II

(Information)

INTERINSTITUTIONAL AGREEMENTS

COUNCIL

ARRANGEMENT

between the European Parliament, the European Council, the Council of the European Union, the European Commission, the Court of Justice of the European Union, the European Central Bank, the European Court of Auditors, the European External Action Service, the European Economic and Social Committee, the European Committee of the Regions and the European Investment Bank on the organisation and operation of a computer emergency response team for the Union's institutions, bodies and agencies (CERT-EU)

(2018/C 12/01)

THE EUROPEAN PARLIAMENT,

THE EUROPEAN COUNCIL, THE COUNCIL OF THE EUROPEAN UNION,

THE EUROPEAN COMMISSION,

THE COURT OF JUSTICE OF THE EUROPEAN UNION,

THE EUROPEAN CENTRAL BANK,

THE EUROPEAN COURT OF AUDITORS,

THE EUROPEAN EXTERNAL ACTION SERVICE,

THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE,

THE EUROPEAN COMMITTEE OF THE REGIONS

AND THE EUROPEAN INVESTMENT BANK

Whereas:

(1) Reinforcing the capacity of all European Union institutions, bodies and agencies to deal with cyber-threats and vulnerabilities and to prevent, detect and respond to cyber-attacks against their information and communication technology (ICT) infrastructures remains a high priority as functioning ICT networks and systems are critical to their ability to fulfil their missions.

(2) Following an initiative by Commission Vice-Presidents Neelie Kroes and Maroš Ševčovič, the Secretaries-General of the Union's institutions and bodies decided in May 2011 to establish a pre-configuration team for a computer emergency response team for the Union's institutions, bodies and agencies (CERT-EU) supervised by an inter-institutional Steering Board.

(3) In July 2012, the Secretaries-General confirmed the practical arrangements and agreed to maintain CERT-EU as a permanent entity to continue to help improve the overall level of information technology (IT) security of the Union's institutions, bodies and agencies as an example of visible inter-institutional cooperation in cyber-security.

(4) Reviews undertaken in 2014 and 2016 have shown that CERT-EU has continued to develop in maturity and has now reached the stage where it should be placed on a formal footing with a more sustainable and transparent governance and financial structure.

(5) Directive (EU) 2016/1148 of the European Parliament and of the Council [1] (the 'NIS Directive') establishes a network of Computer Security Incidents Response Teams (CSIRTs), which shall be composed of representatives of the Member States' CSIRTs and CERT-EU, to contribute to the development of confidence and trust between the Member States and to promote swift and effective operational cooperation.

(6) The governance structure for CERT-EU should set out CERT-EU's role and tasks, the responsibilities of its head, the role and tasks of its Steering Board, and the responsibilities of the Union's institutions, bodies and agencies in supporting CERT-EU.

(7) CERT-EU should be provided with sustainable funding and staffing, while ensuring value for money and an adequate core of permanent staff and while keeping the administrative overhead of CERT-EU as low as possible.

(8) This Arrangement is signed by the participant Union institutions and bodies following completion of their respective internal procedures for that purpose; the Union agencies listed in Annex I which are responsible for their own ICT infrastructure have formally confirmed in writing to the chair of the CERT-EU Steering Board that they will apply it,

HAVE CONCLUDED THIS ARRANGEMENT:

Article 1

Purpose and mission

1. The purpose of this arrangement is to establish the rules for the functioning and organisation of the inter-institutional computer emergency response team for the Union's institutions, bodies and agencies ('CERT-EU').

2. CERT-EU's mission shall be to contribute to the security of the ICT infrastructure of all Union institutions, bodies and agencies ('the constituents') by helping to prevent, detect, mitigate and respond to cyber-attacks and by acting as the cyber-security information exchange and incident response coordination hub for the constituents.

Article 2

CERT-EU's tasks

1. CERT-EU shall collect, manage, analyse and share information with the constituents on threats, vulnerabilities and incidents on unclassified ICT infrastructure. It shall coordinate responses to incidents at inter-institutional and constituent level, including by providing or coordinating the provision of specialised operational assistance.

