Commission Security Authority shall be subject to appeals in accordance with the Staff Regulations.

12. Commission departments shall make sure that national experts seconded to them for a position requiring security authorisation to access EUCI shall present, prior to taking up their assignment, a valid PSC or Personnel Security Clearance Certificate ('PSCC'), according to national law and regulations, to the Commission Security Authority, who, on the basis thereof, will grant a security authorisation for access to EUCI up to the level equivalent to the one referred to in the national security clearance, with a maximum validity for the duration of their assignment.

Access to EUCI for individuals duly authorised by virtue of their functions

13. The Members of the Commission, who have access to EUCI by virtue of their functions on the basis of the Treaty, shall be briefed on their security obligations in respect of protecting EUCI.

Security Clearance and security authorisation records

14. Records of security clearances and authorisations granted for access to EUCI shall be maintained by the Commission Security Authority in accordance with this Decision. These records shall contain as a minimum the level of EUCI to which the individual may be granted access, the date of issue of the security clearance and its period of validity.

15. The Commission Security Authority may issue a PSCC showing the level of EUCI to which the individual may be granted access (CONFIDENTIEL UE/EU CONFIDENTIAL or above), the date of validity of the relevant authorisation for access to EUCI and the date of expiry of the certificate itself.

Renewal of security authorisations

16. After the initial granting of security authorisations and provided that the individual has had uninterrupted service with the European Commission or another Union Institution, body or agency and has a continuing need for access to EUCI, the security authorisation for access to EUCI shall be reviewed for renewal, as a general rule, every five years from the date of notification of the outcome of the last security investigation on which it was based.

17. The Commission Security Authority may extend the validity of the existing security authorisation for a period of up to 12 months, if no adverse information has been received from the relevant NSA or other competent national authority within a period of two months from the date of transmission of the request for renewal and the corresponding security clearance questionnaire. If, at the end of this 12-month period, the relevant NSA or other competent national authority has not notified the Commission Security Authority of its opinion, the individual shall be assigned to duties which do not require a security authorisation.

Article 12

Security authorisation briefings

1. After having participated in the security authorisation briefing organised by the Commission Security Authority, all individuals who have been security authorised shall acknowledge in writing that they have understood their obligations in respect of protecting EUCI and the consequences if EUCI is compromised. A record of such a written acknowledgement shall be kept by the Commission Security Authority.

2. All individuals who are authorised to have access to, or required to handle EUCI, shall initially be made aware, and periodically briefed on the threats to security and must report immediately to the Commission Security Authority any approach or activity that they consider suspicious or unusual.

3. All individuals who cease to be employed in duties requiring access to EUCI shall be made aware of, and where appropriate acknowledge in writing, their obligations in respect of the continued protection of EUCI.

Article 13

Temporary security authorisations

1. In exceptional circumstances, where duly justified in the interests of the service and pending completion of a full security investigation, the Commission Security Authority, may, after consulting the NSA of the Member State of which the individual is a national and subject to the outcome of preliminary checks to verify that no relevant adverse information is known, grant a temporary authorisation for individuals to access EUCI for a specific function, without prejudice to the provisions regarding renewal of security clearances. Such temporary authorisations for access to EUCI shall be valid for a single period not exceeding six months and shall not permit access to information classified TRES SECRET UE/EU TOP SECRET.

2. After having been briefed in accordance with Article 12(1), all individuals who have been granted a temporary authorisation shall acknowledge in writing that they have understood their obligations in respect of protecting EUCI and the consequences if EUCI is compromised. A record of such a written acknowledgement shall be kept by the Commission Security Authority

Article 14

Attendance at classified meetings organised by the Commission

1. Commission departments responsible for organising meetings at which information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above is discussed shall, through their LSO or through the meeting organiser, inform the Commission Security Authority well in advance of the dates, times, venue and participants of such meetings.

2. Subject to the provisions of Article 11(13), individuals assigned to participate in meetings organised by the Commission at which information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above is discussed, may only do so upon confirmation of their security clearance or security authorisation status. Access to such classified meetings shall be denied to individuals for whom the Commission Security Authority has not seen a PSCC or other proof of security clearance, or, to participants of the Commission who are not in possession of a security authorisation.

3. Before organising a classified meeting, the responsible meeting organiser or the LSO of the Commission department organising the meeting, shall request external participants to provide the Commission Security Authority a PSCC or other proof of security clearance. The Commission Security Authority shall inform the LSO or the meeting organiser of PSCC or other proof of PSC received. Where applicable, a consolidated list of names may be used, giving the relevant proof of security clearance.

4. Where the Commission Security Authority is informed by the competent authorities that a PSC has been withdrawn from an individual whose duties require attendance at meetings organised by the Commission, the Commission Security Authority shall notify the LSO of the Commission department responsible for organising the meeting.

Article 15

Potential Access to EUCI

Couriers, guards and escorts shall be security authorised to the appropriate level or otherwise appropriately investigated in accordance with national laws and regulations, be briefed on security procedures for protecting EUCI and be instructed on their duties for protecting such information entrusted to them.

CHAPTER 3

PHYSICAL SECURITY AIMED AT PROTECTING CLASSIFIED INFORMATION

Article 16

Basic principles

1. Physical security measures shall be designed to deny surreptitious or forced entry by an intruder, to deter, impede and detect unauthorised actions and to allow for segregation of personnel in their access to EUCI on a need-to-know basis. Such measures shall be determined based on a risk management process, in accordance with this Decision and its implementing rules.

2. In particular, physical security measures shall be designed to prevent unauthorised access to EUCI by:

(a) ensuring that EUCI is handled and stored in an appropriate manner;

(b) allowing for segregation of personnel in terms of access to EUCI on the basis of their need-to-know and, where appropriate, their security authorisation;

(c) deterring, impeding and detecting unauthorised actions; and

(d) denying or delaying surreptitious or forced entry by intruders.

3. Physical security measures shall be put in place for all premises, buildings, offices, rooms and other areas in which EUCI is handled or stored, including areas housing communication and information systems as referred to in Chapter 5.

4. Areas in which EUCI classified CONFIDENTIEL UE/EU CONFIDENTIAL or above is stored shall be established as Secured Areas in accordance with this Chapter and accredited by the Commission Security Accreditation Authority.

5. Only equipment or devices approved by the Commission Security Authority shall be used for protecting EUCI at the level CONFIDENTIEL UE/EU CONFIDENTIAL or above.

Article 17

Physical security requirements and measures

1. Physical security measures shall be selected on the basis of a threat assessment made by the Commission Security Authority, where appropriate in consultation with other Commission departments, other Union institutions, agencies or bodies and/or competent authorities in the Member States. The Commission shall apply a risk management process for protecting EUCI on its premises to ensure that a commensurate level of physical protection is afforded against the assessed risk. The risk management process shall take account of all relevant factors, in particular:

(a) the classification level of EUCI;

(b) the form and volume of EUCI, bearing in mind that large quantities or a compilation of EUCI may require more stringent protective measures to be applied;

(c) the surrounding environment and structure of the buildings or areas housing EUCI; and

(d) the assessed threat from intelligence services which target the Union, its institutions, bodies or agencies, or the Member States and from sabotage, terrorist, subversive or other criminal activities.

2. The Commission Security Authority, applying the concept of defence in depth, shall determine the appropriate combination of physical security measures to be implemented. To that effect, the Commission Security Authority shall develop minimum standards, norms and criteria, set out in implementing rules.

3. The Commission Security Authority is authorised to conduct entry and exit searches to act as a deterrent to the unauthorised introduction of material or the unauthorised removal of EUCI from premises or buildings.

4. When EUCI is at risk of being overlooked, even accidentally, the Commission departments concerned shall take the appropriate measures, as defined by the Commission Security Authority, to counter this risk.

5. For new facilities, physical security requirements and their functional specifications shall be defined in consent with the Commission Security Authority as part of the planning and design of the facilities. For existing facilities, physical security requirements shall be implemented in accordance with the minimum standards, norms and criteria set out in implementing rules.

Article 18

Equipment for the physical protection of EUCI

1. Two types of physically protected areas shall be established for the physical protection of EUCI:

(a) Administrative Areas; and

(b) Secured Areas (including technically Secured Areas).

2. The Commission Security Accreditation Authority shall establish that an area meets the requirements to be designated as an Administrative Area, a Secured Area or a technically Secured Area.

3. For Administrative Areas:

(a) a visibly defined perimeter shall be established which allows individuals and, where possible, vehicles to be checked;

(b) unescorted access shall be granted only to individuals who are duly authorised by the Commission Security Authority or any other competent authority; and

(c) all other individuals shall be escorted at all times or be subject to equivalent controls.

