Council of the European Union
General Secretariat

Interinstitutional files:
2023/0109 (COD)

Brussels, 08 December 2023

WK 16614/2023 INIT

REDACTED DOCUMENT ACCESSIBLE TO THE PUBLIC (11.06.2025). ONLY MARGINAL PERSONAL DATA HAVE BEEN REDACTED.

LIMITE

CYBER

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

WORKING DOCUMENT

From:	General Secretariat of the Council
To:	Horizontal Working Party on cyber issues (attachés)
Subject:	Proposal for a Regulation of the European Parliament and of the Council laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents - Presentation

Delegations will find in the Annex the presentation given by the Presidency at the Horizontal Working Party for cyber issues on 7 December 2023. Please, note that the content is provisional and subject to modifications.

PRESIDENCIA ESPAÑOLA
CONSEJO DE LA UNIÓN EUROPEA

Cyber Solidarity Act

Third Presidency Compromise Proposal

HWPCIs - 07.12.2023

[redacted] – Cyber Team

Chapter II – The European Cyber Security Alert System

What is it? What for? – Article 3

What it is

A pan-European infrastructure consisting of :

- **ENTITIES with the FUNCTIONALITIES defined in Article 2 of the Regulation, and**
- **The CROSS BORDER PLATFORMS composed by at least three of those entities**

Purpose

- **BETTER PROTECTION and REPONSE to cyber threats**
- **Through SUPPORTING THE DEVELOPMENT OF ADVANCED CAPABILITIES FOR detection, analysis and data processing on cyber threats and incidents.**

- ✓ **Based on VOLUNTARY Cooperation**
- ✓ **Cooperate and SUPPORT EXISTING entities, CSIRTs in particular**
- ✓ **Financed through the DEP Program In particular Objective 3 (Article 3)**

Chapter II – The European Cyber Security Alert System

Which entities? What do they do?

[NATIONAL COOPERATION ENTITY]

Article 2

- Functions defined in Article 2
- To be decided **voluntarily** by each Member State if CSIRT or another entity **(Article 4)**

[CROSS - BORDER COOPERATION PLATFORM]

Articles 6, 7, 8

- Entities from at least three Member States create **voluntarily** a cross- border platform

They **create voluntarily**, a **hosting consortia :**

- ✓ To apply for funding (ECCC joint procurement and grants) **(Article 8a)**
- ✓ To participate in actions **(Article 5)**

They **sign a consortium agreement, deciding voluntarily on its terms**:

- ✓ Conditions for exchange of information within the consortium **(Article 6)**
- ✓ Conditions for exchange of information with Union level entities and networks **(Article 7)**
- ✓ Security measures **(Article 8)**

They **decide voluntarily among themselves on their conditions for interoperability (Article 6 (3))**

- ✓ On the basis of the guidance from ENISA
- ✓ They inform the Commission

Chapter III – The Cyber Emergency Mechanism

What is it? What for? – Articles 9, 10 and 11

Purpose

- Support EU resilience to threats, and prepare and mitigate the short term impact of significant and large-scale cyber security incidents

Types of actions

- Preparedness actions
- Actions supporting response
- Mutual assistance actions

- ✓ <u>Upon request</u> and complimentary to the Member States efforts
- ✓ Cybersecurity emergency reserve implemented by COM and ENISA - Rest of the Emergency Mechanism primarily via ECCC and NNCC
- ✓ Involvement of the NIS Cooperation Group, ENISA, HR and EU-CyCLONe (when relevant) in risk scenarios
- ✓ When services pre-committed for response are not used, they can be used for preparedness
- ✓ Financed through the DEP Program, In particular Objective 3

EU Cyber Security Reserve

Establishment – Article 12

[Art. 12(5)]

- ✓ Sets priorities (reviewed every 2 years) in cooperation with :
  - EU-CyCLONe
  - ENISA
  - NIS Cooperation Group
- ✓ Supervises implementation ensuring complementarity, consistency and synergies
- ✓ Defines types and number of response services via Implementing Acts seeking advice of the NIS Cooperation Group [Art. 12(8)]

Entrusts

enisa

[Art. 12(6)]

Via cooperation agreements:

- ✓ Operation and administration
- ✓ Contracting authority

Prepares mapping of needs [Art. 12(7)]

Internal deployment

Consulting:
- NIS Cooperation Group
- EU-CyCLONe
- IICB (when relevant)

