COUNCIL OF THE EUROPEAN UNION

Brussels, 14 September 2012

13737/12

CIS 5
CSC 56

INFORMATION NOTE

From:	The inter-institutional CERT-EU Steering Board
To:	Delegations
Subject:	CERT (Computer Emergency Response Team) for the EU institutions, bodies and agencies

1. Delegations are informed that on 9 August 2012, the Secretaries-General of the EU institutions confirmed that the *Computer Emergency Response Team* for the EU institutions, bodies and agencies (CERT-EU), established in a pre-configuration format in 2011 (cf. doc. 10539/11), will continue as a permanent entity based in Brussels at the service of all EU institutions, bodies and agencies. On 11 September 2012, the Commission adopted the necessary internal administrative measures to ensure the logistic support for CERT-EU.

2. Delegations will find attached an information note from the inter-institutional CERT-EU Steering Board on CERT-EU's next phase of work.

CERT-EU

Steering Board

Information on CERT-EU's next phase of work

12 September 2012

INFORMATION ON CERT-EU'S NEXT PHASE OF WORK

I. INTRODUCTION

1. On 9 August 2012 the Secretaries-General of the EU institutions confirmed that the *Computer Emergency Response Team* for the EU institutions, bodies and agencies (CERT-EU), established in a pre-configuration format in 2011, will continue as a permanent entity based in Brussels at the service of all EU institutions, bodies and agencies.

2. The arrangements set out below for the immediate period ahead leave the way open for any possible future initiative regarding CERT-EU's legal and organisational status, depending on its ability to gradually step up its capabilities in response to demand and on a careful cost-benefit analysis, bearing in mind the impact of forthcoming post reductions for EU institutions.

II. BACKGROUND

3. Cyber security and operational protection against cyber attacks are high on the political agenda. Initiatives taken in recent years at EU level highlight the importance of governmental CERTs for all EU Member States and of cooperation among these CERTs. A major initiative on an EU Cyber Security Strategy is due later this year. EU institutions, bodies and agencies are taking steps to improve the overall level of protection of their systems. The establishment and activities of CERT-EU are a concrete step in this direction.

4. Following an initiative by Commission Vice-Presidents Neelie Kroes and Maroš Šefčovič under the *Digital Agenda for Europe*, the Secretaries-General decided in May 2011 to establish a pre-configuration team for a *Computer Emergency Response Team* for the EU institutions, bodies and agencies (CERT-EU). This initiative aimed at reinforcing the capacity of EU institutions, bodies and agencies (the constituents) to respond to cyber-attacks against their IT infrastructures, improve their cyber-security and enhance their ability to deal with cyber-threats.

5. The pre-configuration team was speedily set up on 1 June 2011 for an initial duration of one year. A total of 11 staff were placed at its disposal by the European Commission, the General Secretariat of the Council, the European Parliament, the Joint Services of the European Economic and Social Committee and the Committee of the Regions and ENISA (the European Network and Information Security Agency). The team operated under the supervision of a Steering Board of senior representatives of the above-mentioned entities.

6. Over the period, the CERT-EU pre-configuration team has established three basic CERT services identified as main tasks for its initial phase (i.e. alerts and warnings, incident response coordination and announcements). Its remit was to advise and liaise with the internal teams responsible for IT security in each entity, react to incidents on their networks, monitor the threat landscape and issue timely alerts and warnings.

7. A detailed evaluation report with recommendations for the next phase was presented by a group of senior IT experts, based on input provided by constituent institutions, bodies and agencies, Member State CERTs which have worked with CERT-EU and by the pre-configuration team itself. On that basis, operational recommendations have been agreed by the Secretaries-General on how CERT-EU's activities should develop, be oriented and rendered more effective in the next phase of work in terms of: (i) *services to be provided to constituents*; (ii) *organisation and governance*; and (iii) *resourcing*.

III. SERVICES TO BE PROVIDED BY CERT-EU TO CONSTITUENTS

8. The assessments by constituents (EU institutions, bodies and agencies) and Member States' CERTs have shown by and large a high level of satisfaction with the initial work of CERT-EU. Constituents expect CERT-EU to continue to consolidate the services provided so far and add further services when requested focused even more on constituents' needs. CERT-EU has established its credibility and shown itself capable of providing useful services. This work should continue.

9. The key focus for the coming period will be on assisting clients' internal teams, in particular in relation to preventing, detecting, mitigating and responding to cyber-attacks. CERT-EU's service catalogue will cover cyber-security related short-term alerts and warnings, announcements, incident handling activities and exchange of artefact information, technology watch and basic education, training and awareness building services, and may be amended as and when appropriate. CERT-EU's service catalogue is set out in annex I.

