Overview of cybersecurity policies in the EU

Domenico Ferrara, Policy Officer
European Commission, DG CNECT.H.1
Cybersecurity Technology and Capacity Building

1 June 2021

Continuous policy response to the evolving threat landscape:

- ☐ **2013** EU Cybersecurity Strategy: 'An Open, Safe and Secure Cyberspace'
- ☐ **2016** Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry; NIS Directive
- ☐ **2017** Cybersecurity package, proposal for a Cybersecurity Act (CSA)
- ☐ **2018** Proposal for the European competence centre and network
- ☐ **2019** Entry into force of CSA
- ☐ **2020** Cybersecurity Strategy, Review of NIS Directive

Building EU Resilience to cyber attacks

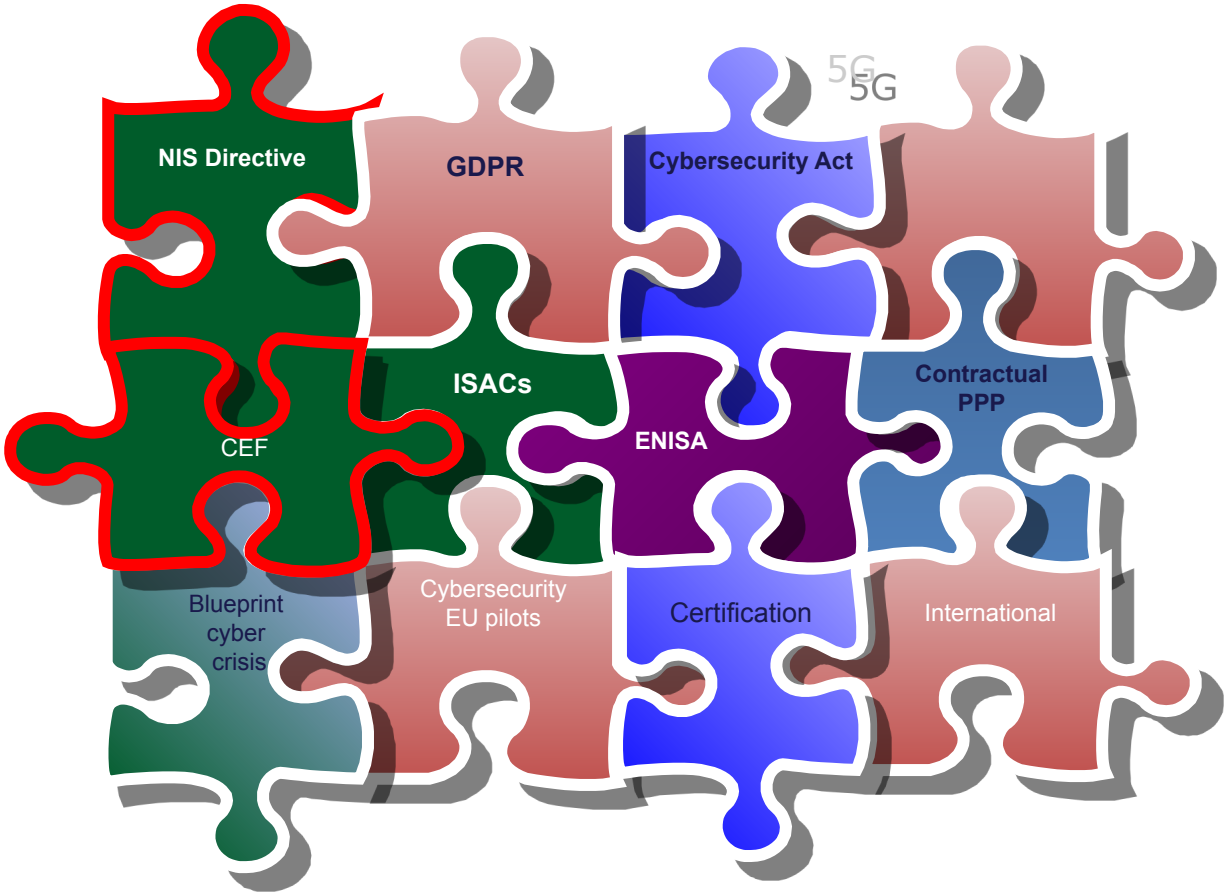
Capacity Building

- Enhanced national capabilities & Risk management requirements (NIS)
- Financial Support from the EU
- Industrial capabilities