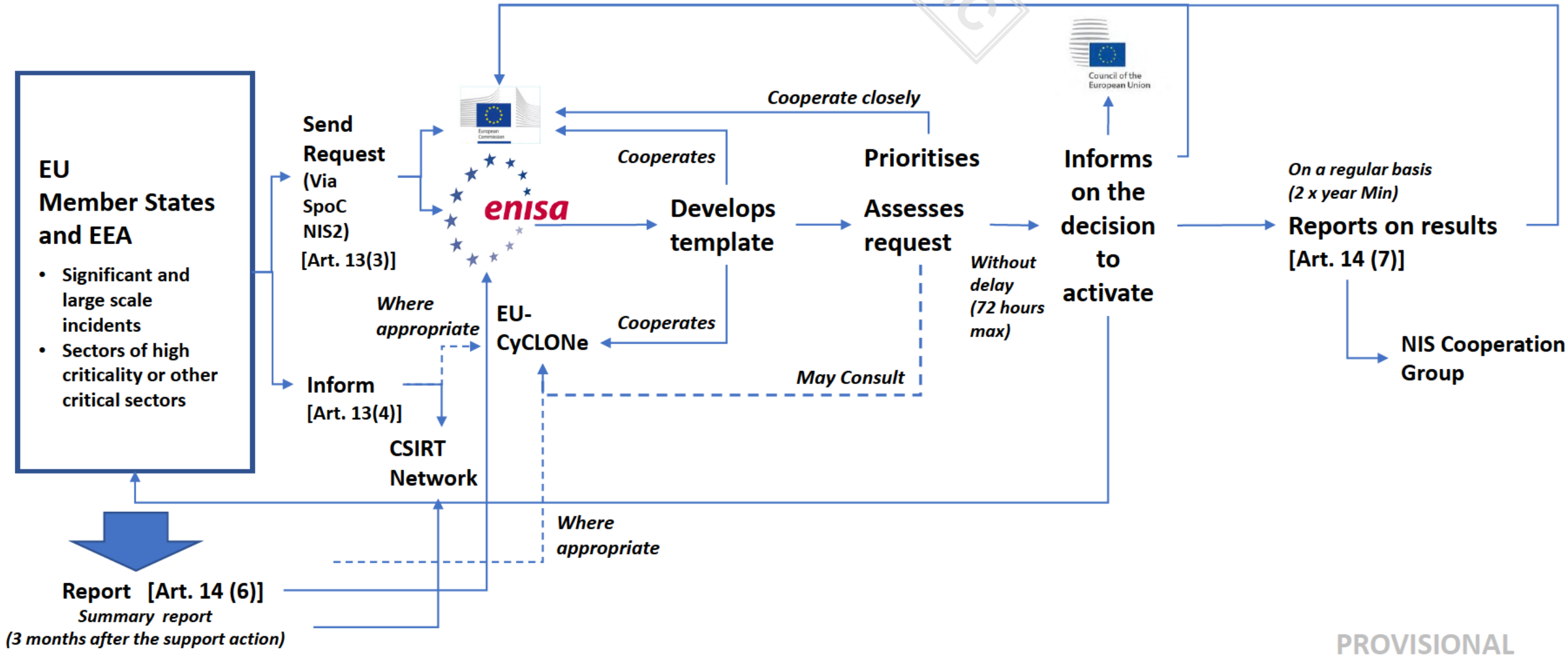
External deployment

Consulting:
- EU-CyCLONe
- Commission
- The High Representative

Informing:
- NIS cooperation group

Implementation phase

Internal deployment



Implementation phase

