Council of the
European Union

Brussels, 6 March 2015

6488/15

CSCI 9
CSC 45

"I/A" ITEM NOTE

From:	The Council Security Committee
To:	COREPER/Council
Subject:	Information Assurance Security Policy on Interconnection

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

2. The Council Security Committee has agreed to recommend a policy laying down standards for interconnection of CIS handling EU classified information (EUCI) 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 Interconnection

IASP 3

TABLE OF CONTENTS

1. 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. The purpose of this policy is to define the rules and constraints for the interconnection of a CIS handling EUCI to another CIS. It also defines a model (see Annex I) used as a common language to describe an interconnection. The document only covers the additional risks to CIS that result from interconnection.

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 (CIS).

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. A system interconnection is defined as the direct[2] connection of two or more IT systems for the purpose of sharing data[3] and other information resources (e.g. communication) in a unidirectional or multidirectional way. The primary reason to interconnect systems is a provision or consumption of the following types of services:

   (a) a service of information exchange,

   (b) a service of technical communication infrastructure provision (there is no intention to exchange any information).

7. This policy does not cover information exchange using removable media.

8. This policy applies to a communication and information system handling EUCI (CIS) that is interconnected with another information system (IS), not necessarily handling EUCI.

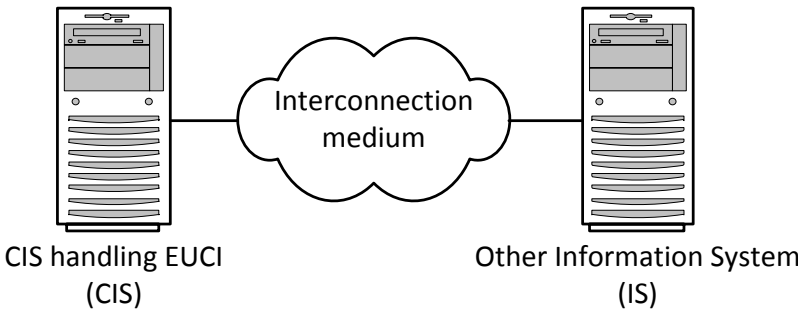

Figure 1 Generic interconnection model

[2] As opposed to cascaded.

[3] Data in this document means the specific representation of information (e.g. a string of bytes), it must have a defined format that specifies how information is encoded.

9. A connection between two IT systems must be considered to be an interconnection when the systems differ in at least one of the following characteristics:

(a) the maximum level of EUCI handled,

(b) security objectives[4],

(c) security mode of operation,

(d) the relevant Security Accreditation Authority (SAA),

(e) the applicable security policies (e.g. an EU and a Member State national system),

(f) the relevant system operational authorities (SOA e.g. the GSC, decentralised EU Agency),

(g) legal requirements,

(h) any other relevant security parameters (need to know or a community of interest, constraints, specific protocols, legacy equipment, level of physical protection, type of bearer network, ownership of the information being disseminated).

Any change in the CIS introducing new components[5], that does not meet any of the criteria defined above, is in principle not considered as an interconnection.

In any other case the decision whether or not a connection or an internal link constitutes an interconnection must be made by responsible SAA(s).

[4] As defined in the System Specific Security Requirements Statement
[5] For example a new workstation, new network equipment, etc

10. Regardless of the intended direction of the information flow, the interconnection may open a bidirectional communication channel[6] between the two CIS and potentially allow access to many services and information that unintentionally go beyond the scope of the business requirements.

11. The interconnection may therefore change the CIS risk assessment in the following way:

    (a) the threat sources for the IS can be transferred to the CIS,

    (b) the vulnerabilities in the IS can increase the likelihood of some risk scenarios and/or their impact on the CIS,

    (c) the vulnerabilities in the IS and the interconnection itself can introduce a number of new risk scenarios for the CIS,

    (d) interconnection introduces a dependency both at the business and technical levels and can therefore introduce availability risks,

    (e) leveraging the functionalities and vulnerabilities of both interconnected systems may produce synergy and new vectors of attack,

    (f) the components used to build the interconnection and/or to mitigate the risks introduced by the interconnection can be themselves the targets of an attack and they can introduce new vulnerabilities.

12. The Boundary Protection Service (BPS) is a service that mitigates security risks introduced by the interconnection. The controls that provide the BPS are called Boundary Protection Components (BPC, e.g. backup procedure, antivirus, physical access control). The special BPCs that mediate information flows and/or provide the security services at the interconnection point are called Boundary Protection Devices (BPD, e.g. firewall, one-way flow regulator).

[6] For example when the interconnection relies on the TCP protocol.

2. POLICY

13. A CIS must treat any interconnected IS as untrusted, thus any assumptions about IS should be appropriately addressed as part of the risk management process. The CIS must implement appropriate controls (e.g. SLAs, Boundary Protection Services) to ensure that the assumptions about the IS are true.

14. A valid business requirement must drive the decision to interconnect CIS.

15. The CIS must prevent the exchange of information and access to services that are not explicitly defined by the business requirements. Prevention of leakage of higher classified information or services to a lower classified system must be assured.