Prevention & Response Coordination

- ENISA operational support & Cooperation between national CSIRTs
- Coordinated response to large-scale cybersecurity incidents and crises & exercises
- Single Market for certified ICT products and services (CSA)

EU in action about cybersecurity



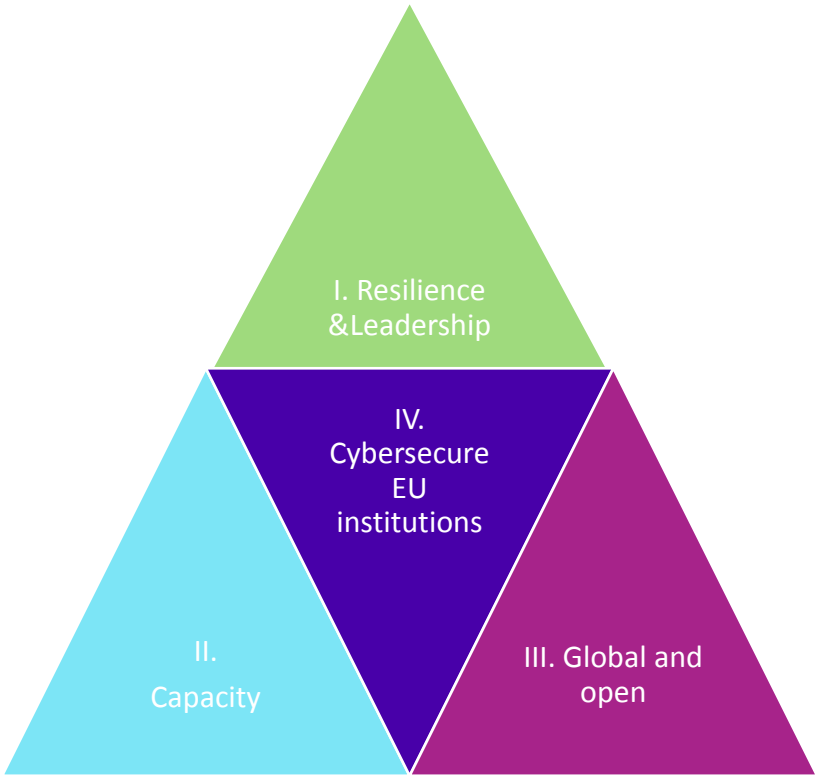
The Cybersecurity Strategy

Why a new Strategy ?

- **Critical services** have gone digital
- **IoT** proliferating: 25 bn connected objects
- **Cyberattacks** increasing 241% (DDoS)
- **Dependency** accelerated by pandemic - also expanding **attack surface** (hospitals, vaccine distribution)
- **Geopolitical** contest over cyberspace; authoritarian regimes damage open global Internet & try dominate international bodies/ norm setting
- **Digital transformation can only succeed with cybersecurity**

Overview of tools and actions

- Smart digital investment: up to €4.5bn for cybersecurity 2021-27 (MFF+RRF+MS+Industry)
- New regulatory tools
- New policy instruments
- Comprehensive
  - *internal market*
  - *law enforcement*
  - *diplomacy*
  - *defence*



Resilience and leadership

Infrastructure

- Adopt NIS 2.0 [CID]

Cyber Shield

- Develop Network of Security Operations Centres

Ultra secure connectivity

- Quantum enabled encryption

5G networks

- Complete implementation of Toolbox

Internet security

- Develop DNS4EU

Supply chain autonomy

- Encourage EUR 4.5 bn investment across digital supply chain through Competence Centre and Network

Skills

- Eg investment in business resilience against cyber-enabled IP theft

Operational capacity: prevent deter, respond

Joint Cyber Unit

- Milestones and process to be set out in 2021

Cybercrime

- Complete Security Union agenda

Cyberdiplomacy toolbox

- Embed Member State cyber intel in INTCEN
- Deterrence posture

Cyber Defence

- Vision and strategy for CSDP military missions

Global and open cyberspace

- EU leadership on international norms and standards
- Cooperation with partners
- Global resilience and capacity

The NIS Directive

NIS Directive: Main Features

GREATER CAPABILITIES

Member States have to improve their cybersecurity capabilities.