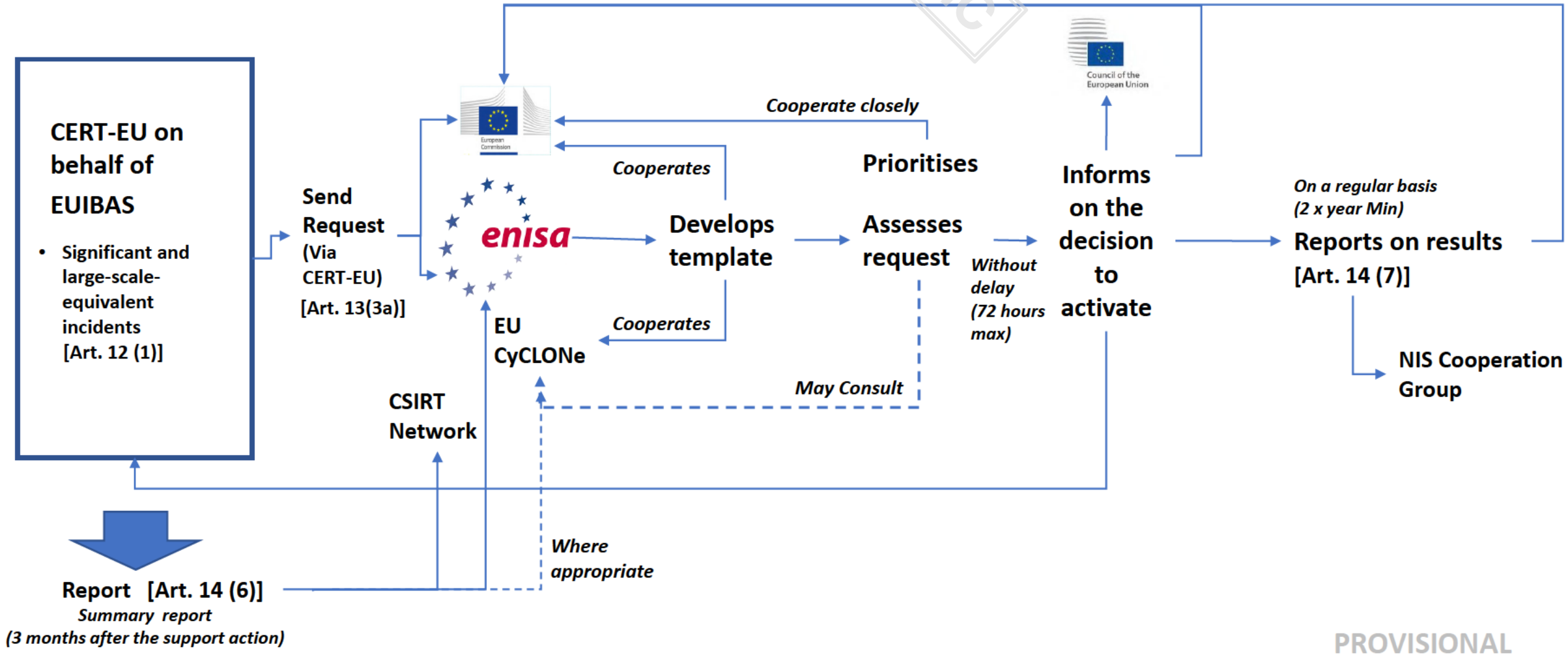
Internal deployment

Users
[Art. 12 (3) (b) (1)]

Filing of requests
[Art. 13]

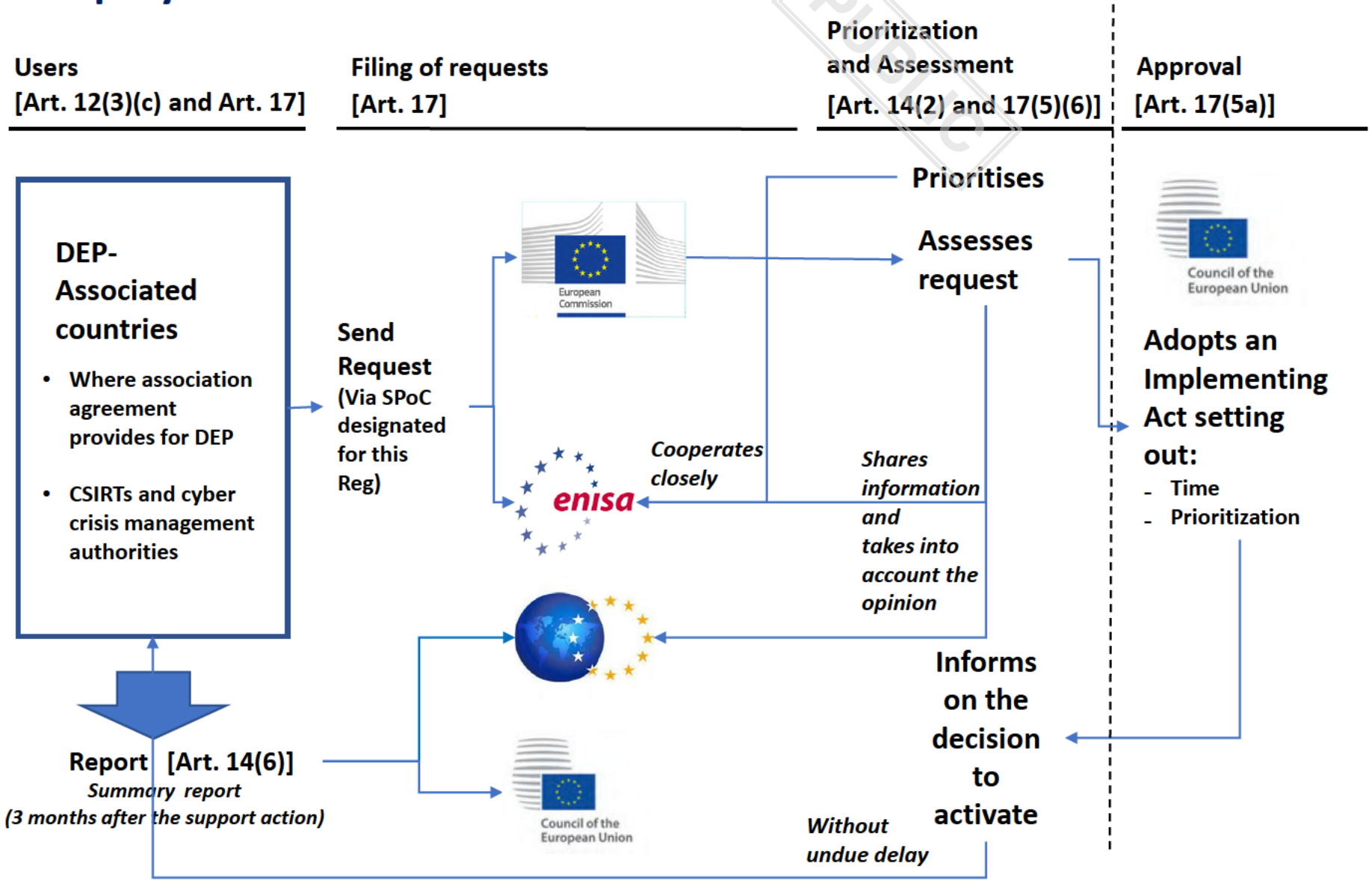
Prioritization and Assessment
[Art. 14 (1) (2)]