16. Interconnection between a CIS and a lower or unclassified IS is not authorised unless the CIS has installed approved Boundary Protection Services between the CIS and the IS, for example by using an approved one-way flow regulator. The BPS selected must mitigate the identified risks to an acceptable level.

17. The interconnection must undergo an accreditation process and requires the approval of the competent SAA.

18. The risk management process for the CIS must be repeated for every new interconnection. As a minimum, the process must take into account the aspects described in Annex II.

19. When an interconnection introduces new high level risks for the CIS, the CIS may require re-accreditation. The re-accreditation of the CIS is necessary when it is interconnected to a an unaccredited IS.

20. A CIS accredited to handle TRES SECRET UE/EU TOP SECRET must not be interconnected to an unprotected or a public network (neither directly nor indirectly - via another IS).

21. When the IS offers only communication infrastructure to carry the data and the data is encrypted by a cryptographic product approved in accordance with Article 10 of the CSR, such a connection is not be deemed to be an interconnection.

22. If new interconnections to an IS, which is already interconnected to a CIS are planned, the relevant CIS Security Accreditation Authority (SAA) must be informed. The same should be offered to the IS SAA in case the CIS is interconnected again.

23. Only the protocols, network service, and the information or data flows required to carry out the operational mission may be installed, configured and used with the interconnection (principle of minimality).

24. Users and processes that make use of or are part of the interconnection may only be given those privileges and authorisations that they require to perform their tasks and duties (principle of least privilege).

25. An interconnected CIS must implement measures to block any activities and information flows that are not a legitimate part of running the interconnection (principle of self-protection).

26. Protection measures must be implemented on various components of the interconnection architecture[7] to avoid that there is only a single line of defence (principle of defence-in-depth).

27. The implementation of an interconnection must be verified[8] by the responsible SAA at the initial implementation of the interconnection and periodically thereafter. The SAA should be involved already during planning and design phase and in the risk assessment of the interconnection.

[7] The architecture, apart from interconnection itself, embraces also the CIS and IS

[8] Checking if implementation reflects the design and the decisions of deploying controls in the risk treatment process

28. Interconnection development is either a part of the CIS development project or a separate project when it is added to an already deployed CIS. Project management methodology, service management and the interconnection lifecycle are outside the scope of this document. However, the interconnection lifecycle includes the security lifecycle phases described in IASP-L[9]:

(a) interconnection security justification - the objective of the security justification is to elicit all the security requirements for the interconnection and the necessary security requirements for the IS,

(b) interconnection security engineering - the business security requirements are translated into security principles and controls, chosen and implemented by the appropriate mix of people, procedures and technology. At the end of this phase, the interconnection should be operational in the production environment and accredited to a required level,

(c) interconnection security sustainment - after the interconnection is established, it must be actively maintained and monitored to ensure that it operates properly and securely,

(d) interconnection secure disposal - when the need to interconnect is no longer valid or one of the interconnected CIS is entering its disposal phase, the interconnection is removed from service, using authorised procedures.

[9] IASP-L IA Security Policy on Security throughout the CIS Life Cycle (doc. 14968/2012)

DEFINITIONS

Accreditation	The process leading to a formal statement by the Security Accreditation Authority (SAA) that a system is approved to operate with a defined level of classification, in a particular security mode in its operational environment and at an acceptable level of risk, based on the premise that an approved set of technical, physical, organisational and procedural security measures has been implemented;
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.
Communication and information system	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. See Article 10(2) of CSR.
CIS	A communication and information system handling EUCI.
Confidentiality	The property that information is not disclosed to unauthorised individuals, entities or processes;
EU classified information (EUCI)	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. See Article 2(1) of CSR
Integrity	The property of safeguarding the accuracy and completeness of information and assets;
Non-repudiation	The ability to prove an action or event has taken place, so that this event or action cannot subsequently be denied.
Risk	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.

Annex I

INTERCONNECTION MODEL

1. This annex defines a possible model to describe interconnection. The objective of the model is to uncover the risks to CIS generated by the interconnection.

2. An interconnection can be described by two parameters, "Security Conditions" and "Role" (see Figure 2), where the "Security Conditions" represent the set of attributes such as: differences in accreditation levels, ownership, modes of operation etc and the "Role" describes the role of the CIS in the interconnection, defined by:

   (a) "flow direction" (direction of flow of information) from the point of view of the CIS and

   (b) "service provision" - the role of the CIS in providing or consuming the service delivered by the interconnection.

