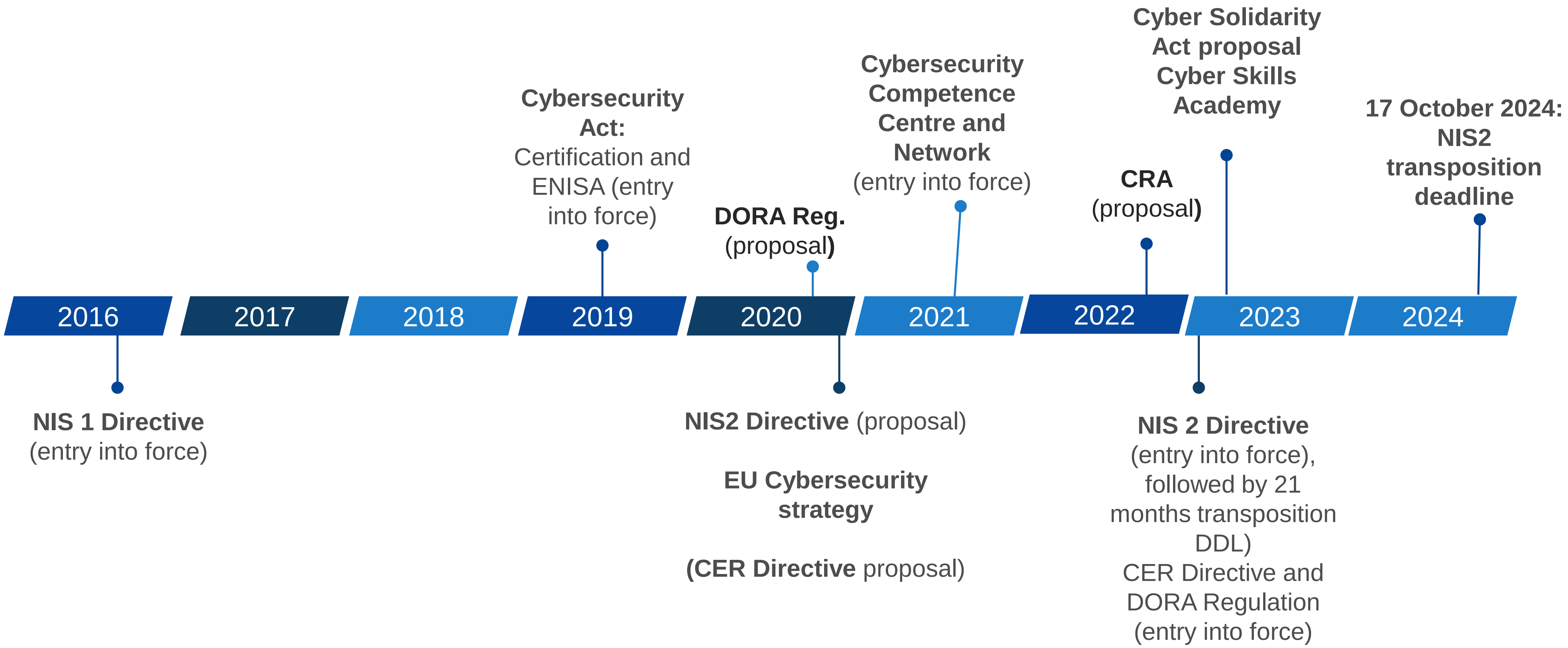
EU cybersecurity policy framework & health

ENISA eHealth Security Conference, 20 September 2023

Juuso Järviniemi, Policy Officer
Unit H2 – Cybersecurity and Digital Privacy Policy
DG CONNECT, European Commission

Existing legislative framework



NIS 1 Directive
(entry into force)

Cybersecurity Act:
Certification and ENISA (entry into force)

DORA Reg.
(proposal)

NIS2 Directive (proposal)

EU Cybersecurity strategy

(CER Directive proposal)

Cybersecurity Competence Centre and Network
(entry into force)

CRA
(proposal)

Cyber Solidarity Act proposal
Cyber Skills Academy

NIS 2 Directive
(entry into force), followed by 21 months transposition DDL)
CER Directive and DORA Regulation (entry into force)

17 October 2024: NIS2 transposition deadline

NIS2: More harmonised security requirements & incident reporting

- Accountability for top management for non-compliance with cybersecurity risk management measures
- Risk-based approach: appropriate and proportionate cybersecurity measures
- Defining a minimum set of measures

(such as risk analysis and information security policy, incident handling, business continuity, supply chain security)

- Reporting of significant incidents
- MS to inform each other and ENISA of incidents with cross-border nature

European Commission

NIS2: Health entities in scope

- **Sectors of high criticality:**
  - Healthcare providers
  - EU reference laboratories
  - Research & development of medicinal products
  - Manufacture of basic pharmaceutical products
  - Manufacture of medical devices critical during public health emergency

- **Other critical sectors:**
  - Manufacture of medical devices & in vitro diagnostic medical devices

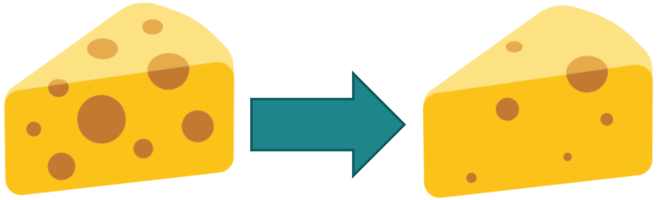
NIS2: Next steps

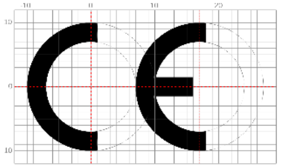
- Transposition deadline: 17 October 2024

- Deadline for implementing acts: 17 October 2024

Cyber Resilience Act: Main elements

- **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)
- Harmonised **standards** to follow
- **Conformity assessment** – differentiated by level of risk
- **Market surveillance and enforcement**





Cyber Resilience Act & Health

- **Medical devices:**
  - CRA not applicable to medical devices (Reg. 2017/745) or in-vitro diagnostic medical devices for human use & accessories (Reg. 2017/746)
  - Acknowledgement of existing guidance on cybersecurity for medical devices
- **Electronic health records:**
  - Connection with NIS2 implementing acts
  - EHDS proposal complements the essential requirements set by CRA
  - EHR systems which are not ”placed on the market” → NIS2

Cyber Solidarity Act: Improved preparedness, detection & response to incidents

To address:

- growing cybersecurity risks and an overall complex threat landscape, with a clear risk of rapid spill-over of cyber incidents from one Member State to others;
- need for strengthening of common EU detection and situational awareness;
- need to support Member States preparedness and response capabilities to major cybersecurity incidents.

We propose:

- to strengthen common EU detection, situational awareness and response capabilities;
- to gradually support building an EU-level cyber reserve with services from trusted private providers;
- to support testing of critical entities for potential vulnerabilities based on EU risk assessments.

Cyber threat intelligence & Health

- Cross-border SOCs as a place for pooling data and cyber threat intelligence -> spread of threat information among actors including CERTs, CSIRTs, ISACs, critical infrastructures

- EU Health ISAC: First physical meeting in May 2023 -> information sharing to strengthen health sector resilience

Conclusion

- NIS2 covers the health sector more widely than NIS1 -> contributes to stronger resilience
- Cyber Resilience Act connects with sectoral health legislation: EHDS, medical devices
- Cyber Solidarity Act strengthens common detection, situational awareness and response capabilities

European Commission

Thank you

European Commission