Council of the
European Union

Brussels, 6 July 2015
(OR. en)

10416/15

CSCI 43
CSC 162

"I/A" ITEM NOTE

From:	The Council Security Committee
To:	COREPER/Conseil
Subject:	Information Assurance Security Policy on Communication and Information System Security Engineering

1. The Council Decision on the security rules for protecting EU classified information[1] requires that "where necessary, the Council, on recommendation by the Security Committee, shall approve security policies setting out measures for implementing this Decision." (cf. Article 6(1)).

2. The Council Security Committee has agreed to recommend a policy laying down standards for Communication and Information Systems (CIS) Security Engineering for the protection of EU classified information (EUCI) on CIS in terms of confidentiality, integrity, availability and, where appropriate, authenticity and non-repudiation.

3. Subject to confirmation by COREPER, the Council is invited to approve the attached security policy.

[1] Council Decision 2013/488/EU, OJ L 274 of 15.10.2013, p.1.

This page intentionally left blank

IA Security Policy on Communication and Information System Security Engineering

IASP 5

I PURPOSE AND SCOPE

1. This policy, approved by the Council in accordance with Article 6(1) of the Council Security Rules (hereinafter 'CSR'), lays down standards for protecting EU classified information (EUCI). It constitutes a commitment to help achieve an equivalent level of implementation of the CSR.

2. This policy defines specific security principles and activities to be integrated in an organisation's CIS engineering framework to ensure that security issues are taken into account in due time when developing CIS.

3. The Council and General Secretariat of the Council (GSC) will apply this security policy with regard to protection of EUCI in their premises and communication and information systems.

4. Member States will act in accordance with national laws and regulations to the effect that the standards laid down in security policies are respected when EUCI is handled in national structures, including in national CIS.

5. EU Agencies and bodies established under Title V, Chapter 2, of the TEU, Europol and Eurojust should use this security policy as a reference for implementing security rules in their own structures.

6. System Security Engineering (SSE) must ensure that the security posture of a CIS is aligned to its risk-based security expectations. The lack of such an alignment, due to the non expected existence or absence of capabilities, leaves potential paths open for undetected misuses of the CIS. This policy specifies minimum principles and activities to be performed during the engineering phase of a CIS (as defined in the IA security policy on CIS life cycle[1]) to reduce, on a risk management basis, these potential paths.

[2] See Doc 16268/12.

7. This policy does not describe a specific SSE framework. Rather the organisation must integrate this policy in its CIS engineering framework and ensure that relevant resources are in place to support its implementation. Appropriate guidelines will detail, by security objective, common minimum implementation of these principles and activities.

II SYSTEM SECURITY ENGINEERING

System security engineering principles

8. The organisation must develop procedures to implement the principles defined below. Any deviation of these principles must be justified in the CIS security documentation.
   (a) continuous challenge of security: any security assumptions and evidences must be challenged on a regular basis as deemed appropriate by the accreditation authority;
   (b) secure layouts: best practices in architecture and design layouts must be followed, implementing at least the concepts of defence in depth, layering/segmentation, minimality and simplicity. The rationales behind the choice of layouts must be documented;
   (c) security product: CIS must be based on qualified products in accordance with the respective IA policy and as recorded in the Enterprise Security Architecture (ESA). The selection of a product that does not fulfil this requirement must be documented and justified by the responsible IA Operational Authority and is subject to approval within the accreditation process. The implementation is defined through agreed and up to date configuration(s) and mastered by trained personnel;
   (d) security training: personnel involved in engineering activities that address or impact security (e.g. architecture, design, coding, configuration, testing, procurement...) must be trained up to an appropriate level; a record of such training should be kept;

(e) security services: each CIS must implement, at least, identification and authentication, access control and accountability security services. Corresponding mechanisms must meet the level of strength and assurance requested by the System-specific Security Requirement Statement (SSRS);

(f) security roles: system development and quality assurance (including accreditation) roles may not be performed by the same actors;

(g) separation of systems: operational and testing systems should be different. If the operational system is also used to perform upgrade testing (e.g. patch, new release of software…), the security documentation must include all the tasks to be performed to avoid the compromise of the CIS security objectives.