2. CERT-EU shall offer standard CERT services for all constituents. The catalogue setting out CERT-EU's detailed service offering, and any updates, shall be approved by the Steering Board. When revising the list of services, the Head of CERT-EU shall take into account the resources allocated to him or her.

3. CERT-EU may monitor constituents' network traffic with the consent of the relevant constituent.

4. CERT-EU may provide assistance to constituents regarding incidents on classified IT networks and systems if explicitly requested to do so by the constituent concerned.

5. CERT-EU shall not initiate activities or knowingly intervene in any matters that fall within the competence of national security and intelligence services or of specialised departments within the constituents. Any contacts with CERT-EU initiated or sought by national security and intelligence services shall be communicated to the Commission's Security Directorate and the chair of the CERT-EU Steering Board without delay.

[1] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p. 1).

6. CERT-EU shall inform constituents about its incident handling procedures and processes.

7. CERT-EU may, if expressly requested by constituents' policy departments, contribute its technical advice or input on relevant policy matters.

Article 3

Cooperation between constituents and CERT-EU

1. CERT-EU and the constituents shall work in accordance with the 'need-to-share' principle, subject to paragraph 3. CERT-EU shall ensure that efficient means of communication are available for the purpose of facilitating information sharing with constituents.

2. Constituents shall provide to CERT-EU information on cyber-security threats and vulnerabilities affecting them. When CERT-EU is aware of a threat or a vulnerability affecting or potentially affecting a constituent, it shall alert the constituent concerned by providing all relevant information, including the level of criticality, as soon as practicable so that protective or remedial measures can be implemented. CERT-EU may assist in providing such protective or remedial measures. Other constituents shall be informed where the threat or vulnerability potentially affects them.

3. Constituents shall inform CERT-EU without undue delay if they experience a significant cyber incident and provide all relevant technical details unless doing so could jeopardise the security interests of a constituent or a third party. Any incident shall be deemed to be significant unless it is repetitive or basic and likely to be already well-understood in terms of method and technologies. Non-technical information may be shared with CERT-EU at the discretion of the affected constituent. Incident information communicated to CERT-EU shall not be shared outside CERT-EU, even in anonymised form, unless the affected constituent has given consent. To prepare for situations in which information needs to be shared rapidly in order to protect constituents' networks and systems, CERT-EU shall work with its constituents in advance on how to do this.

4. CERT-EU, acting in dialogue with constituents, shall maintain a catalogue of available expertise among them which could potentially be drawn on, within means and capabilities, in the event of a major cyber incident affecting one or more of them. Where appropriate, CERT-EU may organise and coordinate information sharing and technical support directly between constituents to address a cyber-security incident.

5. Within the scope of its remit, CERT-EU shall cooperate closely with the European Union Agency for Network and Information Security (ENISA) and the European Cybercrime Centre at Europol.

6. CERT-EU shall share information on specific incidents with law enforcement authorities only with the prior consent of the competent services of the relevant constituent or constituents.

7. CERT-EU shall keep a record of all information shared with constituents and exchanged with other parties. Constituents may request CERT-EU to provide details of their information shared with other parties.

8. Should the need arise, CERT-EU may enter into service level or cooperation arrangements with any constituent for the provision of CERT services. CERT-EU may also enter into service level or cooperation arrangements regarding the provision of CERT services against payment for EU civilian crisis management operations under Title V, Chapter 2 of the Treaty on European Union. In each case, such service level or cooperation arrangements shall be subject to approval of the Steering Board.

Article 4

Cooperation of CERT-EU with Member State CERTs

1. CERT-EU shall cooperate and exchange information with Member States' national or government CERTs or CSIRTs on cyber-security threats, vulnerabilities and incidents, on possible counter-measures and on all matters relevant for improving the protection of constituents' ICT infrastructure, including through the CSIRT network referred to in Article 12 of the NIS Directive.

2. CERT-EU shall cooperate with Member State CERTs in order to gather information on general and specific threats to constituents and on tools or methods, including techniques, tactics and procedures, best practices and general vulnerabilities for dissemination to its constituents. CERT-EU may exchange information on tools or methods, including techniques, tactics and procedures, best practices and general threats and vulnerabilities with such CERTs.