- NATIONAL COMPUTER SECURITY INCIDENT RESPONSE TEAM (CSIS-RT)
- NATIONAL NIS STRATEGY
- NATIONAL NIS AUTHORITY

COOPERATION

Increased EU-level cooperation

- EU MEMBER STATES COOPERATION GROUP (STRATEGIC)
  - EU MEMBER STATES; EUROPEAN COMMISSION; EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY
- EMERGENCY TEAMS (CSIRTS) NETWORK (OPERATIONAL)
  - EU MEMBER STATES; CERT-EU; EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY

RISK MANAGEMENT

Operators of essential services and Digital Service Providers have to adopt risk management practices and notify significant incidents to their national authorities.

- SECURITY MEASURES
- NOTIFICATION OF MAJOR INCIDENTS

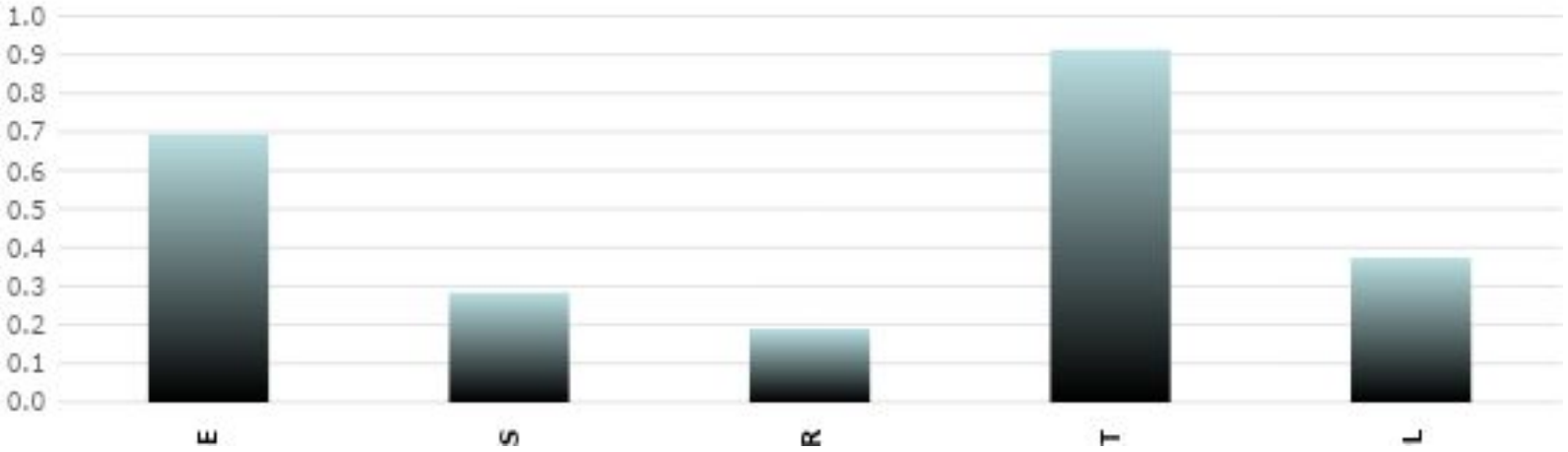
Main challenges of existing NIS 1

Not all sectors that may be considered critical are in scope	Great inconsistencies and gaps due to the NIS scope being *de facto* defined by MS (case by case OES identification)	Diverging security requirements across MS
Diverging incident notification requirements	Ineffective supervision and limited enforcement	Voluntary and ad-hoc cooperation and info sharing between MS and between operators

European Commission

Main challenges of existing NIS 1

Example: Discrepancies in the identification of operators of essential services (OES)



Identified OES in the five biggest Member States (per 100 000 inhabitants)

European Commission

The NIS 2 vision - main objectives

1

Cover a larger portion of economy and society (**more sectors**)

2

Within sectors: systematically focus on bigger and critical players (**replace current identification process**)

3

Align security requirements (incentivize investments and awareness including by mandating board-level accountability), expand **supply chain** and supplier relationships risk management

4

Streamline **incident reporting** obligations

5

Align provisions on national supervision and enforcement

6

More operational cooperation approach including on crisis management

7

Align with proposed Resilience of Critical Entities Directive

European Commission

Two regulatory regimes

	Essential entities	Important entities
Scope	Scope of NIS1 + certain new sectors	Most new sectors + certain entities from NIS1 scope
Security requirements	Risk-based security obligations, including accountability of top management	
Reporting obligations	Significant incidents and significant cyber-threats	
Supervision	Ex-ante + ex post	Ex-post
Sanctions	Minimum list of administrative sanctions, including fines. Only for essential entities*: ultima ratio* possibility to suspend authorisation or impose temporary ban on managerial duties	
Jurisdiction	General rule: MS where the service is provided Exception: Main establishment + ENISA registry for certain digital infrastructures and digital providers	