10. Each constituent will remain solely responsible for operating its communication and information systems, for organising and managing security and for maintaining a high level of information security. Any activities on IT systems such as forensics, artefact analysis, penetration testing, intrusion detection services, tracking or tracing may only be performed by CERT-EU when explicitly invited to do so by the requesting constituent. The Steering Board will continuously supervise CERT-EU's performance, its constituents' needs and guide the scope for increased service offer based on these needs; it may also consider *ad hoc* requests or recommendations for additional services from constituents.

11. CERT-EU will operate taking due account of the following general considerations:

(a) each constituent is solely responsible for operational contacts with law enforcement authorities; CERT-EU will not undertake such contacts in relation to specific incidents. Once an incident has been reported to a law enforcement authority or subject to a mandated security investigation, CERT-EU may only provide specific assistance when requested by the affected constituent;

(b) activities with an intelligence/counter-intelligence dimension are the sole responsibility of each constituent, and will not be undertaken by CERT-EU;

(c) the constituents are responsible for their own security policies and guidelines. CERT-EU may only provide assistance in this respect at the discretion of constituents;

(d) security issues related to deploying or operating systems accredited to handle EU classified information or to cryptographic equipment are the sole responsibility of each constituent; any role for CERT-EU in relation to such systems in the future will be determined by the Steering Board.

12. To facilitate a smooth exchange of technical information between CERT-EU and its constituents:

    (a) the Steering Board has agreed principles governing information exchange; these will be further developed, in particular to include guidance on handling information related to incidents;

    (b) all members of the Steering Board have committed to immediately alerting CERT-EU when a serious cyber-attack or related problem is detected in its systems, unless it is not appropriate to do so.

13. CERT-EU's activities will be driven by service-mindedness and client focus in response to constituents' needs. Priority will be given to consolidating and improving the services already being provided, in particular supporting and coordinating information exchange about and response to cyber incidents. Any constituent may request CERT-EU:

    (a) to dispatch experts on-site to assist local teams with the immediate handling of the incident;

    (b) to provide additional incident handling support to deal with a cyber-attack. CERT-EU may provide its own expertise, or request other institutions which have committed expertise to an incident response pool to provide assistance if able to do so (see point 25 (c));

    (c) to undertake basic artefact analysis. Whenever such analysis is explicitly requested by a constituent, CERT-EU will first seek assistance from existing capacities within the constituency and, should this turn out to be insufficient, from Member States' CERTs or trusted third parties endorsed by the Steering Board (including private companies specialising in this field) with the explicit agreement of the constituent. CERT-EU will maintain a constituent archive of known artefacts and their impact as well as corresponding response strategies.

14. CERT-EU should gradually become acknowledged as the single point of contact for providing CERT-relevant information (e.g. on vulnerabilities, threats and warnings) to and receiving it from Member States' CERTs and third parties. This will not impair the ability of any constituent to cooperate with any entities it deems fit to improve its own security posture or resolve problems.

IV. ORGANISATION AND GOVERNANCE

15. The CERT-EU structure will remain as light as possible and preserve its inter-institutional character. In order to ensure better administrative support CERT-EU is placed under the direct functional authority of the Director-General of DG DIGIT in the European Commission.

16. An inter-institutional Steering Board will be maintained with a strong supervisory function and a streamlined mandate. The Steering Board will have a compact, fixed composition of senior managers from those institutions, bodies and agencies currently providing human resources to CERT-EU. The Steering Board's mandate is set out in Annex II.

17. As the Steering Board's role is to ensure strategic supervision, a technical forum will be established under its responsibility which meets regularly to discuss operational topics relevant for the work of CERT-EU. Its mandate will be decided by the Steering Board. This forum will be open to attendance by all EU institutions, bodies and agencies.

18. The Steering Board, based on input from CERT-EU, will provide an annual report on CERT-EU's activities to the Secretaries-General, starting with 2012. By 31 December 2013 at the latest, the Steering Board will make a recommendation to the Secretaries-General for organising an evaluation of CERT-EU's activities by independent high-level IT security experts with experience in establishing, managing and/or supervising CERTs.

V. RESOURCING

19. CERT-EU has been set up in a budgetary neutral manner, with no additional budget being requested by any institution for its operation to date.

20. To preserve flexibility, CERT-EU will continue to operate in the immediate future with staff placed at its disposal by the European Commission, the General Secretariat of the Council, the European Parliament, the Joint Services of the European Economic and Social Committee and the Committee of the Regions and ENISA (the European Network and Information Security Agency). Other institutions, bodies and agencies may make additional staff available. Staff remain administratively dependent on their institution of origin, but work under the functional authority of the Head of CERT-EU.

21. In addition, a list will be drawn up of specialised technical experts within the constituents who, subject to availability, could be called upon by CERT-EU for a short duration when a serious incident occurs in another constituent. Upon request, CERT-EU and its constituents will endeavour to make expert staff mutually available for a limited period of time (e.g. in the framework of incident handling to support local teams handling incidents and resolving technical problems).

Annex I

CERT-EU SERVICE CATALOGUE

Section I of this catalogue lists services currently offered by CERT-EU. Section II describes services which may be provided at a later date based on demand and subject to decisions by the Steering Board.