3. CERT-EU may exchange incident-specific information with such CERTs with the consent of the affected constituent.

Article 5

Cooperation with third party CERTs and other partners

1. CERT-EU may cooperate with industry sector-specific CERTs and non-EU CERTs on tools and methods, such as techniques, tactics and procedures, best practices and on general threats and vulnerabilities. For all cooperation with such CERTs, including in frameworks where non-EU CERTs cooperate with Member State CERTs, CERT-EU shall seek prior approval from the Steering Board.

2. CERT-EU may cooperate with other partners, such as commercial entities or individual experts, to gather information on general and specific threats, vulnerabilities and possible counter-measures. For wider cooperation with such partners, CERT-EU shall seek prior approval from the Steering Board.

3. Provided a non-disclosure arrangement or contract is in place with the relevant partner, CERT-EU may, with the consent of the affected constituent, provide information relating to a specific incident in a constituent to such partners where they can contribute to its analysis. Such non-disclosure agreements or contracts shall be legally verified in accordance with the relevant internal Commission procedures. Non-disclosure agreements or contracts shall not require prior approval by the Steering Board but its chair shall be informed.

4. CERT-EU may exceptionally enter into service level arrangements with entities other than the constituents with the prior approval of the Steering Board.

Article 6

Tasks of the Head of CERT-EU

1. The Head of CERT-EU shall be responsible for the smooth running of CERT-EU, acting within its remit under the direction of the Steering Board. He or she shall be responsible for implementing the strategic direction, guidance, objectives and priorities set by the Steering Board, and for the sound management of CERT-EU, including of its financial and human resources. He or she shall report regularly to the Steering Board Chair.

2. The Head of CERT-EU shall be bound by the rules applicable to the Commission and shall act as authorising officer by sub-delegation when implementing the general budget of the European Union, in accordance with the relevant internal rules of the Commission on delegation of powers and limits in such cases. He shall act under the Commission's authority solely for the application of administrative and financial rules and procedures.

3. The Head of CERT-EU shall submit quarterly reports to the Steering Board on the performance of CERT-EU, implementation of the budget, contracts or other arrangements entered into and missions undertaken by staff. He or she shall also submit an annual report to the Steering Board pursuant to Article 8(1)(e).

4. The Head of CERT-EU shall assist the responsible authorising officer by delegation in drafting the annual activity report containing financial and management information, including the results of controls, drawn up in accordance with Article 66(9) of the Financial Regulation, and shall report regularly to him or her on the implementation of measures in respect of which powers have been sub-delegated to him.

5. The Head of CERT-EU shall draw up annually a financial planning of administrative revenue and expenditure for its activities to be approved by the Steering Board in accordance with Article 8(1)(c).

Article 7

The Steering Board

1. A Steering Board shall provide strategic direction and guidance to CERT-EU and monitor implementation of its general priorities and objectives. Its members shall be senior management representatives designated by each of the signatories to this Arrangement, and by ENISA which shall represent the interests of the agencies listed in Annex I that run their own ICT infrastructure. Members may be assisted by an alternate. Other representatives of constituents may be invited by the chair to attend Steering Board meetings.

2. The Steering Board shall designate a chair from among its members for a period of two years. His or her alternate shall become a full member of the Board for the same duration.

3. The Steering Board shall meet at the initiative of its chair or at the request of any of its members. It shall adopt internal rules of procedure.

4. Each signatory to this Arrangement and ENISA shall have one vote, exercised by the corresponding member or members. Steering Board decisions shall be taken by simple majority except where otherwise provided. The chair shall not vote except in the event of a tied vote where he or she may exercise a casting vote.

5. Should urgent decisions be required for operational reasons, the Steering Board may exceptionally act with the agreement of the chair and the members representing the European Commission, the Council, the European Parliament and the affected constituent or constituents.

6. The Steering Board may act by a simplified written procedure initiated by the chair under which the relevant decision shall be deemed approved within the timeframe set by the chair, except where a member objects.

