

A European Programme for Critical Infrastructure Protection

EPCIP


The Communication from the Commission on
a European Programme for Critical
Infrastructure Protection

The EPCIP Framework

The European Programme for Critical Infrastructure Protection
EPCIP Communication

Measures designed to facilitate the implementation of EPCIP

- EPCIP Action Plan
- CIWIN
- CIP expert groups
- CIP information sharing
- identification and analysis of interdependencies

Support for Member States concerning National Critical Infrastructures

Contingency planning

External dimension

Accompanying financial measures

In particular the proposed EU programme on "Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks" for the period 2007-2013,

Proposal for a Directive concerning ECI

A procedure for the identification and designation of European Critical Infrastructures (ECI).

A common approach to the assessment of the needs to improve the protection of such infrastructures. This will be implemented by way of a Directive .

Key principles will guide the implementation of EPCIP:

Subsidiarity – The Commission's efforts in the CIP field will focus on infrastructure that is critical from a European, rather than a national or regional perspective. Although focusing on European Critical Infrastructures, the Commission may where requested and taking due account of existing Community competences and available resources provide support to Member States concerning National Critical Infrastructures.

Complementarity - the Commission will avoid duplicating existing efforts, whether at EU, national or regional level, where these have proven to be effective in protecting critical infrastructure. EPCIP will therefore complement and build on existing sectoral measures.

Confidentiality - Both at EU level and MS level, Critical Infrastructure Protection Information (CIPI) will be classified appropriately and access granted only on a need-to-know basis. Information sharing regarding CI will take place in an environment of trust and security.

Stakeholder Cooperation – All relevant stakeholders will, as far as possible, be involved in the development and implementation of EPCIP. This will include the owners/operators of critical infrastructures designated as ECI as well as public authorities and other relevant bodies.

Proportionality – measures will only be proposed where a need has been identified following an analysis of existing security gaps and will be proportionate to the level of risk and type of threat involved.

Sector-by-sector approach – Since various sectors possess particular experience, expertise and requirements with CIP, EPCIP will be developed on a sector-by-sector basis and implemented following an agreed list of CIP sectors .

EPCIP Communication

Workstream 1 – consecutive EPCIP strategies

Workstream 2 -

ECI Directive

Comitology decisions on criteria

Designation of ECI

Comitology decisions on OSPs

Workstream 3 -

Support for MS concerning NCI

National CIP Programmes

The EPCIP Action Plan

The EPCIP Action Plan will be implemented taking into account sector specificities and involving, as appropriate, other stakeholders. The EPCIP Action Plan organizes CIP related activities around three work streams:

Work Stream 1

Will deal with the strategic aspects of EPCIP and the development of measures horizontally applicable to all CIP work.

Work Stream 2

Will deal with European Critical Infrastructures and implemented at a sectoral level.

Work Stream 3

Will support the Member States in their activities concerning National Critical Infrastructures

The EPCIP Action Plan will be implemented taking into account sector specificities and involving, as appropriate, other stakeholders.

The CIP stakeholder dialogue

Expert groups will support EPCIP by facilitating exchanges of views on related CIP issues on an advisory basis.

CIP expert groups will not replace other existing groups already established or which could be adapted to fulfil the needs of EPCIP, nor will they interfere with direct information exchanges between industry, the MS authorities and the Commission.

An EU level CIP expert group will have a clearly stated objective, a timeframe for the objective to be achieved and a clearly identified membership. CIP Expert Groups will be dissolved following the achievement of their objectives.

Specific functions of CIP expert groups may vary across CI sectors depending on the unique characteristics of each sector. These functions may include the following tasks:

- Assist in identifying vulnerabilities, interdependencies and sectoral best practices;
- Assist in the development of measures to reduce and/or eliminate significant vulnerabilities and the development of performance metrics;
- Facilitating CIP information-sharing, training and building trust;
- Develop and promote "business cases" to demonstrate to sector peers the value of participation in infrastructure protection plans and initiatives;
- Provide sector-specific expertise and advice on subjects such as research and development.

The CIP information sharing process

Stakeholders will take appropriate measures to protect information concerning such issues as the security of critical infrastructures and protected systems, interdependency studies and CIP related vulnerability, threat and risks assessments.

Any personnel handling classified information will have an appropriate level of security vetting by the Member State of which the person concerned is a national.

The Commission shall take appropriate measures, in accordance with Decision 2001/844/EC, ECSC, Euratom, to protect information subject to the requirement of confidentiality to which it has access or which is communicated to it by Member States.

