



The EU coordinated approach to 5G cybersecurity

CEN-CENELEC – ETSI – ENISA conference on
standardisation- Panel 5, 4 February 2021

Julie Ruff, European Commission, DG CNECT

The EU 5G Toolbox: list of measures

RISKS

may be mitigated by  contribute to the mitigation of 

MITIGATING MEASURES

STRATEGIC MEASURES

- a) Regulatory powers
- b) Third party suppliers
- c) Diversification of suppliers
- d) Sustainability and diversity of 5G supply and value chain

TECHNICAL MEASURES

- a) Network security - baseline measures
- b) Network security - 5G specific measures
- c) Requirements related to suppliers' processes and equipment
- d) Resilience and continuity

enabled, supported or made effective with  enable, assist or improve effectiveness of 

SUPPORTING ACTIONS

Identifies **8 strategic and 11 technical measures** to mitigate the risks, and 10 corresponding supporting actions

The EU 5G Toolbox: Risk mitigation plans

Details risk mitigation plans for 9 risk categories identified in the EU risk assessment

MEASURES	Indicative timeframe ¹			Potential impact factors				SPECIFIC MEASURES	RISKS												
	Short-term	Medium-term	Long-term	Resource costs	Sector specific economic impact	Sector specific economic impact	Broader economic / societal		R1: Misconfiguration of networks	R2: Lack of access controls	R3: Low product quality	R4: Dependency on a single supplier	R5: State interference through 5G supply chain	R6: Exploitation of 5G networks by org. crime	R7: Significant disruption of crit. Infras. services	R8: Massive failure due to power interruption	R9: IoT exploitation				
STRATEGIC MEASURES																					
Regulatory powers	✓			✓	✓	✓	✓	SM01													
								SM02													
Third party suppliers	✓			✓	✓	✓	✓	SM03													
								SM04													
Diversification of suppliers	✓	✓		✓	✓	✓	✓	SM05													
								SM06													
5G supply and value chain	✓	✓	✓	✓	✓	✓	✓	SM07													
								SM08													
TECHNICAL MEASURES																					
Baseline network security	✓			✓	✓			TM01													
								TM02													
5G specific network security	✓			✓	✓			TM03													
								TM04													
								TM05													
								TM06													
								TM07													
Requirements related to suppliers' processes and equipment	✓	✓		✓	✓	✓		TM08													
								TM09													
								TM10													
Resilience, continuity	✓			✓	✓			TM11													

Example of risk mitigation plan (risk of low equipment quality)

Risk 3: Low equipment quality

Risk mitigation plan: Apply pressure or incentives on suppliers to increase product quality and increase network security and resilience

Most relevant/high-impact measures	Expected effectiveness	Potential implementation factors	Indicative timeframe
Regulatory powers: SM01: Strengthening the role of national authorities SM02: Performing audits on operators and requiring information	Depends on scope of measures, but can be HIGH or VERY HIGH.	<ul style="list-style-type: none"> Resource costs Sector-specific economic impacts (operators) (potentially) Broader economic and/or societal impacts 	SHORT term
Network security – baseline measures TM01: Ensuring the application of baseline security requirements (secure network design and architecture) TM02: Ensuring and evaluating the implementation of security measures in existing 5G standards	Depends on scope of measures, but can be MEDIUM.	<ul style="list-style-type: none"> Resource costs Sector-specific economic impacts 	SHORT term
Network security – 5G specific measures TM03: Ensuring strict access controls TM04: Increasing the security of virtualised network functions TM05: Enforcing secure 5G network management, operation and monitoring TM07: Reinforcing software integrity, update and patch management	Depends on scope of measures, but can be HIGH.	<ul style="list-style-type: none"> Resource costs Sector-specific economic impacts (operators and suppliers) 	SHORT term. Depends on 5G deployment calendar.
Requirements related to suppliers' processes and equipment TM08: Raising the security standards in suppliers' processes through robust procurement conditions TM09: Using EU-wide certification for 5G network components and/or suppliers' processes	MEDIUM (possibly HIGH at a long term)	<ul style="list-style-type: none"> Resource costs Sector-specific economic impacts (operators and suppliers) 	MEDIUM and LONG term

EU Toolbox recommendations

National level- Member States should:

- strengthen regulatory powers
- strengthen security **requirements** for **mobile network operators**;
- **assess suppliers and apply relevant restrictions/exclusions for high risk suppliers**;
- ensure that each operator has an appropriate **multi-vendor strategy and avoid dependency on high risk suppliers**