CIS security context view

9. The security of a CIS can be jeopardised far before the system is released for operational use: inadequate assessment of potential vulnerabilities in the engineering and future operational environments can open opportunities for the integration (or persistence) of unwanted components or functionalities that could impact the security posture.

10. To identify and accurately assess these potential vulnerabilities, the organisation must develop, and keep up to date, a CIS Security Context view. Integrated in the ESA, the view must:

(a) identify and monitor all assets used during the CIS life cycle, being either technical (e.g. re-used algorithms, coding standards, tools such as compiler...), personnel (e.g. know-how, clearance...), facilities (e.g. protection level, access...) or procedures (e.g. procurement, supply chain, patching...);

(b) define the level of trustworthiness attributed to these assets;

(c) be supported by appropriate procedures to define how to introduce, modify or withdraw assets;

(d) be challenged, in terms of security assumptions and assurance, to guarantee its continuous compliance with the organisation's risk appetite.

11. When developing a new CIS (or a new component of an existing CIS) the view will be used to complement the conceptual security architecture developed during the justification phase with additional architectural requirements to counter potential vulnerabilities and threats. These additional requirements must be addressed in the system specific risk assessment and documented in the SSRS.

System security engineering activities

12. To ensure proper integration of security into systems, the organisation CIS architectural framework and project management procedures must include at least the following activities:
    (a) selection of languages for business and architectural modelling able to represent CIS security concerns;
    (b) production of detailed architecture and design views incorporating security services and mechanisms;
    (c) development of a security assurance case framework to define how claims and supporting evidences must be expressed and tested.

13. The organisation must develop a strategy for the development of CIS (or components of) by either internal resources or external supplier(s). This strategy must address the security aspects of at least the following aspects:
    (a) internal ability to develop CIS compliant with specific security objectives;
    (b) criteria to select between internal or external development of a CIS;
    (c) procurement provisions to ensure adequate consideration of security requirements when selecting an offer;
    (d) provisions to be included in contracting documents to define the rights and obligations of suppliers.

14. To frame the development of CIS the organisation must
    (a) develop a repository of documented and mastered architecture and solutions fulfilling the most generic business needs of the organisation;
    (b) define a catalogue of mastered security controls that can be used to implement a security posture. These controls must be supported by relevant procedures on how to provide evidence of efficiency;
    (c) define approved environments for CIS development, detailing the assets (i.e. facilities, software, tools, personnel ...) to be used to guarantee system integrity and confidentiality of testing during its development. These approved environments will be aligned with the CIS Security Context view.

15. During the development of a system, procedures must ensure that
    (a) any deviation from the ESA repository must be justified, any use of a new product or variant having to be either supported by a proof of capability in terms of security configuration and operation or explicitly accepted by the Security Accreditation Authority;
    (b) when a complex system has to be broken down, the security objectives of components remain in line with those of the whole system;
    (c) when architecture or design undergoes major evolutions, updated views have to be endorsed by stakeholders to confirm that their security concerns are still adequately addressed.

System security testing

16. The organisation must plan progressive security testing during the development of the system. The tests that must be performed to guarantee the CIS security posture when the system is installed in the operational facilities must be documented in a CIS installation testing document. This document will be part of the Security Operating Procedures (SecOPs).

17. Security assurance case(s) must be developed to define how security claims can be supported by evidence. Evidence should be measurable, reproducible and rely on tangible metrics. The cases must ensure that the strength and assurance of security mechanisms are as required in the SSRS.

18. The organisation must ensure that
    (a) the testing objectives, procedures and tools are in line with the security assurance case;
    (b) testing is performed by trained personnel;
    (c) partial testing of security must be performed as soon as possible in the development process to avoid partial development decisions whose consequences could impede the CIS security objectives;
    (d) when outsourced, testing must be supported by procedures ensuring adequate control of the executed tests and classification of the test data.

Engineering phase deliverables

19. The system released for operational use must be provided with at least the following security documentation:
    (a) SSRS;
    (b) SecOPs;
    (c) Security Resources Plans to substain the security, including detailed conditions and assurance of procurement and outsourcing if any.