7. The Head of CERT-EU shall participate in Steering Board meetings except where otherwise decided by the Board.

8. The secretariat of the Steering Board shall be provided by the institution whose senior management representative is the chair.

9. The secretariat shall inform the EU agencies listed in Annex I about the Steering Board's decisions. Any EU agency shall be entitled to raise with the chair of the Steering Board any matter which it considers should be brought to the Steering Board's attention.

Article 8

Tasks of the Steering Board

1. In providing strategic direction and guidance to CERT-EU, the Steering Board shall in particular:

(a) approve, on the basis of a proposal from the Head of CERT-EU, the annual work programme for CERT-EU and monitor its implementation;

(b) approve, on the basis of a proposal from the Head of CERT-EU, CERT-EU's service catalogue;

(c) approve, on the basis of a proposal submitted by the Head of CERT-EU, the financial planning of revenue and expenditure, including staffing, for CERT-EU activities;

(d) approve each year, on the basis of a proposal from the Head of CERT-EU, the amount of annual financial appropriations to be provided for services to be rendered to constituents and third parties with service level arrangements with CERT-EU;

(e) examine and approve the annual report drawn up by the Head of CERT-EU covering the activities of, and management of funds by, CERT-EU;

(f) approve and monitor key performance indicators for CERT-EU defined on a proposal by the Head of CERT-EU;

(g) approve CERT-EU papers setting out general policies and guidelines recommending good ICT security practice to be followed by the constituents;

(h) approve cooperation arrangements, service level arrangements or contracts between CERT-EU and other entities pursuant to Articles 3(8) and 5(4);

(i) establish as necessary technical advisory groups to assist the Steering Board's work, approve their terms of reference and designate their chair; and

(j) amend the list of Union agencies applying this Arrangement set out in Annex I.

2. The chair may represent or act on behalf of the Steering Board in accordance with arrangements agreed by the Board.

Article 9

Staffing and financial matters

1. While established as an autonomous interinstitutional service provider for all Union institutions, bodies and agencies, CERT-EU shall be integrated into the administrative structure of a Commission directorate-general in order to benefit from the Commission's administrative, financial management and accounting support structures. The Commission shall inform the Steering Board about the administrative location of CERT-EU and any changes thereto.

2. The Commission, after having obtained the unanimous approval of the Steering Board, shall appoint the Head of CERT-EU. The Steering Board shall be consulted at all stages of the procedure prior to the appointment of the Head of CERT-EU, in particular in drafting vacancy notices, examining applications and appointing selection boards in relation to this post.

3. The officials of all Union institutions and bodies shall be informed about any vacancy notice for posts in CERT-EU.

4. Subject to the prerogatives of the Union's budgetary authority, the Union institutions and bodies participating in this Arrangement, with the exception of the European Court of Auditors, the European Central Bank and the European Investment Bank, undertake to transfer or assign to CERT-EU the number of posts set out in Annex II by the 2019 budget year or as otherwise provided for in Annex II. Union institutions and bodies assigning or transferring the defined numbers of posts shall receive full services from CERT-EU. The number of posts set out in Annex II shall be reviewed at least every five years.

5. CERT-EU may agree with the participant Union institutions and bodies on the temporary allocation of additional personnel to CERT-EU.

6. The European Court of Auditors, the European Central Bank and the European Investment Bank shall enter into service level arrangements regarding services offered by CERT-EU in accordance with its service catalogue and their annual financial compensation to be made by each in accordance with Annex II at the beginning of each financial year in return for services provided by CERT-EU during the previous financial year.

7. The financial compensation to be provided by each Union agency to cover the costs of CERT-EU's service offering shall be agreed with the respective Union agencies and included in the general administrative framework governing the provision of Commission services to Union agencies.

8. The Head of CERT-EU shall each year report on the amount of annual financial compensation to be provided by those constituents with service level arrangements with CERT-EU pursuant to paragraph 6 and Union agencies pursuant to paragraph 7. The Steering Board shall each year review that amount of annual financial compensation.

