COUNCIL OF THE EUROPEAN UNION

Brussels, 30 March 2012

8408/12

CSCI 11
CSC 20

I/A ITEM NOTE

From :	Council Security Committee
To :	COREPER/Council
Subject :	Information Assurance Security Policy on Network Defence

1. The Council Decision on the security rules for protecting EU classified information [1] require 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 Network Defence 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.

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

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

This page intentionally left blank

IA Security Policy on Network Defence

IASP 4

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 sets out minimum standards to be observed for the purpose of network defence of such CIS and interconnections between them.

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. 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. Network defence[2] means a coordinated set of measures, processes and activities which

   (a) enhance the resilience of CIS to cyber attack;
   (b) enable early detection of cyber threats to and vulnerabilities of CIS;

[2] While the terms are interchangeable, cyber defence usually refers only to external attacks, network defence usually both for internal and external ones.

(c) enable early detection of attacks and rapid response, to minimise the damage caused to the CIS; and

(d) enable the actual impact of breaches of security to be assessed.

7. Network defence measures are needed owing to the increasing complexity and interdependence of CIS, the widespread availability of powerful attack toolkits, the increasing involvement of criminal and intelligence organisations with access to extensive resources, as well as the increasingly frequent, cross-border, targeted and sophisticated nature of current attacks on CIS.

II. POLICY

8. Network defence measures are to be implemented for each CIS for its protection. The measures must be based on and integrated into the ongoing risk management process and the security accreditation strategy of each CIS.

9. Network defence measures will be reviewed periodically in order to ensure that they are sufficient and proportional to the existing threat scenario. They will also be reviewed when there is a change in the threat scenario to which the CIS in question is exposed, as well as after any incident affecting the security of the information handled by the CIS.

10. For network defence, the following will be in place for every CIS:

(a) CIS will be set up using the built-in monitoring features technically available while observing legal constraints and requirements on the collection and retention of monitoring data of a personal or sensitive nature;

(b) based on a risk-management approach and on the value of the information handled by the CIS, the extent and detail of reporting of the events collected by the monitoring features above will be prioritised and alerts of different urgency and importance generated on the basis of this analysis;

(c) information collected by routine monitoring as well as during incident investigation will be handled securely and in a manner which enables its subsequent use in internal or legal proceedings against any identified perpetrators of security incidents;

(d) users of all levels will be trained in how to use the CIS with the aim of ensuring their understanding the security risks pertinent to it and what to do when they detect unexpected or abnormal behaviour.

11. The Security Authority is ultimately responsible for the correct functioning and implementation of the network defence measures.

12. For this purpose, network defence activities will be supported by

(a) sufficient human resources with expertise in special areas of knowledge as provided by their initial training and continuous professional education;

(b) processes and procedures for building and maintaining security of CIS and their resilience to malfunction or attack;

(c) tools to detect and alert about malfunction of CIS and take action in real time to stop or limit the malfunction;

(d) processes for handling events which could be CIS security incidents;

(e) processes for communication of security events with affected parties and other partners; and

(f) management support and review.

13. Network defence measures will be implemented to ensure:

(a) security assurance:

i design and development aimed at building CIS which are able to detect, repel and survive inadvertent and /or malicious incidents using system hardening to reduce the attack surface and to provide defence in depth;

ii provision of technical protection such as:

- access control using the principle of minimality and least privilege as well as logging to record successful and unsuccessful access;
- intrusion detection and prevention, both for incoming and outgoing information at internal and external interfaces of the CIS;

iii awareness and functional training of users in secure use of CIS as well as in detecting and reporting unusual behaviour.

(b) security maintenance:

i asset, configuration and change management, preferably with record keeping of the exact configuration of all components of CIS at any point in their lifetime;

ii network discovery, mapping and monitoring to detect at least:

- unauthorised changes;
- successful or unsuccessful attempts at unauthorised access;
- vulnerability of components of the CIS to known avenues of attack and
- unexpected or unusual system behaviour.

iii vulnerability alert[3] management and corrective action against known vulnerabilities of CIS components in a timely manner.

[3] Special alerting services of component vendors should be used if required and justified by the security level of the CIS in order to obtain early alerts

(c) security restoration:

i incident response processes;

ii processes for incident investigation and follow-up ;

iii contingency, business continuity and disaster recovery processes;

iv processes to ensure documentation of relevant information about security incidents;

v communication procedures for exchanging information with internal and external CIS users, management and, where appropriate, the general public, and

(d) management commitment, involvement and follow up.

14. Network defence measures for a CIS will include secure mechanisms for sharing information promptly with future institutional CERTs and as appropriate, with trusted internal and external partners, e.g. Government CERTs. Partners should similarly commit to supply information regarding their own network defence events and countermeasures.

15. Information about CIS-specific measures should be classified at the level RESTREINT UE/EU RESTRICTED but may be raised to the level to which the CIS in question is accredited.