Member States shall ensure that Critical Infrastructure Protection Information submitted to the Member States or to the Commission, is not used for any purpose other than the protection of critical infrastructures.

CIP information exchange will facilitate the following:

- Improved and accurate information and understanding about interdependencies, threats, vulnerabilities, security incidents, countermeasures and best practices for the protection of CI;
- Increased awareness of CI issues;
- Stakeholder dialogue;
- Better-focused training, research and development;

The CIP coordination

An EU level mechanism is required in order to serve as the strategic coordination and cooperation platform capable of taking forward work on the general aspects of EPCIP and sector specific actions.

Consequently, a CIP Contact Group will be created.

The CIP Contact Group will bring together the CIP Contact Points from each Member State and will be chaired by the Commission.

Each Member State should appoint a CIP Contact Point who would coordinate CIP issues within the Member State and with other Member States, the Council and the Commission.

The appointment of the CIP Contact Point would not preclude other authorities in the Member State from being involved in CIP issues.


The proposal for a Directive
on the identification and designation of
European Critical Infrastructure and the
assessment of the need to improve their
protection

Scope of the Directive

Establishes a common procedure concerning:

- the identification of European Critical Infrastructure
- the designation of European Critical Infrastructure
- the assessment of the need to improve the protection of European Critical Infrastructure

What is ECI?

- European Critical Infrastructure – critical infrastructures the disruption or destruction of which would significantly affect:
  - two or more Member States, or
  - a single Member State if the critical infrastructure is located in another Member State.
- This includes effects resulting from cross-sector dependencies on other types of infrastructure.

Key components

Three main components:

- Procedure on the identification of European Critical Infrastructure – Article 3
- Procedure on the designation of European Critical Infrastructure – Article 4
- Procedure on the assessment of the need to improve the protection of European Critical Infrastructure – Articles 5-7

Identification of ECI

- Based on a three step process:
  - The development and adoption of cross-cutting and sectoral criteria to identify ECI
  - The identification by each Member State of those infrastructures which satisfy the criteria
  - The notification to the Commission of the critical infrastructures which satisfy the established criteria

Identification of ECI
Step 1 – Criteria development

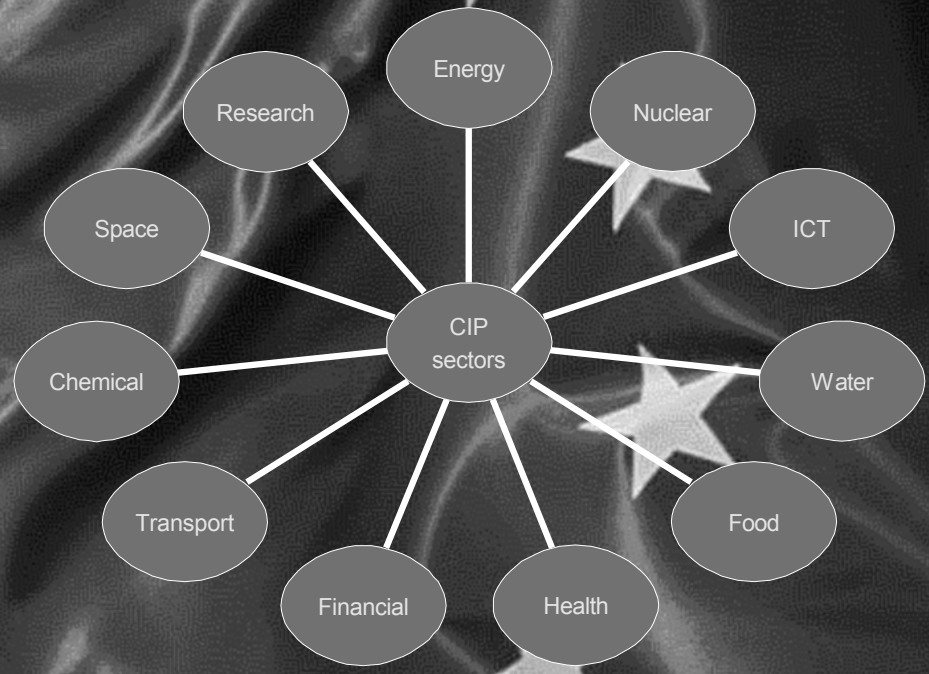
Step 1: the adoption of cross-cutting and sectoral criteria – Article 3(1)