4. For Secured Areas:

(a) a visibly defined and protected perimeter shall be established through which all entry and exit is controlled by means of a pass or personal recognition system;

(b) unescorted access shall be granted only to individuals who are security-cleared and specifically authorised to enter the area on the basis of their need-to-know;

(c) all other individuals shall be escorted at all times or be subject to equivalent controls.

5. Where entry into a Secured Area constitutes, for all practical purposes, direct access to the classified information contained in it, the following additional requirements shall apply:

(a) the level of highest security classification of the information normally held in the area shall be clearly indicated;

(b) all visitors shall require specific authorisation to enter the area, shall be escorted at all times and shall be appropriately security cleared unless steps are taken to ensure that no access to EUCI is possible.

6. Secured Areas protected against eavesdropping shall be designated technically Secured Areas. The following additional requirements shall apply:

(a) such areas shall be equipped with an Intrusion Detection System ('IDS'), be locked when not occupied and be guarded when occupied. Any keys shall be managed in accordance with Article 20;

(b) all persons and material entering such areas shall be controlled;

(c) such areas shall be regularly physically and/or technically inspected by the Commission Security Authority. Such inspections shall also be conducted following any unauthorised entry or suspicion of such entry; and

(d) such areas shall be free of unauthorised communication lines, unauthorised telephones or other unauthorised communication devices and electrical or electronic equipment.

7. Notwithstanding point (d) of paragraph 6, before being used in areas where meetings are held or work is being performed involving information classified SECRET UE/EU SECRET and above, and where the threat to EUCI is assessed as high, any communications devices and electrical or electronic equipment shall first be examined by the Commission Security Authority to ensure that no intelligible information can be inadvertently or illicitly transmitted by such equipment beyond the perimeter of the Secured Area.

8. Secured Areas which are not occupied by duty personnel on a 24-hour basis shall, where appropriate, be inspected at the end of normal working hours and at random intervals outside normal working hours, unless an IDS is in place.

9. Secured Areas and technically Secured Areas may be set up temporarily within an Administrative Area for a classified meeting or any other similar purpose.

10. The LSO of the Commission department concerned shall draw up Security Operating Procedures (SecOPs) for each Secured Area under his responsibility stipulating, in accordance with the provisions of this Decision and its implementing rules:

(a) the level of EUCI which may be handled and stored in the area;

(b) the surveillance and protective measures to be maintained;

(c) the individuals authorised to have unescorted access to the area by virtue of their need-to-know and security authorisation;

(d) where appropriate, the procedures for escorts or for protecting EUCI when authorising any other individuals to access the area;

(e) any other relevant measures and procedures.

11. Strong rooms shall be constructed within Secured Areas. The walls, floors, ceilings, windows and lockable doors shall be approved by the Commission Security Authority and afford protection equivalent to a security container approved for the storage of EUCI of the same classification level.

Article 19

Physical protective measures for handling and storing EUCI

1. EUCI which is classified RESTREINT UE/EU RESTRICTED may be handled:

(a) in a Secured Area,

(b) in an Administrative Area provided the EUCI is protected from access by unauthorised individuals, or

(c) outside a Secured Area or an Administrative Area provided the holder carries the EUCI in accordance with Article 31 and has undertaken to comply with compensatory measures, set out in implementing measures, to ensure that EUCI is protected from access by unauthorised persons.

2. EUCI which is classified RESTREINT UE/EU RESTRICTED shall be stored in suitable locked office furniture in an Administrative Area or a Secured Area. It may temporarily be stored outside an Administrative Area or a Secured Area provided the holder has undertaken to comply with compensatory measures laid down in implementing rules.

3. EUCI which is classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET may be handled:

(a) in a Secured Area;

(b) in an Administrative Area provided the EUCI is protected from access by unauthorised individuals; or

(c) outside a Secured Area or an Administrative Area provided the holder:

(i) has undertaken to comply with compensatory measures, set out in implementing rules, to ensure the EUCI is protected from access by unauthorised persons;

(ii) keeps the EUCI at all times under his personal control; and

(iii) in the case of documents in paper form, has notified the relevant registry of the fact.

4. EUCI which is classified CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET shall be stored in a Secured Area in a security container or a strong room.

5. EUCI which is classified TRES SECRET UE/EU TOP SECRET shall be handled in a Secured Area, set up and maintained by the Commission Security Authority, and accredited to that level by the Commission Security Accreditation Authority.

6. EUCI which is classified TRES SECRET UE/EU TOP SECRET shall be stored in a Secured Area, accredited to that level by the Commission Security Accreditation Authority, under one of the following conditions:

(a) in a security container in accordance with the provisions of Article 18 with one or more of the following supplementary controls:

(1) continuous protection or verification by cleared security staff or duty personnel;

(2) an approved IDS in combination with security response personnel;

or

(b) in an IDS-equipped strong room in combination with security response personnel.

Article 20

Management of keys and combinations used for protecting EUCI

1. Procedures for managing keys and combination settings for offices, rooms, strong rooms and security containers shall be laid down in implementing rules according to Article 60 below. Such procedures shall be intended to guard against unauthorised access.

2. Combination settings shall be committed to memory by the smallest possible number of individuals needing to know them. Combination settings for security containers and strong rooms storing EUCI shall be changed:

(a) on receipt of a new container;

(b) whenever there is a change in personnel knowing the combination;

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

(d) when a lock has undergone maintenance or repair; and

(e) at least every 12 months.

CHAPTER 4

MANAGEMENT OF EU CLASSIFIED INFORMATION

Article 21

Basic principles

1. All EUCI documents should be managed in compliance with the Commission's policy on document management and consequently should be registered, filed, preserved and finally eliminated, sampled or transferred to the Historical Archives in accordance with the common Commission-level retention list for European Commission files.

2. Information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above shall be registered for security purposes prior to distribution and on receipt. Information classified TRES SECRET UE/EU TOP SECRET shall be registered in designated registries.

3. Within the Commission, a EUCI registry system shall be set up in accordance with the provisions of Article 27.

4. Commission departments and premises where EUCI is handled or stored shall be subject to regular inspection by the Commission Security Authority.

5. EUCI shall be conveyed between services and premises outside physically protected areas as follows:

(a) as a general rule, EUCI shall be transmitted by electronic means protected by cryptographic products approved in accordance with Chapter 5;

(b) when the means referred to in point (a) are not used, EUCI shall be carried either:

(i) on electronic media (e.g. USB sticks, CDs, hard drives) protected by cryptographic products approved in accordance with Chapter 5; or

(ii) in all other cases, as prescribed in implementing rules.

Article 22

Classifications and markings

1. Information shall be classified where it requires protection with regard to its confidentiality, in accordance with Article 3(1).

2. The originator of EUCI shall be responsible for determining the security classification level, in accordance with the relevant implementing rules, standards and guidelines regarding classification, and for the initial dissemination of the information.

3. The classification level of EUCI shall be determined in accordance with Article 3(2) and with the relevant implementing rules.

4. The security classification shall be clearly and correctly indicated, regardless of whether the EUCI is on paper, oral, electronic or in any other form.

5. Individual parts of a given document (i.e. pages, paragraphs, sections, annexes, appendices, attachments and enclosures) may require different classifications and be marked accordingly, including when stored in electronic form.

6. The overall classification level of a document or file shall be at least as high as that of its most highly classified component. When information from various sources is collated, the final product shall be reviewed to determine its overall security classification level, since it may warrant a higher classification than its component parts.

7. To the extent possible, documents containing parts with different classification levels shall be structured so that parts with a different classification level may be easily identified and detached if necessary.

8. The classification of a letter or note covering enclosures shall be as high as the highest classification of its enclosures. The originator shall indicate clearly at which level it is classified when detached from its enclosures by means of an appropriate marking, e.g.:

CONFIDENTIEL UE/EU CONFIDENTIAL

Without attachment(s) RESTREINT UE/EU RESTRICTED

Article 23

Markings

In addition to one of the security classification markings set out in Article 3(2), EUCI may bear additional markings, such as:

(a) an identifier to designate the originator;

(b) any caveats, code-words or acronyms specifying the field of activity to which the document relates, a particular distribution on a need-to-know basis or restrictions on use;

(c) releasability markings;

(d) where applicable, the date or specific event after which it may be downgraded or declassified.

Article 24

Abbreviated classification markings

1. Standardised abbreviated classification markings may be used to indicate the classification level of individual paragraphs of a text. Abbreviations shall not replace the full classification markings.