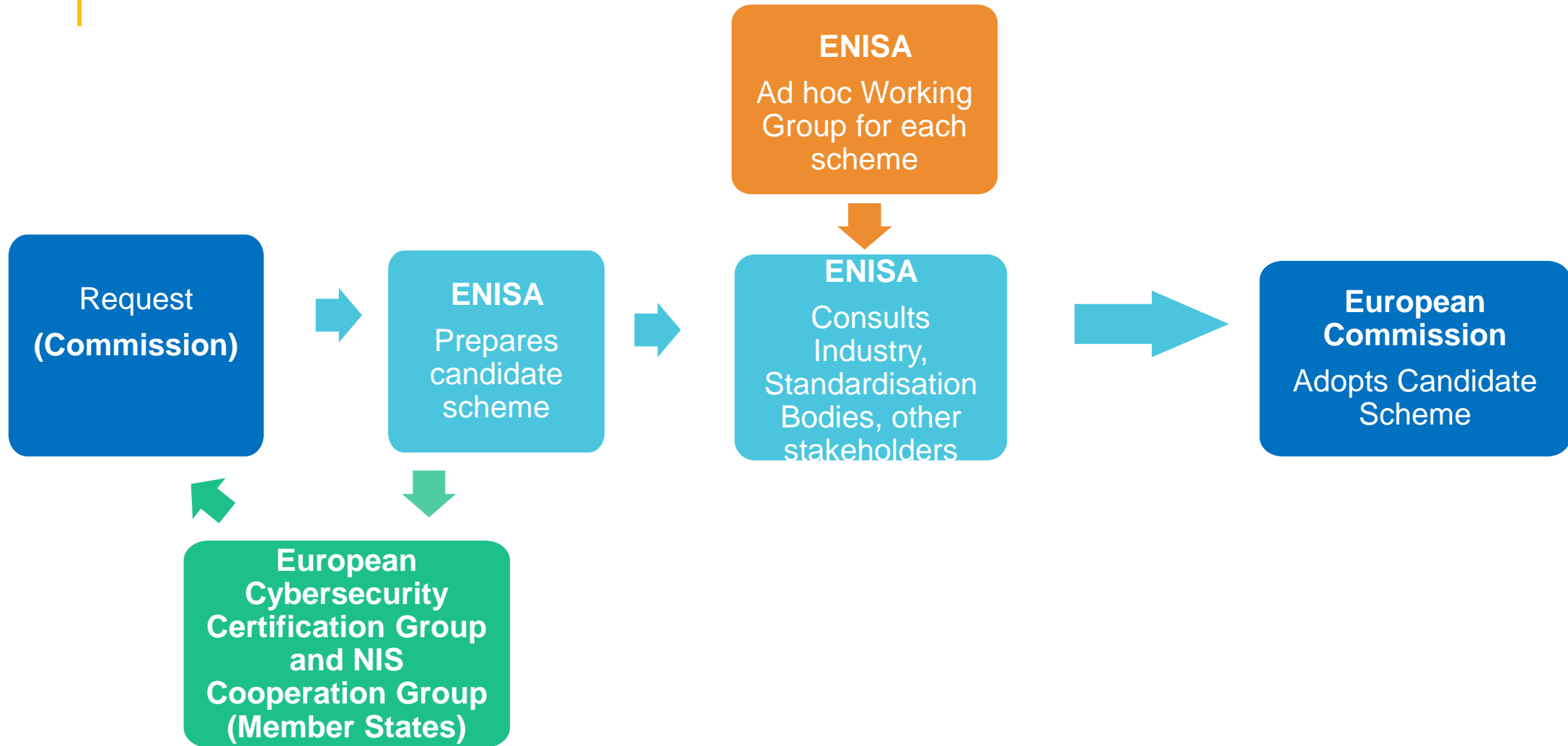
EU level- Commission and Member States should:

- Maintain a **diverse and sustainable 5G supply chain** in order to avoid long-term dependency (including by promoting EU capacities in 5G/6G)
- coordinate between Member States on **standardisation** and develop relevant EU-wide **certification schemes**

Standardisation and certification in the Toolbox

- **TM09: Using EU certification for 5G network components, customer equipment and/or suppliers' processes**
 - **Request for 5G candidate scheme sent to ENISA**
- **TM10: Using EU certification for other non 5G-specific ICT products and services (connected devices, cloud services)**
 - **Candidate schemes on “SOG-IS MRA” – (CC) and Cloud under development**
- **SA03: Supporting and shaping 5G standardization**
 - **Mapping of standards and work to increase representation in standardization fora**
- **SA04: guidance on implementation of security measures in existing 5G standards**
 - **ENISA report under finalisation**

Towards a 5G scheme: next steps



Thank you



© European Union 2021

Reuse of this presentation authorised under the CC BY 4.0 license.