Reporting
[Art. 14 (7)]



Implementation phase

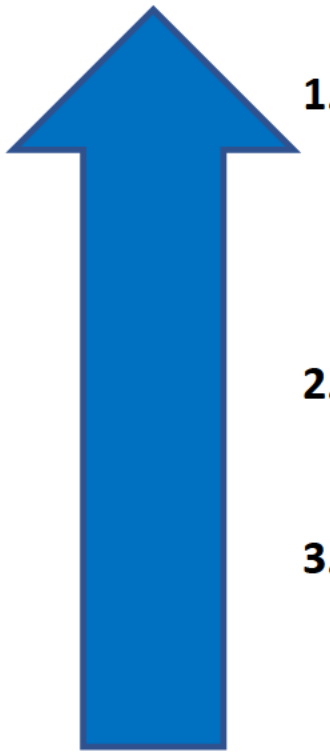
External deployment



EU Cyber Security Reserve

Alternatives for the Council involvement in the external deployment (DEP - Associated countries only)

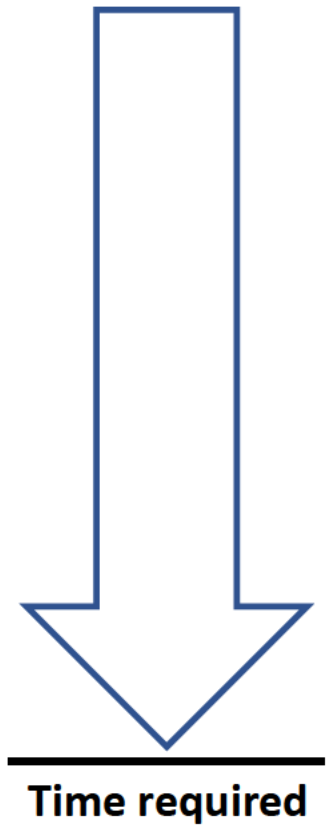
Level of control



1. **Commission prepares the text of the decision and sends it to the Council, which adopts the implementing act by qualified majority. If there is no meeting of the Council and the urgency justifies it: Written procedure by unanimity.**

2. **Obligation to the Commission to consult before taking the final decision**

3. **Council not to be involved in the individual deployment decisions themselves, but the entities where Member States are involved (e.g: EU-CyCLONe) are consulted.**



Time required

See also: CLS Opinion 11943/22, paras 56-61

PUBLIC

¡Gracias!

PRESIDENCIA ESPAÑOLA CONSEJO DE LA UNIÓN EUROPEA