- cross-cutting criteria:
  - are characterized by their horizontal application to all critical infrastructure sectors
  - developed based on the severity of the following effects:
    - public (number of members of the population affected);
    - economic (significance of economic loss and/or degradation of products or services);
    - environmental;
    - political;
    - psychological;
    - public health
  - to be adopted through the comitology regulatory procedure one year after the entry into force of the Directive

Identification of ECI

Step 1 – Criteria development

- sectoral criteria:
  - to be adopted for priority sectors
  - should take into account the characteristics of individual critical infrastructure sectors
  - their development should involve relevant stakeholders
  - To be adopted through the comitology regulatory procedure for each priority sector at the latest one year following the designation as a priority sector



The priority sectors to be used for the purposes of developing the sectoral criteria shall be identified by the Commission on an annual basis

Identification of ECI

Step 2 – application of the criteria

Step 2: the identification by each Member State of those infrastructures which satisfy the criteria - Article 3(3)

Each Member State to identify the critical infrastructures which satisfy the cross-cutting and sectoral criteria

Identification of ECI

Step 3 – notification

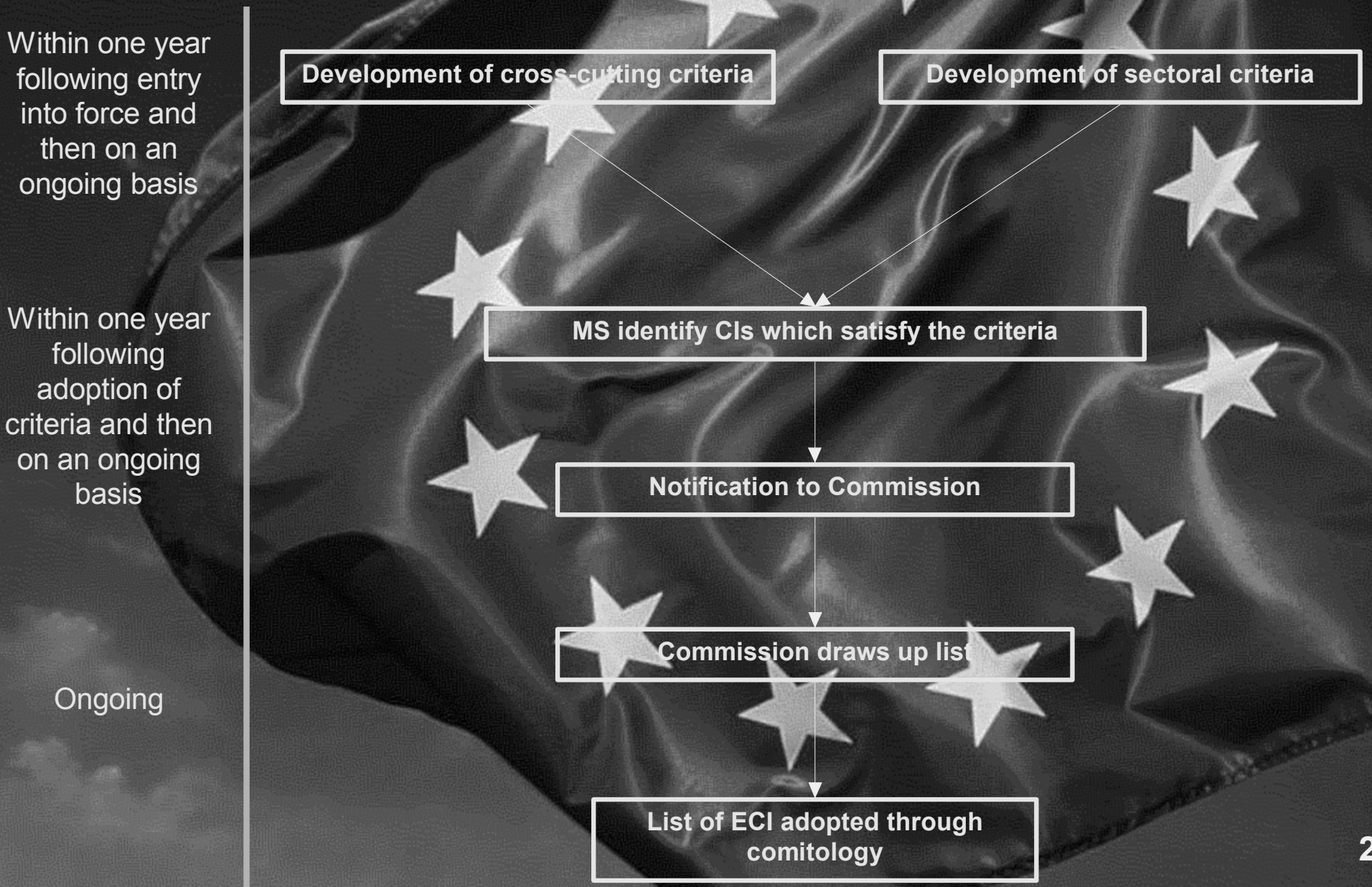
Step 3: each Member State should notify the Commission of the critical infrastructures which satisfy the established cross-cutting and sectoral criteria