European Commission

Scope: size threshold

- **Identification** has proven **inefficient** → difficulty in identifying consistent thresholds
- **Size** as a clear-cut benchmark (all companies, which are medium-sized or larger) and a proxy for importance. **Exceptions:** electronic communications, trust services, TLD registries and public administration.
- **MS** will be in a position to add operators **below the size threshold** in the following cases:
  - **Sole providers** of a service
  - Potential disruption of a service provided by an entity could have an impact on **public safety, public security or public health**
  - Potential disruption of a service provided by an entity could induce **systemic risks**
  - Entities with specific **importance at regional or national level** for a particular sector or type of service, or for other interdependent sectors in a Member State
  - Entities considered as **critical under the proposed Resilience of Critical Entities Directive**

European Commission

Which sectors are covered?

Essential entities	Important entities
Energy (electricity*, district heating, oil, gas and hydrogen)	Postal and courier services
Transport (air, rail, water, road)	Waste management
Banking	Chemicals (manufacture, production, distribution)
Financial market infrastructures	Food (production, processing, distribution)
Health (healthcare, EU reference labs, research and manufacturing of pharmaceuticals and medical devices)	Manufacturing (medical devices; computer, electronic and optical products; electrical equipment; machinery; motor vehicles and (semi-)trailers; transport equipment)
Drinking water	Digital providers (search engines, online market places and social networks)
Waste water	
Digital Infrastructure (IXP, DNS, TLD, cloud, data centres, CDN, electronic communications and trust service providers)	
Public administrations	
Space	

*** New types of entities in electricity:** electricity markets, production, aggregation, demand response and energy storage

European Commission

More harmonised security requirements

- Accountability for top management for non-compliance with cybersecurity risk management measures
- Risk based approach: appropriate and proportionate technical and organisational measures
- Measures to at least include:
  - risk analysis and information system security policies
  - incident handling
  - business continuity and crisis management
  - supply chain security
  - security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure
  - policies and procedures to assess the effectiveness of cybersecurity risk management measures
  - the use of cryptography and encryption
  - Cybersecurity certification

More harmonised reporting requirements

- Entities to report both significant incidents and cyber threats
- Entities to inform recipients of their services
- Incident notification in **three stages**:

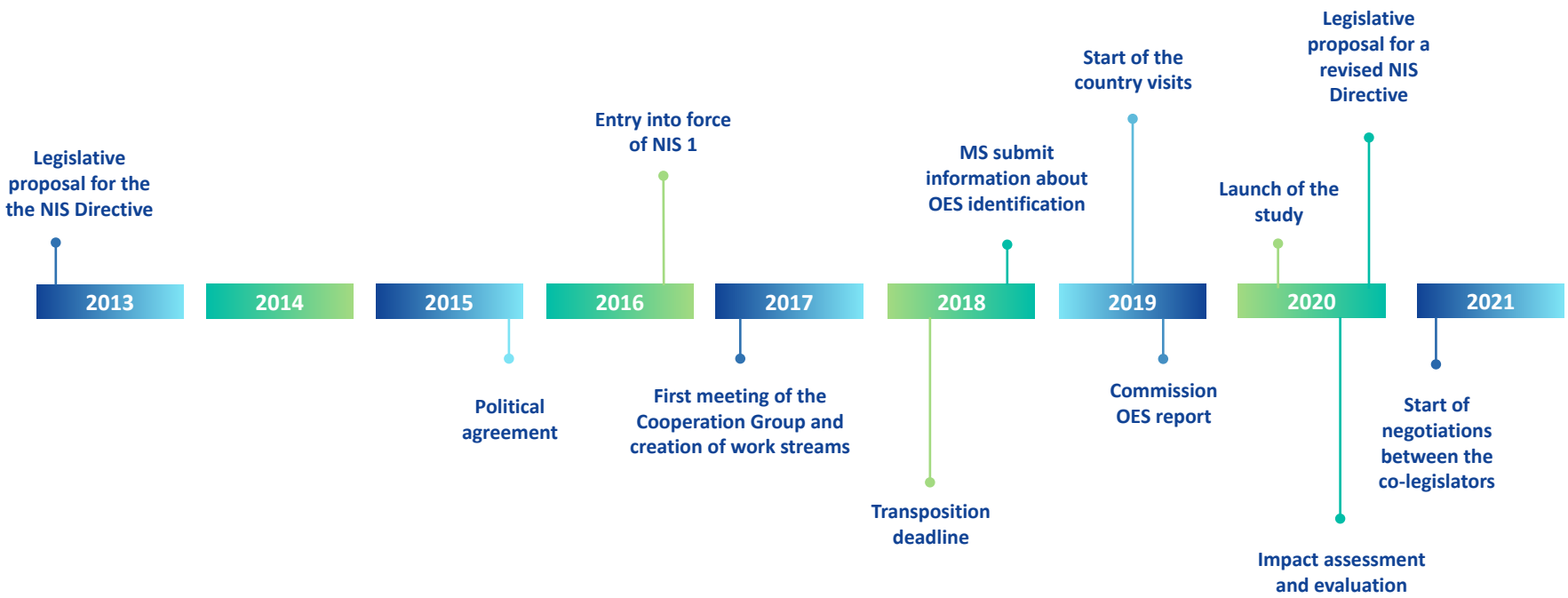
- **MS to inform each other and ENISA of incidents with cross-border nature**