2. The following standard abbreviations may be used within EU classified documents to indicate the classification level of sections or blocks of text of less than a single page:

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

Article 25

Creation of EUCI

1. When creating an EU classified document:

(a) each page shall be marked clearly with the classification level;

(b) each page shall be numbered;

(c) the document shall bear a registration number and a subject, which is not itself classified information, unless it is marked as such;

(d) the document shall be dated;

(e) documents classified SECRET UE/EU SECRET or above shall bear a copy number on every page, if they are to be distributed in several copies.

2. Where it is not possible to apply paragraph 1 to EUCI, other appropriate measures shall be taken in accordance with implementing rules.

Article 26

Downgrading and declassification of EUCI

1. At the time of its creation, the originator shall indicate, where possible, whether EUCI can be downgraded or declassified on a given date or following a specific event.

2. Each Commission department shall regularly review EUCI for which it is the originator to ascertain whether the classification level still applies. A system to review the classification level of registered EUCI which has originated in the Commission no less frequently than every five years shall be established by implementing rules. Such a review shall not be necessary where the originator has indicated from the outset that the information will automatically be downgraded or declassified and the information has been marked accordingly.

3. Information classified RESTREINT UE/EU RESTRICTED having originated in the Commission will be considered to be automatically declassified after thirty years, in accordance with Regulation (EEC, Euratom) No 354/83 as amended by Council Regulation (EC, Euratom) No 1700/2003 ([1]).

Article 27

EUCI registry system in the Commission

1. Without prejudice to Article 52 paragraph 5 below, in each Commission department in which EUCI is handled or stored at the level of CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET, a responsible local EUCI registry shall be identified to ensure that EUCI is handled in accordance with this Decision.

2. The EUCI registry managed by the Secretariat-General shall be the Commission's Central EUCI Registry. It shall act as:

— the Local EUCI Registry for the Commission's Secretariat-General,

— the EUCI registry for the private offices of Members of the Commission, unless these have a designated local EUCI registry,

— the EUCI registry for Directorates-General or services which do not have a local EUCI registry,

— the main point of entry and exit for all information classified RESTREINT UE/EU RESTRICTED and up to including SECRET UE/EU SECRET exchanged between the Commission and its services and third States and international organisations, and, when provided for in specific arrangements, for other Union institutions, agencies and bodies.

3. Within the Commission, a registry shall be designated by the Commission Security Authority to act as the central receiving and dispatching authority for information classified TRES SECRET UE/EU TOP SECRET. Where necessary, subordinate registries may be designated to handle that information for registration purposes.

4. The subordinate registries may not transmit TRES SECRET UE/EU TOP SECRET documents directly to other subordinate registries of the same central TRES SECRET UE/EU TOP SECRET registry or externally without the express written approval of the latter.

5. EUCI registries shall be established as Secured Areas as defined in Chapter 3, and accredited by the Commission's Security Accreditation Authority (SAA).

Article 28

Registry control officer

1. Each EUCI registry shall be managed by a Registry Control Officer ('RCO').

2. The RCO shall be appropriately security-cleared.

3. The RCO shall be subject to the supervision of the LSO within the Commission department, as far as the application of the provisions regarding the handling of EUCI documents and compliance with the relevant security rules, standards and guidelines is concerned.

4. Within his responsibility for managing the EUCI Registry to which he has been assigned, the RCO shall assume the following overall tasks in accordance with this Decision and the relevant implementing rules, standards and guidelines:

— manage operations relating to the registration, preservation, reproduction, translation, transmission, dispatch and destruction or transfer to the historical archives service of EUCI,

— verify periodically the need to maintain the classification of information,

— assume any other tasks related to the protection of EUCI defined in implementing rules.

Article 29

Registration of EUCI for security purposes

1. For the purposes of this Decision, registration for security purposes (hereinafter referred to as 'registration') means the application of procedures which record the life-cycle of EUCI, including its dissemination.

([1]) Council Regulation (EC, Euratom) No 1700/2003 of 22 September 2003 amending Regulation (EEC, Euratom) No 354/83 concerning the opening to the public of the historical archives of the European Economic Community and the European Atomic Energy Community (OJ L 243, 27.9.2003, p. 1).

2. All information or material classified CONFIDENTIEL UE/EU CONFIDENTIAL and above shall be registered in designated registries when it is received in or dispatched from an organisational entity.

3. When EUCI is handled or stored using a Communication and Information System (CIS), registration procedures may be performed by processes within the CIS itself.

4. More detailed provisions concerning the registration of EUCI for security purposes shall be laid down in implementing rules.

Article 30

Copying and translating EU classified documents

1. TRES SECRET UE/EU TOP SECRET documents shall not be copied or translated without the prior written consent of the originator.

2. Where the originator of documents classified SECRET UE/EU SECRET and below has not imposed caveats on their copying or translation, such documents may be copied or translated on instruction from the holder.

3. The security measures applicable to the original document shall apply to copies and translations thereof.

Article 31

Carriage of EUCI

1. EUCI shall be carried in such a way as to protect it from unauthorised disclosure during its carriage.

2. Carriage of EUCI shall be subject to the protective measures, which shall:

— be commensurate with the level of classification of the EUCI carried, and

— be adapted to the specific conditions of its carriage, in particular depending on whether EUCI is carried:

  — within a Commission building or a self-contained group of Commission buildings,

  — between Commission buildings located in the same Member State,

  — within the Union,

  — from within the Union to the territory of a third State, and

  — be adapted to the nature and form of the EUCI.

3. These protective measures shall be laid down in detail in implementing rules, or, in case of projects and programmes referred to in Article 42, as an integral part of the relevant Programme or Project Security Instructions (PSI).

4. The implementing rules or PSI shall include provisions commensurate with the level of EUCI, regarding:

— the type of carriage, such as hand carriage, carriage by diplomatic or military courier, carriage by postal services or commercial courier services,

— packaging of EUCI,

— technical countermeasures for EUCI carried on electronic media,

— any other procedural, physical or electronic measure,

— registration procedures,

— use of security authorised personnel.

5. When EUCI is carried on electronic media, and notwithstanding Article 21, paragraph 5, the protective measures set out in the relevant implementing rules may be supplemented by appropriate technical countermeasures approved by the Commission Security Authority so as to minimise the risk of loss or compromise.

Article 32

Destruction of EUCI

1. EU classified documents which are no longer required may be destroyed, taking account of regulations on archives and of the Commission's rules and regulations on document management and archiving, and in particular with the Common Commission-Level Retention List.

2. EUCI of the level of CONFIDENTIEL UE/EU CONFIDENTIAL and above shall be destroyed by the RCO of the responsible EUCI registry on instruction from the holder or from a competent authority. The RCO shall update the logbooks and other registration information accordingly.

3. For documents classified SECRET UE/EU SECRET or TRES SECRET UE/EU TOP SECRET, such destruction shall be performed by the RCO in the presence of a witness who shall be cleared to at least the classification level of the document being destroyed.

4. The registrar and the witness, where the presence of the latter is required, shall sign a destruction certificate, which shall be filed in the registry. The RCO of the responsible EUCI registry shall keep destruction certificates of TRES SECRET UE/EU TOP SECRET documents for a period of at least 10 years and for documents classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET for a period of at least five years.

5. Classified documents, including those classified RESTREINT UE/EU RESTRICTED, shall be destroyed by methods which shall be defined in implementing rules and which shall meet relevant EU or equivalent standards.

6. Computer storage media used for EUCI shall be destroyed in accordance with procedures laid down in implementing rules.

Article 33

Destruction of EUCI in emergencies

1. Commission departments holding EUCI shall prepare plans based on local conditions for the safeguarding of EU classified material in a crisis including if necessary emergency destruction and evacuation plans. They shall promulgate instructions deemed necessary to prevent EUCI from falling into unauthorised hands.

2. The arrangements for the safeguarding and/or destruction of CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET material in a crisis shall under no circumstances adversely affect the safeguarding or destruction of TRES SECRET UE/EU TOP SECRET material, including the enciphering equipment, whose treatment shall take priority over all other tasks.

3. In the event of an emergency, if there is an imminent risk of unauthorised disclosure, EUCI shall be destroyed by the holder in such a way that it cannot be reconstructed in whole or in part. The originator and originating registry shall be informed of the emergency destruction of registered EUCI.

4. More detailed provisions for destruction of EUCI shall be laid down in implementing rules.

CHAPTER 5

PROTECTION OF EU CLASSIFIED INFORMATION IN COMMUNICATION AND INFORMATION SYSTEMS (CIS)

Article 34

Basic principles of Information Assurance

1. Information Assurance (IA) in the field of communication and information systems is the confidence that such systems will protect the information they handle and will function as they need to, when they need to, under the control of legitimate users.

