037094/EU XXV. GP
Eingelangt am 09/09/14

Council of the
European Union

Brussels, 9 September 2014

12992/14

CIS 4
CSC 196
CSCI 30
CYBER 43

INFORMATION NOTE

From:	The inter-institutional CERT-EU Steering Board
To	Delegations
Subject:	Recommendations by the inter-institutional Steering Board of the Computer Emergency Response Team for the EU institutions, bodies and agencies (CERT-EU) on the future mandate, governance, organisational setup, staffing and funding of CERT-EU

1. On 18 July 2014, the Secretaries-General of the EU institutions endorsed recommendations by the inter-institutional Steering Board of the Computer Emergency Response Team for the EU institutions, bodies and agencies (CERT-EU) on the future mandate, governance, organisational setup, staffing and funding of CERT-EU.

2. Delegations will find attached for information the endorsed recommendations on the future set up of CERT-EU.

MANDATE, GOVERNANCE, ORGANISATIONAL SETUP, STAFFING AND FUNDING OF CERT-EU

I. INTRODUCTION

1. On 18 July 2014 the Secretaries-General of EU institutions and bodies agreed measures to ensure the long-term effectiveness of the *Computer Emergency Response Team* for the EU institutions, bodies and agencies (CERT-EU). These are aimed at clarifying CERT-EU's mandate, services and operational capacity, and placing its governance, organisational setup, staffing and funding on a more sustainable footing now that the start-up phase has been completed.

II. BACKGROUND

2. Effective protection of IT networks against cyber attacks remains a priority for all EU institutions, bodies and agencies. The establishment of a Computer Emergency Response Team for the EU institutional 'family', initially as a pilot in 2011 then confirmed as a permanent entity in 2012, is a showcase example of inter-institutional cooperation in practice. It has helped improve the overall level of IT security in EU institutions, bodies and agencies. It lends credibility to EU institutions by showing they live up to their own recommendations under the EU's wider cyber security strategy.

3. An evaluation of CERT-EU's activities was commissioned in spring 2014 from four independent high-level IT security experts with experience in establishing, managing and supervising CERTs. Their evaluation report contained recommendations which were examined by the CERT-EU Steering Board in May and June 2014.

4. The Steering Board acknowledges the good work carried out by CERT-EU over the past two years. The evaluation report shows that CERT-EU has been providing value added in reinforcing the security of EU information systems. CERT-EU has grown in maturity and become a useful practical tool in the overall cyber defence management of the EU 'family'. It is a recognised peer by Member State national CERTs and has recently been accepted as a member of the trusted grouping of EU Government CERTs (EGC).

III. CERT-EU's MANDATE, SERVICES AND OPERATIONAL CAPABILITY

5. CERT-EU will continue to serve as the central information exchange and cyber incident coordination hub for all EU institutions, bodies and agencies. It is the forum through which practical assistance may be sought by all EU institutions, bodies and agencies to deal with cyber incidents. All constituents will as a general rule request CERT-EU’s support in the first instance, provided a speedy response in critical situations can be assured and taking account of arrangements in place for initial incident response in each constituent.

6. CERT-EU's mandate will focus on delivering well-defined core services. The Steering Board aims to approve a new mandate by the end of 2014 which will contain a catalogue of services and define their concrete nature and scope (e.g. preventive, reactive, etc.), while balancing the specific interests of larger constituents and the needs of smaller constituents.

7. CERT-EU will regularly provide its constituency with an overall assessment of the threat situation affecting EU institutions, bodies and agencies. The threat analysis should take account of ENISA's work. CERT-EU will enhance cooperation and develop synergies with ENISA when providing technical advice, offering training and conducting exercises.

8. CERT-EU will confine its operational interventions to its constituency. It will not engage proactively in intelligence-related activities, in particular attribution of attacks, nor lead work by the EU Member States' CERT community.

9. CERT-EU's contacts with international partners must be in line with existing EU policies and positions and aimed at facilitating the exchange of technical information and responding effectively to cyber incidents.

10. While information sharing and trust in CERT-EU have improved substantially over the period, there is still room for a more systematic reporting of incidents to CERT-EU and a freer sharing of information in a timely manner between the constituents and CERT-EU, particularly of incident-related technical information. The policy on information sharing between constituents and CERT-EU will be reviewed to encourage this. CERT-EU will also draw up rules on handling information provided to it by constituents. CERT-EU will not share outside of its constituency any sensitive information that might jeopardise the security of EU institutions, bodies and agencies, without the prior agreement of the originator of the information. This applies also to information sharing with private companies.