European Commission

Coordinated vulnerability disclosure

- As part of the national cybersecurity strategy, Member States will be required to develop a **policy framework on coordinated vulnerability disclosure**
- Each Member State shall be required to designate one **national CSIRT as a coordinator** and facilitator of the coordinated vulnerability disclosure process at national level.
- In cases where the reported vulnerability affects multiple vendors across the Union, the designated CSIRT shall cooperate with the CSIRT network to facilitate multi-vendor coordinated vulnerability disclosure.
- **European vulnerability registry** run by ENISA

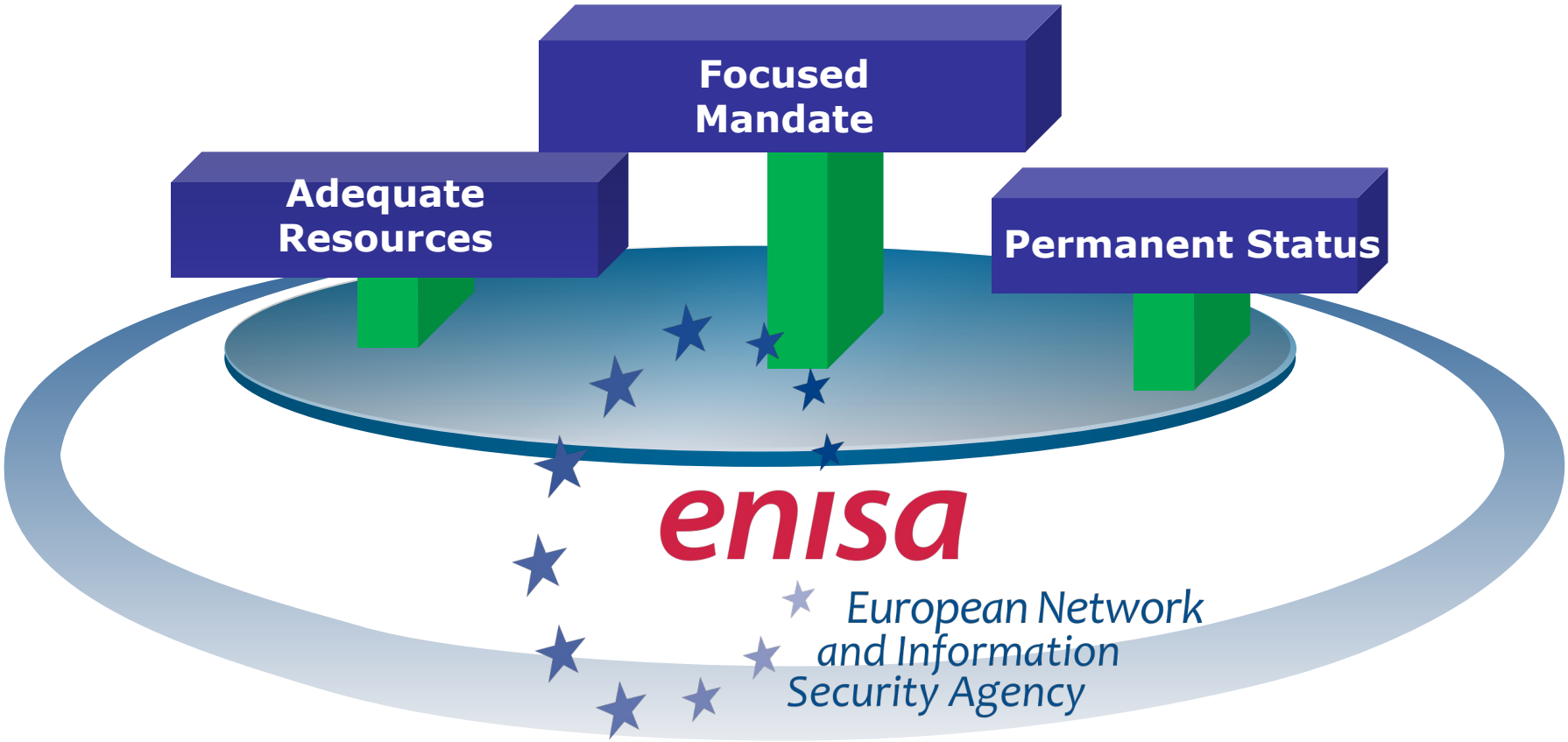
Timeline of the NIS Directive



European Commission

The Cybersecurity Act

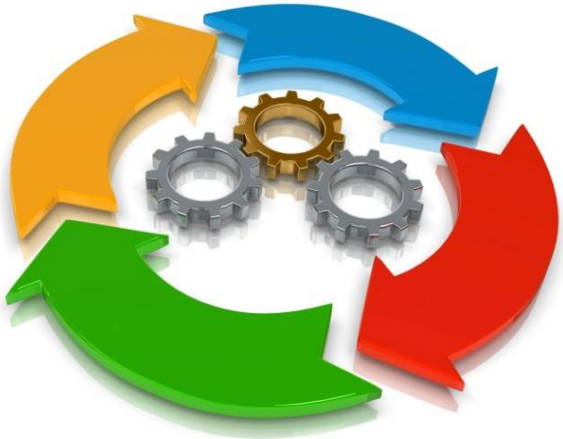
What's new with the regulation?