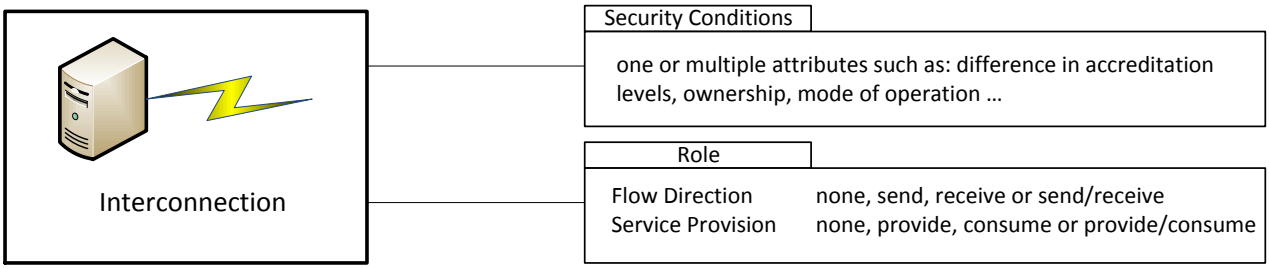

Figure 2 The parameters describing an interconnection

3. The interconnection model required at the business (logical) level should be respected by the technical implementation. This means that the technical implementation should not offer more flow directions or services than required. Any deviations from the business requirements at the technical level should be treated as risk and appropriately mitigated by Boundary Protection Services.

4. The values of the attribute Role are explained below in Table 1.

Attribute	**Value**	**Description**
flow direction	none	There is no business requirement for any exchange of information between the CIS and IS. There may however be an interconnection at the infrastructure level (that can cause an unintentional information flow).
	receive	The CIS receives some information from the IS.
	send	The CIS sends some information to the IS[10].
	send/receive	The CIS sends and receives the information
service provision	none	As there is no service consumed or provided, there is no business reason to interconnect two systems. Such situation is not allowed and the interconnection must not be established.
	consume (service consumer)	The CIS consumes a service provided by the IS. In most implementations the CIS will act as a client of the IS (but there are different models possible).
	provide (service provider)	The CIS offers a service for the IS. The service objective can be information exchange or infrastructure provision (e.g. communication infrastructure). In case of information exchange, the CIS acts typically as a server (but there are different models possible).
	provide/consume	The CIS is required to provide services and at the same time expects some services from the IS.

Table 1 The possible values of the attribute "Role" in the interconnection

[10] Note that a confirmation of receipt (if required) is considered as a flow of information from the receiver to the sender

5. The constraints and requirements for additional security measures for the "Roles" and the "Security Conditions" will be described in supporting IA Security Guidelines.

6. The fact that two different interconnections are described by the same "Role" and "Security Conditions" makes the interconnections similar from the security point of view but it does not make them identical. Therefore, apart from checking the compliance with the guidelines, in each case the decision whether or not an interconnection is "secure enough" must be made as a result of a risk management process.

ASPECTS TO BE CONSIDERED DURING THE RISK MANAGEMENT

1. The impact that the interconnection has on risk management (of the CIS) depends very much on the actual situation (business requirements, technical implementation). This annex defines a generic list of concerns that must be taken into account when applicable. The details linked to specific models and implementations will be laid down in the guidelines.

2. The scope of the risk management process will most likely change when an interconnection is introduced, in particular the following elements need to be analysed:

   (a) Information Assets - they may be new assets in the scope of the risk management process,

   (b) Business processes - most likely one or more of the business processes are changed to justify the interconnection,

   (c) Contractual obligations - the interconnection may imply a contractual obligation for the CIS owner,

   (d) Interfaces - the interconnection constitutes a new interface.

3. The threat identification process should take into account the following unwanted events:

   (a) unauthorised users or programs running in the IS try to access services of the CIS,

   (b) unauthorised users or programs running in the CIS try to access services of the IS,

   (c) the non-releasable information to IS is transferred (by mistake or deliberately) to the IS,

(d) the non-releasable information to CIS is transferred from IS,

(e) the IS becomes unavailable (is there any impact on CIS?),

(f) the service offered by the IS is time or resource consuming or never completes,

(g) the information received from the IS is crafted maliciously (deliberately or accidentally) to exploit vulnerabilities in the CIS,

(h) the information sent from CIS to the IS is crafted maliciously to exploit vulnerabilities in the IS,

(i) the fact that a transaction (e.g. an information exchange) has taken place becomes known to the users of the IS,

(j) the transactions (e.g. of sending or receiving) are denied by IS,

(k) the CIS is unable to receive or process information sent from the IS (e.g. a service is unavailable),

(l) the amount of information or the number of requests to the CIS from the IS is larger than expected and leads to saturation,

(m) the BPS and other components used to build the interconnection have exploitable vulnerabilities allowing to attack the CIS,

(n) the information about technologies, infrastructure, architecture vulnerabilities of the CIS become known to the users of the IS,

(o) the IS is successfully attacked and becomes a source of the attack on the CIS,

(p) the agreed protocols of information exchange are not followed.

4. A Boundary Protection Service alone is unlikely to provide sufficient protection from, or detection of all possible attacks therefore, the following controls must be considered in the risk treatment:

   (a) the architecture of the CIS may require to be redesigned (e.g. to enable adequate defence-in-depth),

   (b) there may be a need for awareness and training for the users and administrators of the CIS to make them aware of the new risks and to explain to them their responsibilities with regards to the interconnection.

_____