2. Effective Information Assurance shall ensure appropriate levels of:

Authenticity: the guarantee that information is genuine and from *bona fide* sources;

Availability: the property of being accessible and usable upon request by an authorised entity;

Confidentiality: the property that information is not disclosed to unauthorised individuals, entities or processes;

Integrity: the property of safeguarding the accuracy and completeness of assets and information;

Non-repudiation: the ability to prove an action or event has taken place, so that this event or action cannot subsequently be denied.

3. IA shall be based on a risk management process.

Article 35

Definitions

For the purpose of this Chapter, the following definitions apply:

(a) 'Accreditation' means the formal authorisation and approval granted to a communication and information system by the Security Accreditation Authority (SAA) to process EUCI in its operational environment, following the formal validation of the Security Plan and its correct implementation;

(b) 'Accreditation Process' means the necessary steps and tasks required prior to the accreditation by the Security Accreditation Authority. These steps and tasks shall be specified in an Accreditation Process Standard;

(c) 'Communication and Information System' (CIS) means any system enabling the handling of information in electronic form. A communication and information system shall comprise the entire assets required for it to operate, including the infrastructure, organisation, personnel and information resources;

(d) 'Residual risk' means the risk which remains after security measures have been implemented, given that not all threats are countered and not all vulnerabilities can be eliminated;

(e) 'Risk' means the potential that a given threat will exploit internal and external vulnerabilities of an organisation or of any of the systems it uses and thereby cause harm to the organisation and to its tangible or intangible assets. It is measured as a combination of the likelihood of threats occurring and their impact;

(f) 'Risk acceptance' is the decision to agree to the further existence of a residual risk after risk treatment;

(g) 'Risk assessment' consists of identifying threats and vulnerabilities and conducting the related risk analysis, i.e. the analysis of probability and impact;

(h) 'Risk communication' consists of developing awareness of risks among CIS user communities, informing approval authorities of such risks and reporting them to operating authorities;

(i) 'Risk treatment' consists of mitigating, removing, reducing (through an appropriate combination of technical, physical, organisational or procedural measures), transferring or monitoring the risk.

Article 36

CIS handling EUCI

1. CIS shall handle EUCI in accordance with the concept of IA.

2. For CIS handling EUCI, compliance with the Commission's information systems security policy, as referred to in Commission Decision C(2006)3602 ([1]), implies that:

(a) the Plan-Do-Check-Act approach shall be applied for the implementation of the information systems security policy during the full life-cycle of the information system;

(b) the security needs must be identified through a business impact assessment;

(c) the information system and the data therein must undergo a formal asset classification;

([1]) C(2006) 3602 of 16 August 2006 concerning the security of information systems used by the European Commission.

(d) all mandatory security measures as determined by the policy on security of information systems must be implemented;

(e) a risk management process must be applied, consisting of the following steps: threat and vulnerability identification, risk assessment, risk treatment, risk acceptance and risk communication;

(f) a security plan, including the Security Policy and the Security Operating Procedures, is defined, implemented, checked and reviewed.

3. All staff involved in the design, development, testing, operation, management or usage of CIS handling EUCI shall notify to the SAA all potential security weaknesses, incidents, breaches of security or compromise which may have an impact on the protection of the CIS and/or the EUCI therein.

4. Where the protection of EUCI is provided by cryptographic products, such products shall be approved as follows:

(a) preference shall be given to products which have been approved by the Council or by the Secretary-General of the Council in its function as crypto approval authority of the Council, upon recommendation of the Commission Security Expert Group;

(b) where warranted on specific operational grounds, the Commission Crypto Approval Authority (CAA) may, upon recommendation of the Commission Security Expert Group, waive the requirements referred to under a) and grant an interim approval for a specific period.

5. During transmission, processing and storage of EUCI by electronic means, approved cryptographic products shall be used. Notwithstanding this requirement, specific procedures may be applied under emergency circumstances or in specific technical configurations after approval by the CAA.

6. Security measures shall be implemented to protect CIS handling information classified CONFIDENTIEL UE/EU CONFIDENTIAL or above against compromise of such information through unintentional electromagnetic emanations ('TEMPEST security measures'). Such security measures shall be commensurate with the risk of exploitation and the level of classification of the information.

7. The Commission Security Authority shall assume the following functions:

— IA Authority (IAA),

— Security Accreditation Authority (SAA),

— TEMPEST Authority (TA),

— Crypto Approval Authority (CAA),

— Crypto Distribution Authority (CDA).

8. The Commission Security Authority shall appoint for each system the IA Operational Authority.

9. The responsibilities of the functions described in paragraphs 7 and 8 will be defined in the implementing rules.

Article 37

Accreditation of CIS handling EUCI

1. All CIS handling EUCI shall undergo an accreditation process, based upon the principles of IA, whose level of detail must be commensurate with the level of protection required.

2. The accreditation process shall include the formal validation by the Commission SAA of the Security Plan for the CIS concerned in order to obtain assurance that:

(a) the risk management process, as referenced in Article 36(2), has been properly carried out;

(b) the System Owner has knowingly accepted the residual risk; and

(c) a sufficient level of protection of the CIS, and of the EUCI handled in it, has been achieved in accordance with this decision.

3. The Commission's SAA shall issue an accreditation statement which determines the maximum classification level of the EUCI that may be handled in the CIS as well as the corresponding terms and conditions for operation. This is without prejudice to the tasks entrusted to the Security Accreditation Board defined in Article 11 of Regulation (EU) No 512/2014 of the European Parliament and of the Council [1].

4. A joint Security Accreditation Board (SAB) shall be responsible for accrediting Commission's CIS involving several parties. It shall be composed of a SAA representative of each party involved and be chaired by an SAA representative of the Commission.

5. The accreditation process shall consist of a series of tasks to be assumed by the parties involved. The responsibility for the preparation of the accreditation files and documentation shall rest entirely upon the CIS System Owner.

6. The accreditation shall be the responsibility of the Commission SAA, who, at any moment in the life cycle of the CIS, shall have the right to:

(a) require that an accreditation process be applied;

(b) audit or inspect the CIS;

(c) where conditions for operation are no any longer satisfied, require the definition and effective implementation of a security improvement plan within a well-defined timescale, potentially withdrawing permission to operate the CIS until conditions for operation are again satisfied.

7. The accreditation process shall be established in a standard on the accreditation process for CIS handling EUCI, which shall be adopted in accordance with Article 10(3) of Decision C(2006) 3602.

Article 38

Emergency circumstances

1. Notwithstanding the provisions of this Chapter, the specific procedures described below may be applied in an emergency, such as during impending or actual crisis, conflict, war situations or in exceptional operational circumstances.

2. EUCI may be transmitted using cryptographic products which have been approved for a lower classification level or without encryption with the consent of the competent authority if any delay would cause harm clearly outweighing the harm entailed by any disclosure of the classified material and if:

(a) the sender and recipient do not have the required encryption facility; and

(b) the classified material cannot be conveyed in time by other means.

3. Classified information transmitted under the circumstances set out in paragraph 1 shall not bear any markings or indications distinguishing it from information which is unclassified or which can be protected by an available cryptographic product. Recipients shall be notified of the classification level, without delay, by other means.

4. A subsequent report shall be made to the competent authority and to the Commission Security Expert Group.

CHAPTER 6

INDUSTRIAL SECURITY

Article 39

Basic principles

1. Industrial security is the application of measures to ensure the protection of EUCI

(a) within the framework of classified contracts, by:

(i) candidates or tenderers throughout the tendering and contracting procedure;

(ii) contractors or subcontractors throughout the life-cycle of classified contracts;

[1] Regulation (EU) No 512/2014 of the European Parliament and of the Council of 16 April 2014 amending Regulation (EU) No 912/2010 setting up the European GNSS Agency (OJ L 150, 20.5.2014, p. 72).

(b) within the framework of classified grant agreements, by

(i) applicants during grant award procedures;

(ii) beneficiaries throughout the life-cycle of classified grant agreements.

2. Such contracts or grant agreements shall not involve information classified TRES SECRET UE/EU TOP SECRET.

3. Unless stated otherwise, provisions in this Chapter referring to classified contracts or contractors shall be applicable also to classified subcontracts or subcontractors.

