Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information

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;

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[(2)].

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.

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

(**2**) 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).

Changes to legislation:
There are currently no known outstanding effects for the Commission Decision (EU, Euratom) 2015/444, CHAPTER 5.