ENISA's growing role in prevention & response

Cybersecurity Certification

*A **voluntary European** cybersecurity certification **framework….***



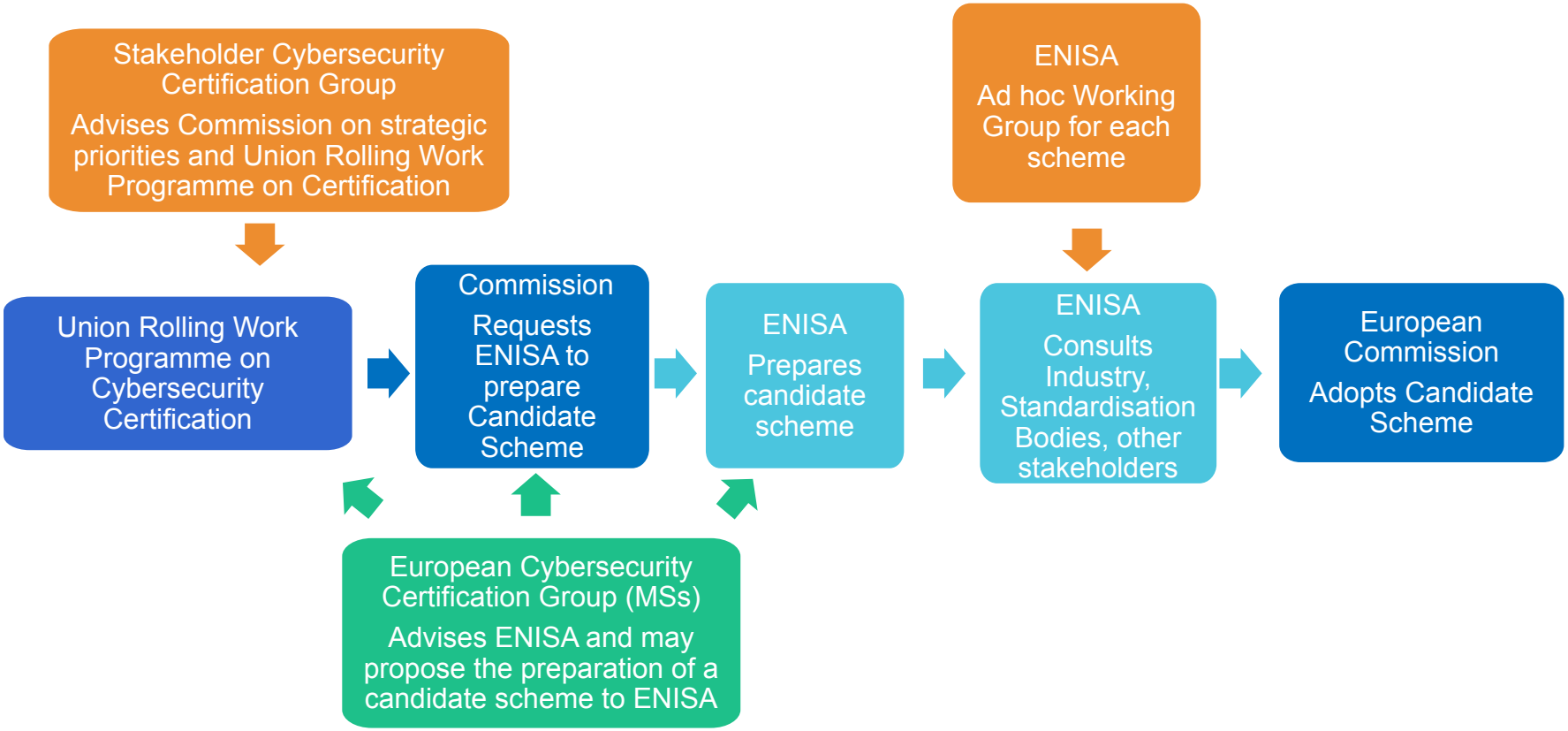
…to enable the creation of tailored EU cybersecurity certification schemes for ICT products and services…

…that are valid across the EU

The European Cybersecurity Certification Framework - features

- One Framework, many schemes
- Voluntary nature: unless specified in future EU/national rules.
- Scope: Products, services, or processes
- Inclusive and transparent governance processes.
- Union Rolling Work Programme for priorities
- Each scheme can contain specific provisions on: re-certification, vulnerability handling and disclosure, provision of updates, surveillance, peer review
- Three **levels of assurance** to be defined on basis of risk of intended use