Article 40

Definitions

For the purpose of this Chapter, the following definitions shall apply:

(a) 'Classified contract' means a framework contract or contract, as referred to in Council Regulation (EC, Euratom) No 1605/2002 ([1]), entered into by the Commission or one of its departments, with a contractor for the supply of movable or immovable assets, the execution of works or the provision of services, the performance of which requires or involves the creation, handling or storing of EUCI;

(b) 'Classified subcontract' means a contract entered into by a contractor of the Commission or one of its departments, with another contractor (i.e. the subcontractor) for the supply of movable or immovable assets, the execution of works or the provision of services, the performance of which requires or involves the creation, handling or storing of EUCI;

(c) 'Classified grant agreement' means an agreement whereby the Commission awards a grant, as referred to in Part I, Title VI, of Regulation (EC, Euratom) No 1605/2002, the performance of which requires or involves the creation, handling or storing of EUCI;

(d) 'Designated Security Authority' (DSA) means an authority responsible to the National Security Authority (NSA) of a Member State which is responsible for communicating to industrial or other entities national policy on all matters of industrial security and for providing direction and assistance in its implementation. The function of DSA may be carried out by the NSA or by any other competent authority.

Article 41

Procedure for classified contracts or grant agreements

1. Each Commission department, as contracting authority, shall ensure that the minimum standards on industrial security set out in this Chapter, are referred to or incorporated in the contract, and complied with when awarding classified contracts or grant agreements.

2. For the purposes of paragraph 1, the competent services within the Commission shall seek the advice of the Directorate-General for Human Resources and Security, and in particular its Security Directorate, and shall ensure that model contracts and subcontracts and model grant agreements include provisions reflecting the basic principles and minimum standards for protecting EUCI to be complied with by contractors and subcontractors, and respectively beneficiaries of grant agreements.

3. The Commission shall closely cooperate with the NSA, the DSA or any other competent authority of the Member States concerned.

4. When a contracting authority, intends to launch a procedure aimed at concluding a classified contract or grant agreement, it shall seek the advice of the Commission Security Authority on issues regarding the classified nature and elements of the procedure, during all its stages.

5. Templates for and models of classified contracts and subcontracts, classified grant agreements, contract notices, guidance on the circumstances where Facility Security Clearances (FSCs) are required, Programme or Project Security Instructions (PSI), Security Aspects Letters (SALs), visits, transmission and carriage of EUCI under classified contracts or classified grant agreements shall be laid down in implementing rules on industrial security, after consulting the Commission Security Expert Group.

([1]) Council Regulation (EC, Euratom) No 1605/2002 of 25 June 2002 on the Financial Regulation applicable to the general budget of the European Communities (OJ L 248, 16.9.2002, p. 1).

6. The Commission may conclude classified contracts or grant agreements which entrust tasks involving or entailing access to or the handling or storage of EUCI by economic operators registered in a Member State or in a third State with which an agreement or an administrative arrangement has been concluded in accordance with Chapter 7 of this Decision.

Article 42

Security elements in a classified contract or grant agreement

1. Classified contracts or grant agreements shall include the following security elements:

Programme or Project Security Instructions

(a) 'Programme or Project Security Instruction' (PSI) means a list of security procedures which are applied to a specific programme or project in order to standardise security procedures. It may be revised throughout the programme or project.

(b) The Directorate-General Human Resources and Security shall develop a generic PSI, the Commission departments responsible for programmes or projects involving handling or storage of EUCI may develop, where appropriate, specific PSIs, which shall be based upon the generic PSI.

(c) A specific PSI shall be developed in particular for programmes and projects characterised by their considerable scope, scale or complexity, or by the multitude and/or the diversity of contractors, beneficiaries and other partners and stakeholders involved, for instance as regards their legal status. The specific PSI shall be developed by the Commission department(s) managing the programme or project, in close cooperation with the Directorate-General Human Resources and Security.

(d) The Directorate-General Human Resources and Security shall submit both the generic and specific PSIs for advice to the Commission Security Expert Group.

Security Aspects Letter

(a) 'Security Aspects Letter' (SAL) means a set of special contractual conditions, issued by the contracting authority, which forms an integral part of any classified contract involving access to or the creation of EUCI, that identifies the security requirements and those elements of the contract requiring security protection.

(b) The contract-specific security requirements shall be described in a SAL. The SAL shall, where appropriate, contain the Security Classification Guide ('SCG') and shall be an integral part of a classified contract or sub-contract, or grant agreement.

(c) The SAL shall contain the provisions requiring the contractor or beneficiary to comply with the minimum standards laid down in this Decision. The contracting authority shall ensure the SAL indicates that non-compliance with these minimum standards may constitute sufficient grounds for the contract or the grant agreement to be terminated.

2. Both PSIs and SALs shall include a SCG as a mandatory security element:

(a) 'Security Classification Guide' (SCG) means a document which describes the elements of a programme, project, contract or grant agreement which are classified, specifying the applicable security classification levels. The SCG may be expanded throughout the life of the programme, project, contract or grant agreement and the elements of information may be re-classified or downgraded; where an SCG exists it shall be part of the SAL.

(b) Prior to launching a call for tender or letting a classified contract, the Commission department, as contracting authority, shall determine the security classification of any information to be provided to candidates and tenderers or contractors, as well as the security classification of any information to be created by the contractor. For that purpose, it shall prepare an SCG to be used for the performance of the contract, in accordance with this Decision and its implementing rules, after consulting the Commission Security Authority.

(c) In order to determine the security classification of the various elements of a classified contract, the following principles shall apply:

(i) in preparing an SCG, the Commission department, as the contracting authority, shall take into account all relevant security aspects, including the security classification assigned to information provided and approved to be used for the contract by the originator of the information;

(ii) the overall level of classification of the contract may not be lower than the highest classification of any of its elements; and

(iii) where relevant, the contracting authority shall liaise, through the Commission Security Authority, with the Member States' NSAs, DSAs or any other competent security authority concerned in the event of any changes regarding the classification of information created by or provided to contractors in the performance of a contract and when making any subsequent changes to the SCG.

Article 43

Access to EUCI for contractors' and beneficiaries' staff

The contracting or granting authority, shall ensure that the classified contract or classified grant agreement includes provisions indicating that staff of a contractor, subcontractor or beneficiary who, for the performance of the classified contract, subcontract or grant agreement, require access to EUCI, shall be granted such access only if:

(a) he has been security authorised to the relevant level or is otherwise duly authorised by their need-to-know has been determined;

(b) they have been briefed on the applicable security rules for protecting EUCI, and have acknowledged their responsibilities with regard to protecting such information;

(c) they have been security cleared 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 authority.

Article 44

Facility security clearance

1. 'Facility Security Clearance' (FSC) means an administrative determination by a NSA, DSA or any other competent security authority that, from the security viewpoint, a facility can afford an adequate level of protection to EUCI to a specified security classification level.

2. A FSC granted by the NSA or DSA or any other competent security authority of a Member State to indicate, in accordance with national laws and regulations, that an economic operator can protect EUCI at the appropriate classification level (CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET) within its facilities, shall be presented to the Commission Security Authority, which will forward it to the Commission department acting as the contracting or granting authority, before a candidate, tenderer or contractor, or grant applicant or beneficiary may be provided with or granted access to EUCI.

3. Where relevant, the contracting authority shall notify, through the Commission Security Authority, the appropriate NSA, DSA or any other competent security authority that an FSC is required for performing the contract. A FSC or PSC shall be required where EUCI classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET has to be provided in the course of the procurement or grant award procedure.

4. The contracting or granting authority shall not award a classified contract or a grant agreement to a preferred bidder or participant before having received confirmation from the NSA, DSA or any other competent security authority of the Member State in which the contractor or subcontractor concerned is registered that, where required, an appropriate FSC has been issued.

5. When the Commission Security Authority has been notified by the NSA, DSA or any other competent security authority which has issued a FSC about changes affecting the FSC, it shall inform the Commission department, acting as contracting or granting authority. In the case of a sub-contract, the NSA, DSA or any other competent security authority shall be informed accordingly.

6. Withdrawal of a FSC by the relevant NSA, DSA or any other competent security authority shall constitute sufficient grounds for the contracting or granting authority, to terminate a classified contract or exclude a candidate, tenderer or applicant from the competition. A provision to that effect shall be included in the model contracts and grant agreements to be developed.

Article 45

Provisions for classified contracts and grant agreements

1. Where EUCI is provided to a candidate, tenderer or applicant during the procurement procedure, the call for tender or call for proposal shall contain a provision obliging the candidate, tenderer or applicant failing to submit a tender or proposal or who is not selected, to return all classified documents within a specified period of time.

2. The contracting or granting authority, shall notify, through the Commission Security Authority, the competent NSA, DSA or any other competent security authority of the fact that a classified contract or grant agreement has been awarded, and of the relevant data, such as the name of the contractor(s) or beneficiaries, the duration of the contract and the maximum level of classification.