11. The Steering Board will define in the first half of 2015 a "full operational capability target" for CERT-EU, including key performance indicators and a roadmap for achieving it in the light of its new mandate and available resources.

12. The head of CERT-EU will be designated by the Steering Board every five years (renewable), with the next designation in June 2016.

III. ORGANISATION, GOVERNANCE, STAFFING AND FUNDING

13. CERT-EU will continue to service all EU institutions, bodies and agencies under the supervision and strategic oversight of a high-level inter-institutional Steering Board composed of full members representing senior management from institutions or bodies contributing resources to CERT-EU, and ENISA (representing all agencies). With a view to strengthening strategic supervision of CERT-EU by the Steering Board, including where rapid decisions may be required, the mandate for the Steering Board has been adjusted (see annex).

14. The administrative setup of CERT-EU should be as lean as possible and synergies for administrative support should be sought so as to reduce its administrative overhead. This will focus technical expertise and staff skills on what is needed for providing practical assistance to its constituents for managing IT security incidents. CERT-EU will also continue to be able to draw on such expert skills where available in the EU institutions, as it has done in the recent past for certain incidents.

15. With that objective in mind, CERT-EU will be fully integrated into the administrative structure of DG DIGIT in the Commission in order to benefit from the support of the administrative and financial management structures in that directorate-general. DG DIGIT will provide CERT-EU with day to day operational guidance. This integration is agreed on the understanding, confirmed by the Commission, that: (i) the Steering Board will not be chaired by a member from the Commission; that (ii) CERT-EU's staff and financial resources will be assigned solely to CERT-EU and ringfenced; and that (iii) IT systems used by CERT-EU for analytical activities will be adequately segregated from Commission systems.

16. CERT-EU needs to be able to rely on a sufficiently large permanent staff base in order to develop efficiently and retain knowledge and technical know-how. Consequently, constituent institutions and bodies capable of doing so are looking favourably at the possibility of transfers of permanent posts to CERT-EU from their establishment plans. All have confirmed that they will not reduce the current level of overall support to CERT-EU for the coming period. With regard to the overall staffing level of CERT-EU, a specific target number will be defined once a full operational capability target has been set (see point 11 above).

17. EU institutions, bodies and agencies which have establishment plans outside the EU budget (i.e. the European Central Bank (ECB) and the European Investment Bank (EIB)) or which, because of limited staff resources in this field, are unable to contemplate a transfer to CERT-EU, will provide CERT-EU with annual financial contributions under Service Level Arrangements (SLAs). These service fees are used to finance a limited number of temporary staff (CAs and SNEs) and to procure services and tools for malware prevention, detection and eradication.

18. Later this year, the Steering Board will review the financing arrangements and service provision offered under the current SLAs in order to determine how best to tailor service charges (i.e. whether these should be based on levels of service provision, the size of the entities involved, or some combination of both).

19. The organisational arrangements set out above do not preclude alternative arrangements being agreed in future, in particular in the light of future reviews of CERT-EU's work.

IV. REVIEW

20. A review of the operation of CERT-EU will be conducted at the latest in 2017. The Steering Board will propose terms of reference for such a review in due time. CERT-EU is strongly encouraged to conduct periodic client satisfaction surveys to assess use of the range of services offered and how they can be tailored to constituents' needs.

Annex

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.

2. The Steering Board is composed of one member of senior management designated by each of the EU institutions or bodies. The Commission may designate up to two further members. EU agencies are represented by ENISA. The Chair of the Steering Board will be designated by the Secretaries-General. Members may be assisted as necessary. The Head of CERT-EU may be invited to meetings.

3. The Steering Board will in particular:
   - oversee and set priorities for the work of CERT-EU and provide strategic direction and guidance;
   - approve CERT-EU's mandate;
   - approve CERT-EU's annual financial and staffing plan;
   - approve CERT-EU's annual work plan, on the basis of a proposal by CERT-EU, and monitor its implementation;
   - approve a summary annual report on CERT-EU's activities prepared by CERT-EU;
   - take any decisions necessary to facilitate the effective functioning of CERT-EU; including decisions to extend its catalogue of tasks or services;
   - establish a Technical Advisory Group, approve its mandate and designate its chair;
   - and designate the Head of CERT-EU on a proposal by a Commission member.

   It may issue instructions to the Head of CERT-EU on any matter within CERT-EU's remit.

4. Should urgent decisions by the Steering Board be required for operational reasons, it may exceptionally act with the agreement of the Chair and the members from the European Commission, the GSC, the European Parliament and the affected constituent(s). The Steering Board will be informed.

5. The Steering Board will inform all EU institutions, bodies and agencies of its meetings and decisions.