Ad hoc requests or recommendations for additional services from the constituents may also be considered by the Steering Board.

I. SERVICES CURRENTLY OFFERED BY CERT-EU

CERT-EU:

(a) disseminates **cyber-security related** short-term **alerts and warnings** (e.g. intrusion alerts, vulnerability warnings and security advisories) using appropriate alert management tools and procedures;

(b) disseminates **announcements** to inform constituents about new developments with medium- to long-term impact, such as new found vulnerabilities or intruder tools. It proactively monitors common threats and planned cyber attacks that could be detected before they are actually executed, and coordinate defensive measures, where appropriate in cooperation with service providers.

(c) supports local teams in **incident handling** (by receiving, triaging, and responding to requests and reports, and analysing incidents and events), in particular by undertaking:

(i) **Incident analysis**. Upon request, CERT-EU will assist EU institutions, bodies and agencies which are targets of an attack in analysing the incident by examining all available information and supporting evidence. The objective is to identify the scope of the incident, the extent of damage caused by the incident, the nature of the incident, and available response strategies or workarounds. CERT-EU will correlate activity across incidents to determine any interrelations, trends, patterns, or intruder signatures.

(ii) **Incident response support (including on-site support)**. Upon request, CERT-EU will assist and guide targets of an attack in recovering from an incident. CERT-EU will provide on-site incident response support upon request by the affected entity.

(iii) **Incident response coordination**. CERT-EU will – upon request from a constituent - coordinate the response efforts among constituents affected by a particular incident. The coordination work may involve collecting contact information, notifying sites of their potential involvement (as target or source of an attack), collecting statistics about the number of sites involved, and facilitating information exchange and analysis.

(d) provides **basic artefact handling services** by sharing technical information within the constituents on artefacts, **appropriate analysis on how to detect and remove them** and sharing of artefacts themselves, according to information exchange principles agreed by the Steering Board.

(e) ensure **technology watch** by monitoring new technical developments on cyber-security products, intrusion techniques and related activities and trends. This may involve presentations, announcements or recommendations focused on more medium- to long-term IT security issues.

(f) provide **basic education, training and awareness building services**.

II. SERVICES TO BE PROVIDED BY CERT-EU SUBJECT TO DEMAND[1]

(a) Support **vulnerability handling** (vulnerability analysis, response and response coordination);

(b) Provide **advanced artefact handling services (artefact analysis, response and response coordination)**;

(c) Provide advanced **education, training and awareness building** – in line with the IT security policies of each constituent - to constituents about cyber security issues through seminars, workshops, courses, tutorials and information campaigns. Topics might include incident prevention methods, incident reporting guidelines, appropriate response methods, incident response tools, and other information to help to prevent, detect, report, and respond to CIS security incidents.

(d) Provide any additional services decided by the Steering Board, taking into account, *inter alia*, the CSIRT services listed by ENISA[2].

---

[1] Any extension of the services set out in section I, must be approved by the Steering Board on the basis of a detailed implementation plan drawn up by CERT-EU. Where CERT-EU responds to an urgent request to perform any service going beyond section I of this service catalogue, it will inform the Steering Board.

[2] http://www.enisa.europa.eu/activities/cert/support/guide/appendix/csirt-services

Annex II

MANDATE OF THE CERT-EU STEERING BOARD

1. CERT-EU will operate under the supervision of an inter-institutional Steering Board reporting to the Secretaries-General[1]. The Steering Board will be composed of senior management representatives designated by their respective institutions, bodies or agencies, as follows:
   - the chair;
   - three members from the European Commission;
   - one member each from the GSC, the European Parliament, the EESC/COR and ENISA.

   Members may be assisted as necessary. The Head of CERT-EU may be invited to its meetings.

2. The Secretaries-General will designate the Chair of the Steering Board *ad personam* for a period of two years.

3. The Steering Board will inform all EU institutions, bodies and agencies of its meetings and decisions. Items discussed by the Steering Board may be classified.

4. The Steering Board will in particular:

   - oversee and set priorities for the work of CERT-EU and provide strategic direction and guidance;

   - adopt an annual work plan on the basis of a proposal by CERT-EU and monitor its implementation and use of resources;

   - take any decisions necessary to facilitate the effective functioning of CERT-EU, including decisions to extend its catalogue of tasks or services;

   - approve the mandate of a technical forum to discuss operational topics relevant for the work of CERT-EU and designate its chair;

   - seek to obtain resource commitments from constituents to enable the gradual development of CERT-EU's activities in line with demand for its services;

   - endorse the Head of CERT-EU on a recommendation from the Steering Board member under whose functional authority CERT-EU is placed;

   - provide an annual report on CERT-EU's activities to the Secretaries-General based on input from CERT-EU.

---

[1] The composition of the Steering Board may be changed with the agreement of the Secretaries-General.