3. When such contracts or grant agreements are terminated, the contracting or granting authority, shall promptly notify, through the Commission Security Authority, the NSA, DSA or any other competent security authority of the Member State in which the contractor or grant beneficiary is registered.

4. As a general rule, the contractor or grant beneficiary shall be required to return to the contracting or granting authority, upon termination of the classified contract or the grant agreement, or of the participation of a grant beneficiary, any EUCI held by it.

5. Specific provisions for the disposal of EUCI during the performance of the classified contract or the classified grant agreement or upon its termination shall be laid down in the SAL.

6. Where the contractor or grant beneficiary is authorised to retain EUCI after termination of a classified contract or grant agreement, the minimum standards contained in this Decision shall continue to be complied with and the confidentiality of EUCI shall be protected by the contractor or the grant beneficiary.

Article 46

Specific provisions for classified contracts

1. The conditions relevant for the protection of EUCI under which the contractor may subcontract shall be defined in the call for tender and in the classified contract.

2. A contractor shall obtain permission from the contracting authority, before sub-contracting any parts of a classified contract. No subcontract involving access to EUCI may be awarded to subcontractors registered in a third country, unless there is a regulatory framework for the security of information as provided for in Chapter 7.

3. The contractor shall be responsible for ensuring that all sub-contracting activities are undertaken in accordance with the minimum standards laid down in this Decision and shall not provide EUCI to a subcontractor without the prior written consent of the contracting authority.

4. With regard to EUCI created or handled by the contractor, the Commission shall be considered to be the originator, and the rights incumbent on the originator shall be exercised by the contracting authority.

Article 47

Visits in connection with classified contracts

1. Where a Commission staff member or contractors' or grant beneficiaries' personnel 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 or grant agreement, visits shall be arranged in liaison with the NSAs, DSAs or any other competent security authority concerned. The Commission Security Authority shall be informed of such visits. However, in the context of specific programmes or projects, the NSAs, DSAs or any other competent security authority may also agree on a procedure whereby such visits can be arranged directly.

2. All visitors shall hold an appropriate security clearance and have a 'need-to-know' for access to the EUCI related to the classified contract.

3. Visitors shall be given access only to EUCI related to the purpose of the visit.

4. More detailed provisions shall be set out in implementing rules.

5. Compliance with the provisions regarding visits in connection with classified contracts, set out in this Decision and in the implementing rules referred to in paragraph 4, shall be mandatory.

Article 48

Transmission and carriage of EUCI in connection with classified contracts or classified grant agreements

1. With regard to the transmission of EUCI by electronic means, the relevant provisions of Chapter 5 of this Decision shall apply.

2. With regard to the carriage of EUCI, the relevant provisions of Chapter 4 of this Decision and its implementing rules shall apply, in accordance with national laws and regulations.

3. For the transport of classified material as freight, the following principles shall be applied when determining security arrangements:

(a) security shall be assured at all stages during transportation from the point of origin to the final destination;

(b) the degree of protection afforded to a consignment shall be determined by the highest classification level of material contained within it;

(c) prior to any cross-border movement of material classified CONFIDENTIEL UE/EU CONFIDENTIAL or SECRET UE/EU SECRET, a transportation plan shall be drawn up by the consignor and approved by the NSA, DSA or any other competent security authority concerned;

(d) journeys shall be point to point to the extent possible, and shall be completed as quickly as circumstances permit;

(e) whenever possible, routes should be only through Member States. Routes through States other than Member States should only be undertaken when authorised by the NSA, DSA or any other competent security authority of the States of both the consignor and the consignee.

Article 49

Transfer of EUCI to contractors or grant beneficiaries located in third states

EUCI shall be transferred to contractors or grant beneficiaries located in third States in accordance with security measures agreed between the Commission Security Authority, the Commission department, as the contracting or granting authority, and the NSA, DSA or other competent security authority of the concerned third country where the contractor or grant beneficiary is registered.

Article 50

Handling of information classified RESTREINT UE/EU RESTRICTED in the context of classified contracts or classified grant agreements

1. Protection of information classified RESTREINT UE/EU RESTRICTED handled or stored under classified contracts or grant agreements shall be based on the principles of proportionality and cost-effectiveness.

2. No FSC or PSC shall be required in the context of classified contracts or classified grant agreements involving the handling of information classified at the level of RESTREINT UE/EU RESTRICTED.

3. Where a contract or grant agreement involves handling of information classified RESTREINT UE/EU RESTRICTED in a CIS operated by a contractor or grant beneficiary, the contracting or granting authority shall ensure, after consulting the Commission Security Authority, that the contract or grant agreement specifies the necessary technical and administrative requirements regarding accreditation or approval of the CIS commensurate with the assessed risk, taking account of all relevant factors. The scope of accreditation or approval of such CIS shall be agreed between the Commission Security Authority and the relevant NSA or DSA.

CHAPTER 7

EXCHANGE OF CLASSIFIED INFORMATION WITH OTHER UNION INSTITUTIONS, AGENCIES, BODIES AND OFFICES, WITH MEMBER STATES, AND WITH THIRD STATES AND INTERNATIONAL ORGANISATIONS

Article 51

Basic principles

1. Where the Commission or one of its departments determines that there is a need to exchange EUCI with another Union Institution, agency, body or office, or with a third State or international organisation, the necessary steps shall be undertaken to establish an appropriate legal or administrative framework to that effect, which may include security of information agreements or administrative arrangements concluded in accordance with the relevant regulations.

2. Without prejudice to Article 57, EUCI shall only be exchanged with another Union Institution, agency, body or office, or with a third State or international organisation, provided such an appropriate legal or administrative framework is in place, and that there are sufficient guarantees that the Union Institution, agency, body or office, or the third State or international organisation concerned applies equivalent basic principles and minimum standards for the protection of classified information.

Article 52

Exchange of EUCI with other Union institutions, agencies, bodies and offices

1. Before entering into an administrative arrangement for the exchange of EUCI with another Union Institution, agency, body or office, the Commission shall seek assurance that the Union Institution, agency, body or office concerned:

(a) has a regulatory framework for the protection of EUCI in place, which lays down basic principles and minimum standards equivalent to those laid down in this Decision and its implementing rules;

(b) applies security standards and guidelines regarding personnel security, physical security, management of EUCI and security of Communication and Information Systems (CIS), which guarantee an equivalent level of protection of EUCI as that afforded in the Commission.

(c) marks classified information which it creates, as EUCI.

2. The Directorate-General Human Resources and Security shall, in close cooperation with other competent Commission departments, be the lead service within the Commission for the conclusion of administrative arrangements for the exchange of EUCI with other Union institutions, agencies, bodies or offices.

3. Administrative arrangements shall as a general rule take the form of an Exchange of Letters, signed by the Director-General for Human Resources and Security on behalf of the Commission.

4. Before entering into an administrative arrangement on the exchange of EUCI, the Commission Security Authority shall conduct an assessment visit aimed at assessing the regulatory framework for protecting EUCI and ascertaining the effectiveness of measures implemented for protecting EUCI. The administrative arrangement shall enter into force, and EUCI shall be exchanged, only if the outcome of this assessment visit is satisfactory and the recommendations made further to the visit have been complied with. Regular follow-up assessment visits shall be conducted to verify that the administrative arrangement is complied with and the security measures in place continue to meet the basic principles and minimum standards agreed.

5. Within the Commission, the EUCI registry managed by the Secretariat General shall, as a general rule, be the main point of entry and exit for classified information exchanges with other Union institutions, agencies, bodies and offices. However, where on security, organisational or operational grounds it is more appropriate for protecting EUCI, local EUCI registries established within Commission departments in accordance with this Decision and its implementing rules, shall operate as the point of entry and exit for classified information regarding matters within the competence of the Commission departments concerned.

6. The Commission Security Expert Group shall be informed of the process of concluding administrative arrangements pursuant to paragraph 2.

Article 53

Exchange of EUCI with Member States

1. EUCI may be exchanged with and released to Member States provided that they protect that information in accordance with the requirements applicable to classified information bearing a national security classification at the equivalent level as set out in the table of equivalence of security classifications contained in Annex I.

2. Where Member States introduce classified information bearing a national security classification marking into the structures or networks of the European Union, the Commission shall protect that information in accordance with the requirements applicable to EUCI at the equivalent level as set out in the table of equivalence of security classifications contained in Annex I.

Article 54

Exchange of EUCI with third States and international organisations

1. Where the Commission determines that it has a long-term need to exchange classified information with third States or international organisations, the necessary steps shall be undertaken to establish an appropriate legal or administrative framework to that effect, which may include security of information agreements or administrative arrangements concluded in accordance with the relevant regulations.

