COUNCIL OF THE EUROPEAN UNION

Brussels, 16 November 2012

16268/12

CSCI 48
CSC 79

"I/A" ITEM NOTE

From :	The Council Security Committee
To :	COREPER/Council
Subject :	Information Assurance Security Policy on Security throughout the Communication and Information System Life Cycle

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 security throughout the communication and information system life cycle for the protection of EU classified information (EUCI) on communication and information systems (CIS) in terms of confidentiality, integrity, availability and, where appropriate, authenticity and non-repudiation.

[1] Council Decision 2011/292/EU, OJ L 141 of 27.5.2011, p. 17

3. By specifying mandatory activities to be performed during the CIS life cycle, this policy aims at increasing the confidence between partners that secure CIS are developed using an agreed process and that incurred expenses can be traced back to business needs and security obligations.

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

This page intentionally left blank

IA Security Policy on Security throughout the Communication and Information System (CIS) Life Cycle

IASP L

TABLE OF CONTENTS

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 on security throughout the communication and information system life cycle defines the minimum security-related activities which must be performed during the life cycle of a communication and information system (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. The Member States will act in accordance with national laws and regulations to the effect that the standards laid down in this security policy with regard to protecting EUCI 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. This policy does not refer to a particular CIS life cycle model but rather uses generic phases of a life cycle which are:
   (a) Phase 1: elicitation of the business needs;
   (b) Phase 2: construction of a compliant CIS;
   (c) Phase 3: use and maintenance of this CIS;
   (d) Phase 4: disposal of this CIS.

7. Each phase includes the minimum security-related activities and deliverables that CIS personnel must integrate in the particular CIS life cycle model and approach (V-model, waterfall,…) used in an organisation.

8. The control of the execution of these activities must be part of every CIS accreditation strategy.

9. The definitions set out in the annex are used for the purposes of this policy.

II SYSTEM SECURITY LIFE CYCLE

10. To ensure proper integration and maintenance of security, the CIS life cycle must include the activities defined in the phases below.
    (a) Phase 1: system security justification: the business needs and risks are assessed to elicit technology independent security requirements for the system;
    (b) Phase 2: system security engineering: the system is prepared to satisfy the defined requirements before being released to the owner for day-to-day usage within authorised limits of use;
    (c) Phase 3: system security sustainment: the system is operated as authorised; various activities are performed to keep its security posture at an acceptable level;
    (d) Phase 4: system secure disposal: the system is removed from service, using authorised procedures.

11. Each phase defines the minimum activities to be performed (not necessarily in a sequential way) and minimum deliverables. An appropriate organisational structure has to be put in place to provide the relevant resources in support of these activities.

12. Each phase ends with a decision point, where stakeholders agree that security is on the right track and authorise the start, in whole or part, of the next phase.

13. An Enterprise Security Architecture (ESA) must be developed in support of this security integration in the CIS life cycle, based on an understanding of the organisation's needs, acting as a rational framework for the selection of security solutions. This will help the CIS security optimisation at the organisation level considered as a whole rather than to achieve local optimisation at business unit level.

14. Additional policies or guidelines may be developed to support either a specific phase activity (such as software security in the engineering phase, continuous monitoring in the sustainment phase), or for more than one phase (such as configuration management) or for the whole life cycle (such as security accreditation).

III PHASE 1: SYSTEM SECURITY JUSTIFICATION

15. The main goal of system security is to support the organisations' missions. In order to tailor security in a targeted way, three factors must be considered:
    (a) the context in which the system has to be built and used;
    (b) the goals to achieve in terms of business needs;
    (c) the technical capabilities and maturity needed to construct and operate the system.

16. As a minimum, the following activities must be performed:

(a) Business users and security trained CIS personnel must assess, at the inception of the system, the business functional needs, including expected future needs, taking into consideration the type of system and for what, by whom, when, where, why, and how it will be used.

(b) Security requirements - both functional and non-functional – will be derived from these needs, using a risk management approach taking into account the contextual aspects (organisation culture and strategy, organisation resources, security policies and laws, IT and security master plans, place of use…) which have an influence on the future solution. A methodology must be employed, and results documented, to allow an external review of how these requirements have been elicited;

(c) The strategy and steps to be followed in order to be accredited;

(d) A conceptual security architecture, described in terms of business information flows and the supporting security requirements, has to be developed in adequacy with the CIS and security feasibility and maturity of the organisation. Any deviation from the ESA has to be justified.

17. As a minimum, the following documentation must be produced:

(a) business functional needs;

(b) description of the applicable context;

(c) risk assessment, focusing on the risks to business assets and processes;

(d) conceptual security architecture;

(e) first iteration of the System Specific Security Requirements Statement (SSRS).

