Cyber Resilience Act proposal

European Commission, DG CONNECT

Main elements of the proposal

- **Cybersecurity rules** for the placing on the market of hardware and software
- Based on **New Legislative Framework** (well-established EU product-related legislative setting)
- **Obligations** for manufacturers, distributors and importers
- Cybersecurity **essential requirements** across the life cycle (5 years)
- **Conformity assessment** – differentiated by level of risk
- **Market surveillance and enforcement**
- **Full harmonisation** for the placement of the market

Interplay with other legislation

Repeal/amend
(Radio Equipment Delegated Regulation)

Complementarity
(e.g. Measurement Instrument Directive, Machinery Regulation)

Exclusion
(motor vehicles, (*in vitro*) medical devices, certified aeronautical equipment)

Only one conformity assessment and MSA
(AI Act)

Presumption of conformity
(Cybersecurity Act)

Conformity assessment (Article 6, 24 and Annex III)

- **Default category (vast majority):** self-assessment
- **Critical products**
  - **Class I** : Harmonised standard or third-party assessment
  - **Class II** : mandatory third-party assessment (e.g. smart meters)
- **Highly critical products:**
  - mandatory certification based on EU cybersecurity certification schemes (Cybersecurity Act)

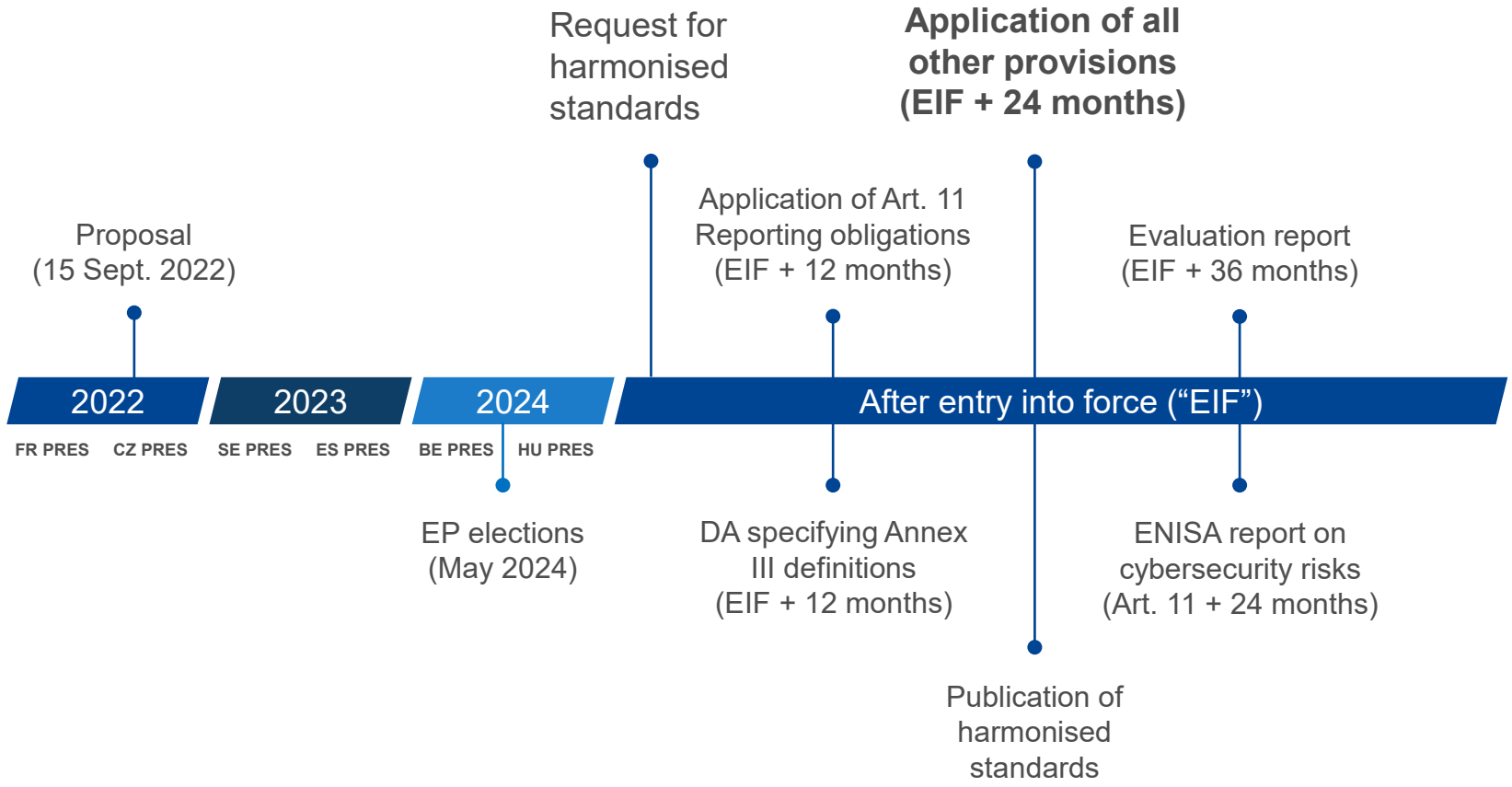
How to do third party assessment ?

New Legislative Framework		EU Cybersecurity Act
EU-Type examination and internal production control (B+C)	**Full quality assurance (H)**	**European cybersecurity certification schemes (article 18 of CRA)**
Notified body… To examine technical design and development + vulnerability handling processes, and ensures surveillance **Manufacturer…** To ensure that production process is in line with approved type	**Manufacturer…** To operate an approved quality system for design, development, production + vulnerability handling processes **Notified body…** To carry out the assessment and the surveillance of the QS	• Where presumption of conformity exist • Upcoming scheme: **European cybersecurity scheme based on Common Criteria** (EUCC) • Any future scheme to take into account CRA requirements

CSA – CRA interplay

- EU cybersecurity certfication schemes might provide presumption of conformity with essential requirements (Article 18 para. 3) and possible exemption from conformity assessment under CRA (Article 18 para. 4)
- Possibility to make EU cybersecurity certification mandatory for « highly critical products » (Article 6)
- Common Criteria-based European cybersecurity certification scheme (**EUCC**) (Rec. 40 of the CRA) : EC to specify presumption of conformity
  - Hardware security modules, smart cards, smart cards, etc
- Any future scheme to take into account the requirements of the CRA

Tentative implementation timeline



European Commission

Standardisation work

- **Harmonised standards** to be developed by ESOs – CEN / CENELEC / ETSI.
- Presumption of conformity for harmonised standards facilitates compliance
- Building on **existing European, national, international standards**
- Preparatory work has started : mapping, gap analysis …

- **How to get involved ?** Contact CEN-CENELEC (JTC13) and ETSI (TC Cyber)

Thank you

maika.fohrenbach@ec.europa.eu

European Commission