2. Such security of information agreements and administrative agreements referred to in paragraph 1 shall contain provisions to ensure that when third States or international organisations receive EUCI, such information is given protection appropriate to its classification level and according to minimum standards which are equivalent to those laid down in this Decision.

3. The Commission may enter into administrative arrangements in accordance with Article 56 where the classification level of EUCI is as a general rule no higher than RESTREINT UE/EU RESTRICTED.

4. Administrative arrangements for the exchange of classified information referred to in paragraph 3 shall contain provisions to ensure that when third States or international organisations receive EUCI, such information is given protection appropriate to its classification level and according to minimum standards which are equivalent to those laid down in this Decision. The Commission Security Expert Group shall be consulted on the conclusion of security of information agreements or administrative arrangements.

5. The decision to release EUCI originating in the Commission to a third State or international organisation shall be taken by the Commission department, as originator of this EUCI within the Commission, on a case-by-case basis, according to the nature and content of such information, the recipient's need-to-know and the measure of advantage to the Union. If the originator of the classified information for which release is desired, or of the source material it may contain, is not the Commission, the Commission department which holds this classified information, shall first seek the originator's written consent to release. If the originator cannot be established, the Commission department, which holds this classified information, shall assume the former's responsibility after consulting the Commission Security Expert Group.

Article 55

Security of information agreements

1. Security of information agreements with third states or international organisations are concluded in accordance with Article 218 TFEU.

2. Security of information agreements shall:

(a) establish the basic principles and minimum standards governing the exchange of classified information between the Union and a third State or international organisation;

(b) provide for technical implementing arrangements to be agreed between the competent security authorities of the relevant Union institutions and bodies and the competent security authority of the third State or international organisation in question. Such arrangements shall take account of the level of protection provided by the security regulations, structures and procedures in place in the third State or international organisation concerned;

(c) provide that prior to the exchange of classified information under the agreement, it shall be ascertained that the receiving party is able to protect and safeguard classified information provided to it in an appropriate manner.

3. The Commission shall, when a need to exchange classified information is determined according to Article 51(1), consult the European External Action Service, the General Secretariat of the Council and other Union institutions and bodies, where appropriate, in order to determine whether a recommendation according to Article 218(3) TFEU should be submitted.

4. No EUCI shall be exchanged by electronic means unless explicitly provided for in the security of information agreement or technical implementing arrangements.

5. Within the Commission, the EUCI registry managed by the Secretariat-General shall, as a general rule, be the main point of entry and exit for classified information exchanges with third States and international organisations. However, where on security, organisational or operational grounds it is more appropriate for protecting EUCI, local EUCI registries established within Commission departments in accordance with this Decision and its implementing rules, shall operate as the point of entry and exit for classified information regarding matters within the competence of the Commission departments concerned.

6. In order to assess the effectiveness of the security regulations, structures and procedures in the third State or international organisation concerned, the Commission shall, in collaboration with other Union institutions, agencies or bodies, participate in assessment visits, in mutual agreement with the third State or international organisation concerned. Such assessment visits shall evaluate:

(a) the regulatory framework applicable for protecting classified information;

(b) any specific features of the security policy and the way in which security is organised in the third State or international organisation which may have an impact on the level of classified information that may be exchanged;

(c) the security measures and procedures actually in place; and

(d) security clearance procedures for the level of EUCI to be released.

Article 56

Administrative arrangements

1. Where a long-term need exists in the context of a Union political or legal framework to exchange information classified as a general rule no higher than RESTREINT UE/EU RESTRICTED with a third State or international organisation, and where the Commission Security Authority, after consulting the Commission Security Expert Group, has established, in particular, that the party in question does not have a sufficiently developed security system for it to be possible to enter into a security of information agreement, the Commission may decide to enter into an administrative arrangement with the relevant authorities of the third State or international organisation in question.

2. Such administrative arrangements shall as a general rule take the form of an Exchange of Letters.

3. An assessment visit shall be conducted prior to the conclusion of the arrangement. The Commission Security Expert Group shall be informed of the outcome of the assessment visit. Where there are exceptional reasons for exchanging classified information urgently, EUCI may be released provided every attempt is made to conduct an assessment visit as soon as possible.

4. No EUCI shall be exchanged by electronic means unless explicitly provided for in the administrative arrangement.

Article 57

Exceptional ad hoc release of EUCI

1. Where no security of information agreement or administrative arrangement is in place, and where the Commission or one of its departments determines that there is an exceptional need in the context of an Union political or legal framework to release EUCI to a third State or international organisation, the Commission Security Authority shall, to the extent possible, verify with the security authorities of the third State or international organisation concerned that its security regulations, structures and procedures are such that EUCI released to it will be protected to standards no less stringent than those laid down in this Decision.

2. The decision to release the EUCI to the third State or international organisation concerned, shall, after consultation of the Commission Security Expert Group, be taken by the Commission on the basis of a proposal by the member of the Commission responsible for security matters.

3. Following the Commission's decision to release EUCI and subject to prior written consent of originator, including the originators of source material it may contain, the competent Commission department shall forward the information concerned, which shall bear a releasability marking indicating the third State or international organisation to which it has been released. Prior to or upon actual release, the third party in question shall undertake in writing to protect the EUCI it receives in accordance with the basic principles and minimum standards set out in this Decision.

CHAPTER 8

FINAL PROVISIONS

Article 58

Replacement of previous decision

This Decision shall repeal and replace Commission Decision 2001/844/EC, ECSC, Euratom ([1]).

Article 59

Classified information created before the entry into force of this Decision

1. All EUCI classified in accordance with Decision 2001/844/EC, ECSC, Euratom shall continue to be protected in accordance with the relevant provisions of this Decision.

2. All classified information held by the Commission on the date that Decision 2001/844/EC, ECSC, Euratom entered into force, with the exception of Euratom classified information, shall:

(a) if created by the Commission, continue to be considered to have been reclassified RESTREINT UE by default, unless its author had decided to give it another classification by 31 January 2002 and had informed all addressees of the document concerned;

(b) if created by authors outside the Commission, retain its original classification and thus be treated as EUCI of the equivalent level, unless the author agrees to declassification or downgrading of the information.

Article 60

Implementing rules and security notices

1. As necessary, the adoption of the implementing rules for this decision will be the subject of a separate empowerment decision of the Commission in favour of the Member of the Commission responsible for security matters, in full compliance with the internal rules of procedure.

2. After being empowered following the above-mentioned Commission Decision, the Member of the Commission responsible for security matters may develop security notices setting out security guidelines and best practices within the scope of this Decision and its implementing rules.

3. The Commission may delegate the tasks mentioned in the first and second paragraph of this Article to the Director-General for Human Resources and Security by a separate delegation decision, in full compliance with the internal rules of procedure.

Article 61

Entry into force

This Decision shall enter into force on the day following that of its publication in the *Official Journal of the European Union*.

Done at Brussels, 13 March 2015.

For the Commission

The President

Jean-Claude JUNCKER

([1]) Commission Decision 2001/844/EC,ECSC,Euratom of 29 November 2001 amending its internal Rules of Procedure (OJ L 317, 3.12.2001, p. 1).

ANNEX I

EQUIVALENCE OF SECURITY CLASSIFICATIONS

EU	TRES 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
Belgium	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)	nota (1) below
Bulgaria	Строго секретно	Секретно	Поверително	За служебно ползване
Czech Republic	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Denmark	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Germany	Streng geheim	Geheim	VS (2) — Vertraulich	VS — Nur für den Dienstgebrauch
Estonia	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Ireland	Top Secret	Secret	Confidential	Restricted
Greece	Άκρως Απόρρητο Abr: ΑΑΠ	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Spain	Secreto	Reservado	Confidencial	Difusión Limitada
France	Très Secret Défense	Secret Défense	Confidentiel Défense	nota (3) below
Croatia	VRLO TAJNO	TAJNO	POVJERLJIVO	OGRANIČENO
Italy	Segretissimo	Segreto	Riservatissimo	Riservato
Cyprus	Άκρως Απόρρητο Abr: (ΑΑΠ)	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Latvia	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Lithuania	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Luxembourg	Très Secret Lux	Secret Lux	Confidentiel Lux	Restreint Lux
Hungary	'Szigorúan titkos!'	'Titkos!'	'Bizalmas!'	'Korlátozott terjesztésű!'
Malta	L-Ogħla Segretezza	Sigriet	Kunfidenzjali	Ristrett
Netherlands	Stg. ZEER GEHEIM	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep. VERTROUWELIJK
Austria	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Poland	Ściśle Tajne	Tajne	Poufne	Zastrzeżone
Portugal	Muito Secreto	Secreto	Confidencial	Reservado

EU	TRES SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Romania	Strict secret de importanță deosebită	Strict secret	Secret	Secret de serviciu
Slovenia	Strogo tajno	Tajno	Zaupno	Interno
Slovakia	Prísne tajné	Tajné	Dôverné	Vyhradené
Finland	ERITTÄIN SALAINEN YTTERST HEMLIG	SALAINEN HEMLIG	LUOTTAMUKSELLINEN KONFIDENTIELL	KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG
Sweden ([4])	HEMLIG/TOP SECRET HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET	HEMLIG/SECRET HEMLIG	HEMLIG/CONFIDENTIAL HEMLIG	HEMLIG/RESTRICTED HEMLIG
United Kingdom	UK TOP SECRET	UK SECRET	No equivalent ([5])	UK OFFICIAL — SENSITIVE

([1]) Diffusion Restreinte/Beperkte Verspreiding is not a security classification in Belgium. Belgium handles and protects 'RESTREINT UE/EU RESTRICTED' information in a manner no less stringent than the standards and procedures described in the security rules of the Council of the European Union.