18. Appropriate authorities (the SAA and the CIS management as a minimum) must agree on the feasibility and viability of these requirements and architecture before starting the next phase.

IV PHASE 2: SYSTEM SECURITY ENGINEERING

19. The conceptual security architecture is translated into an actual CIS, with the ESA as the main reference. As different security solutions lead to increased complexity and cost in terms of support, in particular with regard to security administration and management, any deviation from the ESA must be justified. Any use of new products or variants must be supported by a proof of capability in terms of security configuration and operation.

20. As a minimum, the following activities must be performed:
    (a) The conceptual security architecture and its security requirements are to be translated into security principles and controls, chosen and implemented by the appropriate mix of people, procedures and technology. Mastered IT products configurations have to be applied and fine-tuned where relevant;
    (b) When there is a major design evolution, views must be presented to allow stakeholders to confirm that, from their viewpoint, all concerns and responsibilities are adequately addressed;
    (c) The security risk assessment has to be progressively refined to identify potential additional risks. The rationales leading to the risk treatment decisions must be documented;
    (d) The resources (personnel and know-how, equipment and budget) required to sustain security over the CIS life cycle must be planned, including detailed conditions and assurance of procurement and outsourcing if any;
    (e) The security controls have to be progressively tested as defined in the accreditation strategy to validate their presence and effectiveness. The testing must be based on agreed methodologies and practices. When security relies on users' participation, such testing must also assess the user acceptance;
    (f) The security configuration is documented in a configuration plan which acts as the official security reference baseline;
    (g) Operational plans on how to use and administer the security controls, how to protect and sustain the on-going security posture, are developed;

21. As a minimum, the following documentation must be produced:
    (a) System Specific Security Requirements Statement (SSRS);
    (b) Security Operational Procedures, including all relevant operational plans;
    (c) Security Test Plans for validation of the security posture and contingency activities;
    (d) Security Resources Plans (budget, contracts…).

22. The SAA must endorse the conformity of the proposed CIS against the security context before a CIS can be accredited and formally authorise its release for day-to-day usage and sustainment of its security posture.

V PHASE 3: SYSTEM SECURITY SUSTAINMENT

23. During day-to-day operations, actions performed on the CIS might have an impact on its security. Actions must be performed in accordance with the security operational procedures in order to keep the security in line with the accreditation. Deviations from authorised actions are subject to detection and reported as appropriate.

24. As a minimum, the following activities must be performed:
    (a) Security administration has to be carried out in conformity with the operational plans;
    (b) Maintenance of the security configuration must be in conformity with the configuration plan. Authorised changes and improvements must lead to the update of the configuration plan, whereas significant modifications have to be addressed to the CIS and business authorities for further (re)consideration;
    (c) Risk management activities and compliance testing must be regularly performed to ensure that security controls are still effective and that the gap between the security baseline and the actual security posture remains acceptable;
    (d) The system must be monitored on a permanent basis on its security performance and on actions made by entities (user, processes,…) to detect unexpected activities and react to malicious ones in conformity with the contingency plans.

25. As a minimum, the following information must be periodically produced, even if no modification has to be reported:
    (a) Malicious actions;
    (b) Availability of resources in support of security;
    (c) Update of the configuration plan.

26. The SAA must periodically validate the security posture of the CIS and confirm its relevance against its security context and the security requirements.

27. When relevant, appropriate authorities may authorise the disposal of, in whole or part, the CIS when they are confident that this will have no impact on the security posture of the system.

VI PHASE 4: SYSTEM SECURE DISPOSAL

28. When the system is disposed of, specific activities are performed to ensure that security will not be compromised.

29. As a minimum, the following activities must be performed:
    (a) The information and system components must be handled according to their future use (archiving, transfer, destruction,…);
    (b) Resources are to be released as appropriate;
    (c) The last CIS configuration must be recorded for archiving with the configuration plan.

30. As a minimum, signed certificates of completion of disposal activities must be produced.

31. The SAA must control that the disposal activities have been performed in accordance with the security policies before closing the security aspects of the CIS life cycle.

ANNEX

DEFINITIONS

Architecture	The fundamental organisation of a system, embodied in its components, their relationships to each other and the environment, and the principles governing its design and evolution.
Conceptual security architecture	Layout of the different elements and enforcement points of security services and their relationship to the information to be protected, without any construction details.
Enterprise Architecture (EA)	A coherent whole of principles, methods, and models that are used in the design and realisation of an enterprise's organisational structure, business processes, information systems, and infrastructure.
Enterprise Security Architecture	Security view of the EA, including both security processes management of and technical approach to information security.
Life Cycle	Evolution of a system, product, service, project or other human-made entity from conception through retirement.
Life Cycle model	Framework of processes and activities concerned with the life cycle that may be organised into stages, which also acts as a common reference for communication and understanding.