Establishment of an EU Cybersecurity Certification Scheme



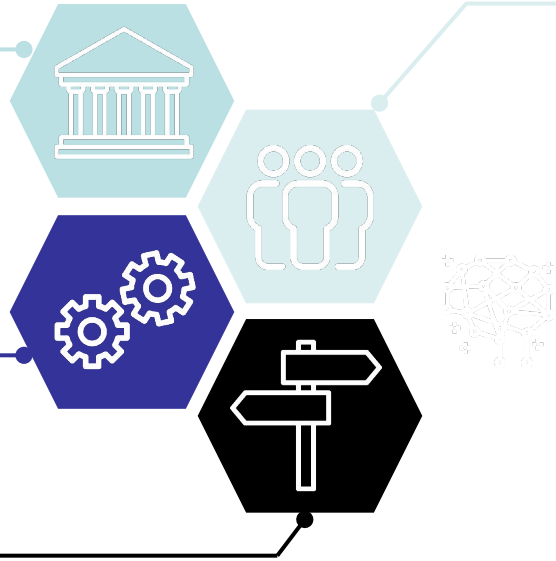
Union Rolling Work Programme for European cybersecurity certification

- Identifies strategic priorities for future European cybersecurity certification schemes;
- Multi-annual document to be drafted by the Commission with inputs from SCCG and ECCG and other stakeholders;
- Cybersecurity Strategy stated that the URWP should be adopted in 2021;
- It shall be updated at least once every three years and more often if necessary.

European cybersecurity certification framework – state of play

Cybersecurity Act

- Entry into force June '19



Advisory groups

- ECCG - established
- SCCG - established

Candidate Schemes

- "SOG-IS MRA" – (Common Criteria)
- Cloud services
- 5G networks

Union Rolling Work Programme for European cybersecurity certification

- Publication 2021

Thank you for your attention!