9. The budgetary and financial management of CERT-EU activities, including assigned revenues from other Union institutions or bodies, shall be performed by the Commission in accordance with Regulation (EU, Euratom) No 966/2012 of the European Parliament and of the Council [1] on the financial rules applicable to the general budget of the Union and relevant rules and regulations. Any budget appropriations or revenues provided to CERT-EU through service level arrangements will be specifically identified within its financial planning.

Article 10

Professional confidentiality

CERT-EU and constituents shall treat any information received from another constituent or a third party as subject to the obligation of professional secrecy in accordance with Article 339 of the Treaty on the Functioning of the European Union or equivalent applicable frameworks. They shall not divulge any such information to third parties unless specifically authorised to do so by the constituent or party concerned.

Article 11

Protection of personal data

The processing of personal data carried out under this Arrangement shall be subject to Regulation (EC) No 45/2001 of the European Parliament and of the Council [2].

Article 12

Audit, questions and public access to documents

1. The function of internal auditor shall be performed by the Internal Audit Service of the Commission while respecting the provisions of Article 10. The Steering Board may suggest audits to be undertaken to the Internal Audit Service of the Commission.

2. The Head of CERT-EU shall be responsible for answering questions from the European Ombudsman and the European Data Protection Supervisor in accordance with the Commission's internal procedures.

3. The Commission's procedures under Regulation (EC) No 1049/2001 of the European Parliament and the Council [3] shall apply with regard to requests for public access to documents held by CERT-EU taking account of the obligation under that Regulation to consult other constituents whenever a request concerns their documents.

Article 13

Review

In view of the evolving cyber threat landscape and the Union's response to it, including the policy priorities set out in the EU cybersecurity strategy, the Steering Board shall regularly review the organisation and operation of CERT-EU. It may make recommendations to review or amend this Arrangement, or any other recommendations for the effective operation of CERT-EU, to the participating institutions and bodies.

Article 14

Scope and date of application

1. This Arrangement shall apply to Union institutions and bodies which are signatories to this Arrangement, and to the Union agencies which run their own ICT infrastructure which are listed in Annex I.

2. This Arrangement shall apply from the date of its signature. It shall be published in the *Official Journal of the European Union*.

---

[1] Regulation (EU, Euratom) No 966/2012 of the European Parliament and of the Council of 25 October 2012 on the financial rules applicable to the general budget of the Union and repealing Council Regulation (EC, Euratom) No 1605/2002 (OJ L 298, 26.10.2012, p. 1).

[2] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1).

[3] Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (OJ L 145, 31.5.2001, p. 43).

This Arrangement is drawn up in the Bulgarian, Croatian, Czech, Danish, Dutch, English, Estonian, Finnish, French, German, Greek, Hungarian, Italian, Latvian, Lithuanian, Maltese, Polish, Portuguese, Romanian, Slovak, Slovenian, Spanish and Swedish languages, in a single original which shall be deposited with the General Secretariat of the Council of the European Union who shall transmit a certified true copy to all signatories.

Done at Frankfurt, Luxembourg and Brussels, 20 December 2017.

For the European Parliament
The Secretary-General
K. WELLE

For the European Council and the Council
The Secretary-General
J. TRANHOLM-MIKKELSEN

For the European Commission
Secretary-General
A. ITALIANER

For the Court of Justice of the European Union
Director-General DG Infrastructure
F. SCHAFF

For the European Central Bank
Director General Information Systems
K. DE GEEST

Chief Services Officer
M. DIEMER

For the European Court of Auditors
The Secretary-General
E. RUIZ GARCÍA

For the European External Action Service
General Director for Budget and Administration
G. DI VITA

For the European Economic and Social Committee
The Secretary-General
L. PLANAS PUCHADES

For the European Committee of the Regions
The Secretary-General
J. BURIÁNEK

For the European Investment Bank
Director General and Financial Controller
P. KLAEDTKE

ANNEX I

List of Union Agencies referred to in Article 14(1)