This should be done at the latest one year after the adoption of the relevant criteria and thereafter on an ongoing basis

Designation of ECI

- Article 4(1)
  - Commission draws up a list of critical infrastructures to be designated as ECI based on:
    - Notifications received from the Member States
    - Any other information at its disposal
  - The list of critical infrastructures designated as European Critical Infrastructure is adopted under the comitology regulatory procedure
  - The list may be amended

Identification and designation of ECI



Improving protection
Obligations on ECI

- Articles 5 and 6 introduce two basic obligations for CI owners/operators designated as ECI:
  - To establish and update an Operator Security Plan (OSP)
  - To designate a Security Liaison Officer (LSO)
- These obligations are meant to:
  - Directly improve CIP
  - Contribute to the assessment of the need to improve the protection of European Critical Infrastructure

Improving protection

Operator Security Plan

Contents

- The OSP should identify the assets of the European Critical Infrastructure and establish relevant security solutions for their protection
- The basic contents should include:
  - identification of important assets;
  - a risk analysis based on major threat scenarios, vulnerability of each asset, and potential impact;
  - identification, selection and prioritisation of counter-measures and procedures with a distinction between:
    - Permanent security measures
    - Graduated security measures

However, sector specific requirements for OSPs can be adopted through the Comitology regulatory procedure

Timeframe

- The OSP should be submitted to the relevant Member State authority within one year following designation as an ECI
- If sector specific requirements concerning the OSPs are developed, the OSPs should be submitted within one year following the adoption of the sector specific requirements.

Supervision

- Each Member State should set up a system ensuring adequate and regular supervision of the OSPs and their implementation

Improving protection

Security Liaison Officer

Role

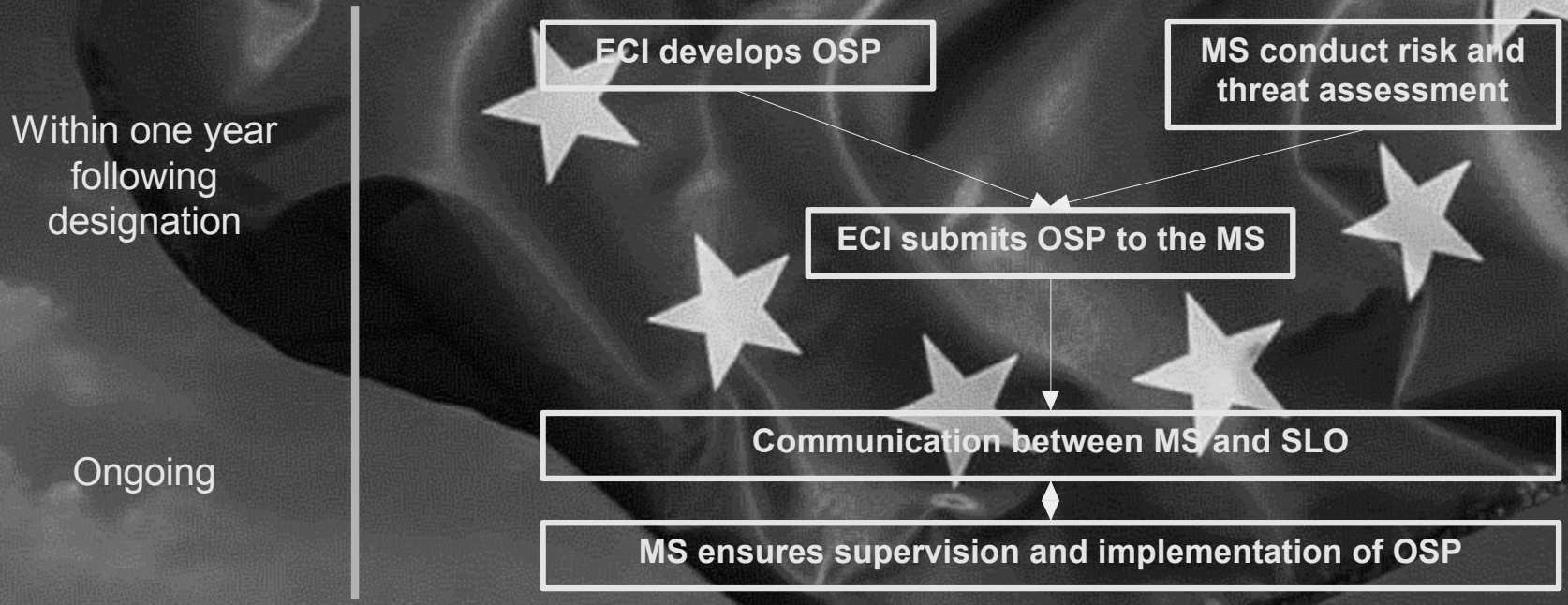
- To be the point of contact for security related issues between the owner/operator of the ECI and the relevant critical infrastructure protection authorities in the Member State
- To receive information from the Member States concerning identified risks and threats