([2]) Germany: VS = Verschlusssache.

([3]) France does not use the classification 'RESTREINT' in its national system. France handles and protects 'RESTREINT UE/EU RESTRICTED' information in a manner no less stringent than the standards and procedures described in the security rules of the Council of the European Union.

([4]) Sweden: the security classification markings in the top row are used by the defence authorities and the markings in the bottom row by other authorities.

([5]) The UK handles and protects EUCI marked CONFIDENTIEL UE/EU CONFIDENTIAL in accordance with the protective security requirements for UK SECRET.

ANNEX II

LIST OF ABBREVIATIONS

Acronym	Meaning
CA	Crypto Authority
CAA	Crypto Approval Authority
CCTV	Closed Circuit Television
CDA	Crypto Distribution Authority
CIS	Communication and Information Systems handling EUCI
DSA	Designated Security Authority
EUCI	EU Classified Information
FSC	Facility Security Clearance
IA	Information Assurance
IAA	Information Assurance Authority
IDS	Intrusion Detection System
IT	Information Technology
LSO	Local Security Officer
NSA	National Security Authority
PSC	Personnel Security Clearance
PSCC	Personnel Security Clearance Certificate
PSI	Programme/Project Security Instructions
RCO	Registry Control Officer
SAA	Security Accreditation Authority
SAL	Security Aspects Letter
SCG	Security Classification Guide
SecOPs	Security Operating Procedures
TA	TEMPEST Authority
TFEU	Treaty on the Functioning of the EU

ANNEX III

LIST OF NATIONAL SECURITY AUTHORITIES

BELGIUM

Autorité nationale de Sécurité
SPF Affaires étrangères, Commerce extérieur et Coopération au Développement
15, rue des Petits Carmes
1000 Bruxelles
Tel. Secretariat: +32 25014542
Fax +32 25014596
E-mail: nvo-ans@diplobel.fed.be

BULGARIA

State Commission on Information Security
90 Cherkovna Str.
1505 Sofia
Tel. +359 29333600
Fax +359 29873750
E-mail: dksi@government.bg
Website: www.dksi.bg

CZECH REPUBLIC

Národní bezpečnostní úřad
(National Security Authority)
Na Popelce 2/16
150 06 Praha 56
Tel. +420 257283335
Fax +420 257283110
E-mail: czech.nsa@nbu.cz
Website: www.nbu.cz

DENMARK

Politiets Efterretningstjeneste
(Danish Security Intelligence Service)
Klausdalsbrovej 1
2860 Søborg
Tel. +45 33148888
Fax +45 33430190

Forsvarets Efterretningstjeneste
(Danish Defence Intelligence Service)
Kastellet 30
2100 Copenhagen Ø
Tel. +45 33325566
Fax +45 33931320

GERMANY

Bundesministerium des Innern
Referat ÖS III 3
Alt-Moabit 101 D
D-11014 Berlin
Tel. +49 30186810
Fax +49 30186811441
E-mail: oesIII3@bmi.bund.de

ESTONIA

National Security Authority Department
Estonian Ministry of Defence
Sakala 1
15094 Tallinn
Tel. +372 7170113 0019, +372 7170117
Fax +372 7170213
E-mail: nsa@mod.gov.ee

GREECE

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
Tel. +30 2106572045
+ 30 2106572009
Fax +30 2106536279, +30 2106577612

SPAIN

Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Avenida Padre Huidobro s/n
28023 Madrid
Tel. +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
Tel. +33 171758177
Fax + 33 171758200

CROATIA

Office of the National Security Council
Croatian NSA
Jurjevska 34
10000 Zagreb
Croatia
Tel. +385 14681222
Fax + 385 14686049
Website: www.uvns.hr

IRELAND

National Security Authority
Department of Foreign Affairs
76 — 78 Harcourt Street
Dublin 2
Tel. +353 14780822
Fax +353 14082959

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)
4 Emanuel Roidi street
1432 Nicosia
Tel. +357 22807569, +357 22807643,
+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
LV-1001 Riga
Tel. +371 67025418
Fax +371 67025454
E-mail: ndi@sab.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 66701, +370 706 66702
Fax +370 706 66700
E-mail: nsa@vsd.lt

LUXEMBOURG

Autorité nationale de Sécurité
Boîte postale 2379
1023 Luxembourg
Tel. +352 24782210 central
+ 352 24782253 direct
Fax +352 24782243

HUNGARY

Nemzeti Biztonsági Felügyelet
(National Security Authority of Hungary)
H-1024 Budapest, Szilágyi Erzsébet fasor 11/B
Tel. +36 (1) 7952303
Fax +36 (1) 7950344

Postal address:
H-1357 Budapest, PO Box 2
E-mail: nbf@nbf.hu
Website: www.nbf.hu

MALTA

Ministry for Home Affairs and National Security
P.O. Box 146
MT-Valletta
Tel. +356 21249844
Fax +356 25695321

NETHERLANDS

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Postbus 20010
2500 EA Den Haag
Tel. +31 703204400
Fax +31 703200733

Ministerie van Defensie
Beveiligingsautoriteit
Postbus 20701
2500 ES Den Haag
Tel. +31 703187060
Fax +31 703187522

AUSTRIA

Informationssicherheitskommission
Bundeskanzleramt
Ballhausplatz 2
1014 Wien
Tel. +43 1531152594
Fax +43 1531152615
E-mail: ISK@bka.gv.at

POLAND

Agencja Bezpieczeństwa Wewnętrznego — ABW
(Internal Security Agency)
2A Rakowiecka St.
00-993 Warszawa
Tel. +48 22 58 57 944
Fax +48 22 58 57 443
E-mail: nsa@abw.gov.pl
Website: www.abw.gov.pl

PORTUGAL

Presidência do Conselho de Ministros
Autoridade Nacional de Segurança
Rua da Junqueira, 69
1300-342 Lisboa
Tel. +351 213031710
Fax +351 213031711

ROMANIA

Oficiul Registrului Național al Informațiilor Secrete de Stat
(Romanian NSA — ORNISS National Registry Office for Classified Information)
4 Mures Street
012275 Bucharest
Tel. +40 212245830
Fax +40 212240714
E-mail: nsa.romania@nsa.ro
Website: www.orniss.ro

SLOVENIA

Urad Vlade RS za varovanje tajnih podatkov
Gregorčičeva 27
1000 Ljubljana
Tel. +386 14781390
Fax +386 14781399
E-mail: gp.uvtp@gov.si

SLOVAKIA

Národný bezpečnostný úrad
(National Security Authority)
Budatínska 30
P.O. Box 16
850 07 Bratislava
Tel. +421 268692314
Fax +421 263824005
Website: www.nbusr.sk

FINLAND

National Security Authority
Ministry for Foreign Affairs
P.O. Box 453
FI-00023 Government
Tel. 16055890
Fax +358 916055140
E-mail: NSA@formin.fi

SWEDEN

Utrikesdepartementet
(Ministry for Foreign Affairs)
SSSB
S-103 39 Stockholm
Tel. +46 84051000
Fax +46 87231176
E-mail: ud-nsa@foreign.ministry.se

UNITED KINGDOM

UK National Security Authority
Room 335, 3rd Floor
70 Whitehall
London
SW1A 2AS
Tel. 1: +44 2072765649
Tel. 2: +44 2072765497
Fax +44 2072765651
E-mail: UK-NSA@cabinet-office.x.gsi.gov.uk