ACER	Agency for the Cooperation of Energy Regulators
BEREC Office	Body of European Regulators for Electronic Communications
CPVO	Community Plant Variety Office
EU-OSHA	European Agency for Safety and Health at Work
FRONTEX	European Border and Coast Guard Agency
eu-LISA	European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice
EASO	European Asylum Support Office
EASA	European Aviation Safety Agency
EBA	European Banking Authority
ECDC	European Centre for Disease Prevention and Control
Cedefop	European Centre for the Development of Vocational Training
ECHA	European Chemicals Agency
EEA	European Environment Agency
EFCA	European Fisheries Control Agency
EFSA	European Food Safety Authority
Eurofound	European Foundation for the Improvement of Living and Working Conditions
GSA	European GNSS Agency
EIGE	European Institute for Gender Equality
EIOPA	European Insurance and Occupational Pensions Authority
EMSA	European Maritime Safety Agency
EMA	European Medicines Agency
EMCDDA	European Monitoring Centre for Drugs and Drug Addiction
ENISA	European Union Agency for Network and Information Security
CEPOL	European Union Agency for Law Enforcement Training
Europol	European Union Agency for Law Enforcement Cooperation
ERA	European Union Agency for Railways
ESMA	European Securities and Markets Authority
ETF	European Training Foundation
FRA	European Union Agency for Fundamental Rights
EUIPO	European Union Intellectual Property Office

Eurojust	European Union Agency for Criminal Justice Cooperation
CdT	Translation Centre for the Bodies of the European Union
EDA	European Defence Agency
EIT	European Institute of Innovation and Technology
EUISS	European Union Institute for Security Studies
SATCEN	European Union Satellite Centre
SRB	Single Resolution Board

ANNEX II

Full time equivalent posts or budget contributions committed to CERT-EU by the participants

ESTABLISHMENT PLAN POSTS

Institution/Body	Relative share of EU staff	Corresponding full time equivalent posts to be transferred/assigned to CERT-EU
European Parliament	19,5 %	3 ([1])
European Council/Council	9 %	2
Commission ([2])	55 %	8
Court of Justice	6 %	1 ([3])
European External Action Service	4,5 %	1 ([4])
European Economic and Social Committee/European Committee of the Regions	3,5 %	1 ([5])
European Court of Auditors	2,5 %	0 ([6])
	TOTAL:	16

Annual financial commitments to CERT-EU	
European Central Bank ([7])	EUR 120 000 ([8])
European Investment Bank ([7])	EUR 120 000 ([8])

([1]) The European Parliament will complete the transfer of the two outstanding posts at the latest as part of the 2021 budget. In the intervening period it undertakes to maintain its current commitment: one half FTE placed at the disposal of CERT-EU and an annual financial contribution (EUR 120 000 ([8])) laid down in a service level arrangement.

([2]) In the case of the Commission, posts will internally be placed at the disposal of CERT-EU. The Commission also provides a contribution in kind to CERT-EU in the form of offices, logistics and IT infrastructure. The relative share of establishment plan staff assigned from the Commission does not take account of posts in Union offices or in various Union executive agencies for which the Commission provides IT infrastructure.

([3]) The Court of Justice of the European Union is unable to commit to transferring a post within the period provided for in Article 9(4). Until it is in a position to do so, it undertakes to maintain its current commitment of an annual financial contribution laid down in a service level arrangement.

([4]) The European External Action Service is unable to commit to transferring a post within the period provided for in Article 9(4). Until it is in a position to do so, it undertakes to maintain its current commitment of an annual financial contribution laid down in a service level arrangement.

([5]) The European Economic and Social Committee and the European Committee of the Regions are unable to commit to transferring a post within the period provided for in Article 9(4). Until they are in a position to do so, they undertake to maintain their current commitment of making available two half-time experts.

([6]) Given the relative size of the European Court of Auditors, rather than transferring a post, it will make a financial commitment to CERT-EU in accordance with Article 9(6).

([7]) As the European Central Bank and the European Investment Bank do not operate under the EU staff regulations and therefore cannot make post transfers, both entities will continue to make an annual financial contribution to CERT-EU under a service level arrangement in accordance with Article 9(6).

([8]) These amounts may be adjusted as foreseen in Article 9(8).