Timeframe

To be designated within one year following the designation of the critical infrastructure as a European Critical Infrastructure

Improving protection
Risk and threat assessments

- Each Member State should conduct a risk and threat assessment in relation to ECI situated on their territory within one year following the designation of the critical infrastructure as an ECI
- This information will be the basis for the Member State's supervision of the OSPs
- Common methodologies for carrying out vulnerability, threat and risk assessments in respect of European Critical Infrastructures may be developed on a sectoral basis in accordance with the comitology regulatory procedure

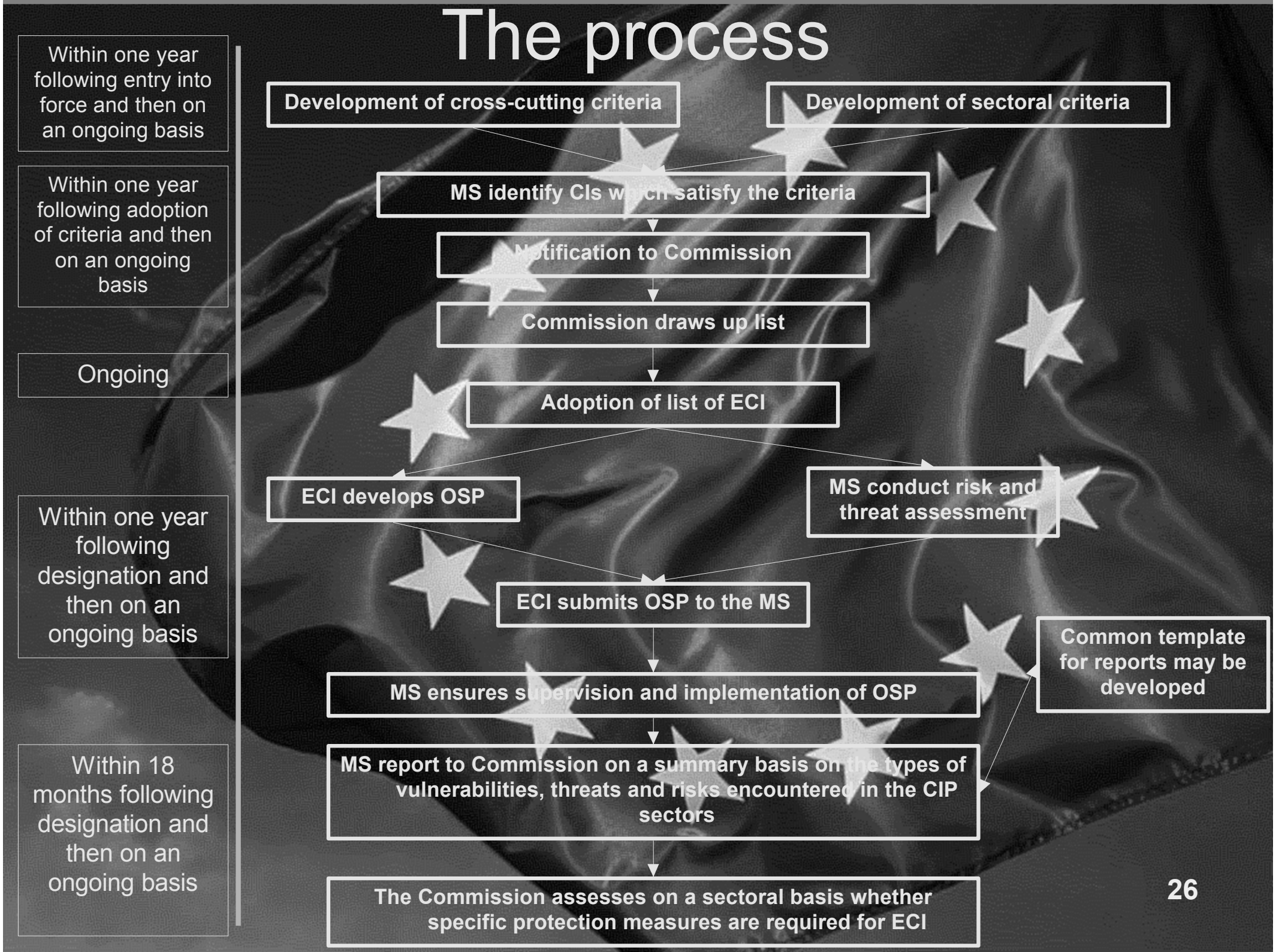


Improving protection
Reporting – Articles 7

- The Member States should report to the Commission on a summary basis on the types of vulnerabilities, threats and risks encountered in the CIP sectors
- This should be done within 18 months following the designation of ECI in a particular sector and thereafter on an ongoing basis every two years
- A common template for these reports should be developed

- The Commission will assess on a sectoral basis whether specific protection measures are required for ECI.

The process


Within one year following entry into force and then on an ongoing basis
Within one year following adoption of criteria and then on an ongoing basis
Ongoing
Within one year following designation and then on an ongoing basis
Within 18 months following designation and then on an ongoing basis
Development of cross-cutting criteria
Development of sectoral criteria
MS identify CIs which satisfy the criteria
Notification to Commission
Commission draws up list
Adoption of list of ECI
ECI develops OSP
MS conduct risk and threat assessment
ECI submits OSP to the MS
MS ensures supervision and implementation of OSP
Common template for reports may be developed
MS report to Commission on a summary basis on the types of vulnerabilities, threats and risks encountered in the CIP sectors
The Commission assesses on a sectoral basis whether specific protection measures are required for ECI

Support to ECI – Article 8

- The owners/operators of designated European Critical Infrastructures will have access to available best practices and methodologies related to critical infrastructure protection
- Funding under the preparedness programme

Confidentiality and CIP information exchange – Article 10

- On the Commission side:
  - appropriate measures will be taken in accordance with Decision 2001/844/EC to protect classified information
    - Any individual who is responsible for compromising EU classified information shall be liable to:
      - disciplinary action according to the relevant rules and regulations;
      - further legal action including the launching of criminal law procedures.
- On the Member State side:
  - Any person handling classified information pursuant to the ECI Directive shall have an appropriate level of security vetting by the Member State concerned
  - Member States shall ensure that Critical Infrastructure Protection Information submitted to the Member States or to the Commission, is not used for any purpose other than the protection of critical infrastructures

Organisation

- CIP Contact Points – Article 9:
  - Each Member State should nominate a CIP Contact Point
  - The Contact Point should coordinate critical infrastructure protection issues within the Member State, with other Member States and with the Commission
- The Committee procedure – Article 11:
  - the implementation of the ECI Directive will be done through a Committee:
    - composed of the CIP Contact Points
    - chaired by the Commission
- The Directive foresees the use of the comitology regulatory procedure
- Legal basis:
  - References to comitology procedure in ECI Directive (Article 11)
  - Council Decision 1999/468/EC laying down the procedures for the exercise of implementing powers conferred on the Commission


Thank you

Committee procedure (comitology)

Regulatory procedure

- Commission submits to the committee a draft of the measures to be taken.
- The committee delivers its opinion on the draft within a specified time-limit. The opinion is delivered by QMV (Article 205(2) of the Treaty)
- If the committee gives a positive opinion the Commission adopts the measures envisaged.
- If the committee gives a negative opinion or if no opinion is delivered, the Commission submits the proposal to the Council.
- If the Council indicates by qualified majority that it opposes the proposal, the Commission shall re-examine it. It may submit an amended proposal to the Council, re-submit its proposal or present a legislative proposal on the basis of the Treaty.
- If the Council has neither adopted the proposed implementing act nor indicated its opposition to the proposal for implementing measures, the proposed implementing act shall be adopted by the Commission.