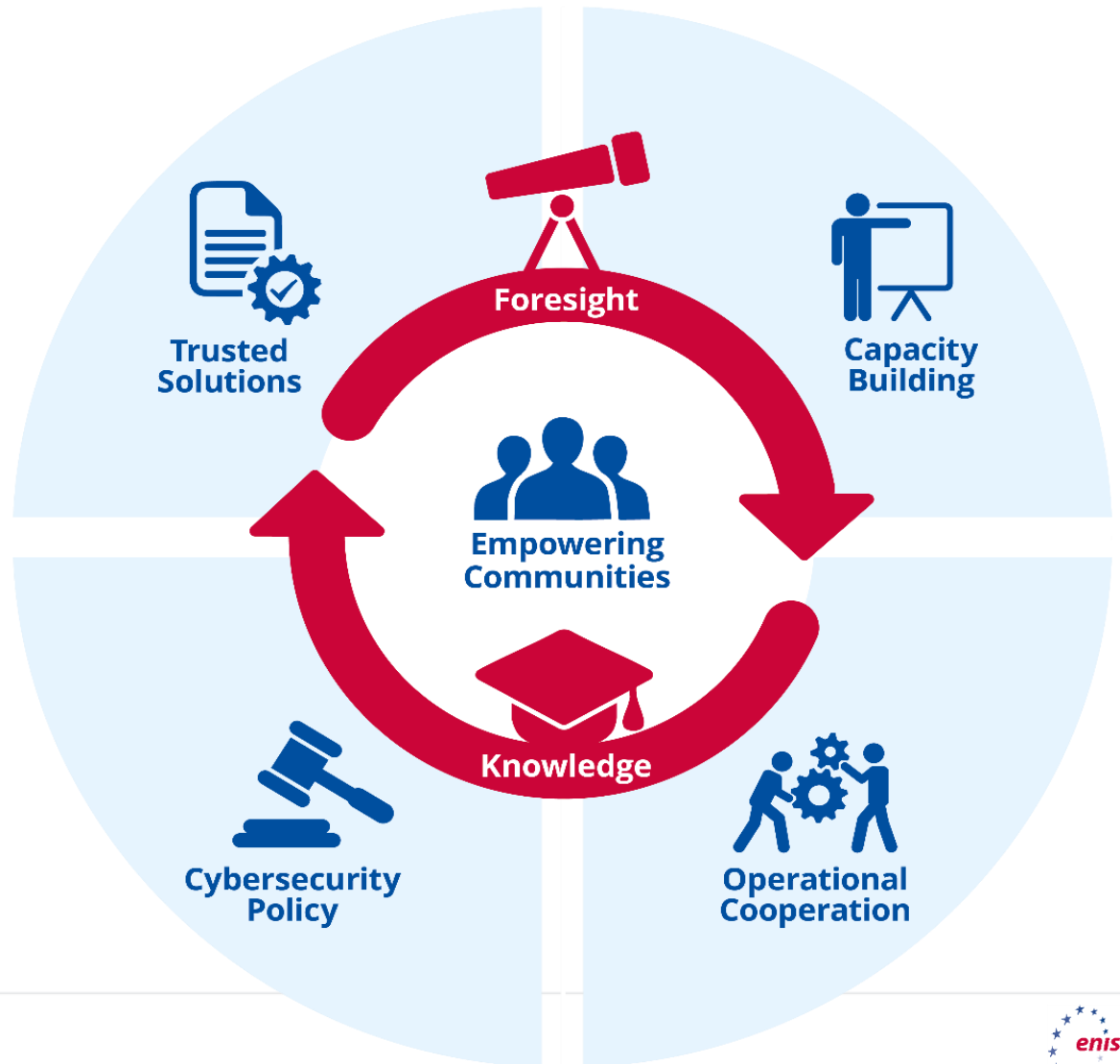# CYBER-MAR WEBINAR

AVIATION SECTOR OVERVIEW

18 │ 01 │ 2022   Ricardo Figueiredo

A TRUSTED AND CYBER SECURE EUROPE

Our mission is to achieve **a high common level of cybersecurity** across the Union in cooperation with the wider community

Foresight

Capacity Building

Trusted Solutions

Empowering Communities

Cybersecurity Policy

Knowledge

Operational Cooperation

"CYBERSECURITY ACT"

- REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

- on ENISA (the European Union Agency for Cybersecurity)

"ENISA shall carry out the tasks assigned to it under this Regulation for the purpose of achieving a high common
level of cybersecurity across the Union, including by actively supporting Member States, Union institutions, bodies, offices
and agencies in improving cybersecurity. "

NIS DIRECTIVE

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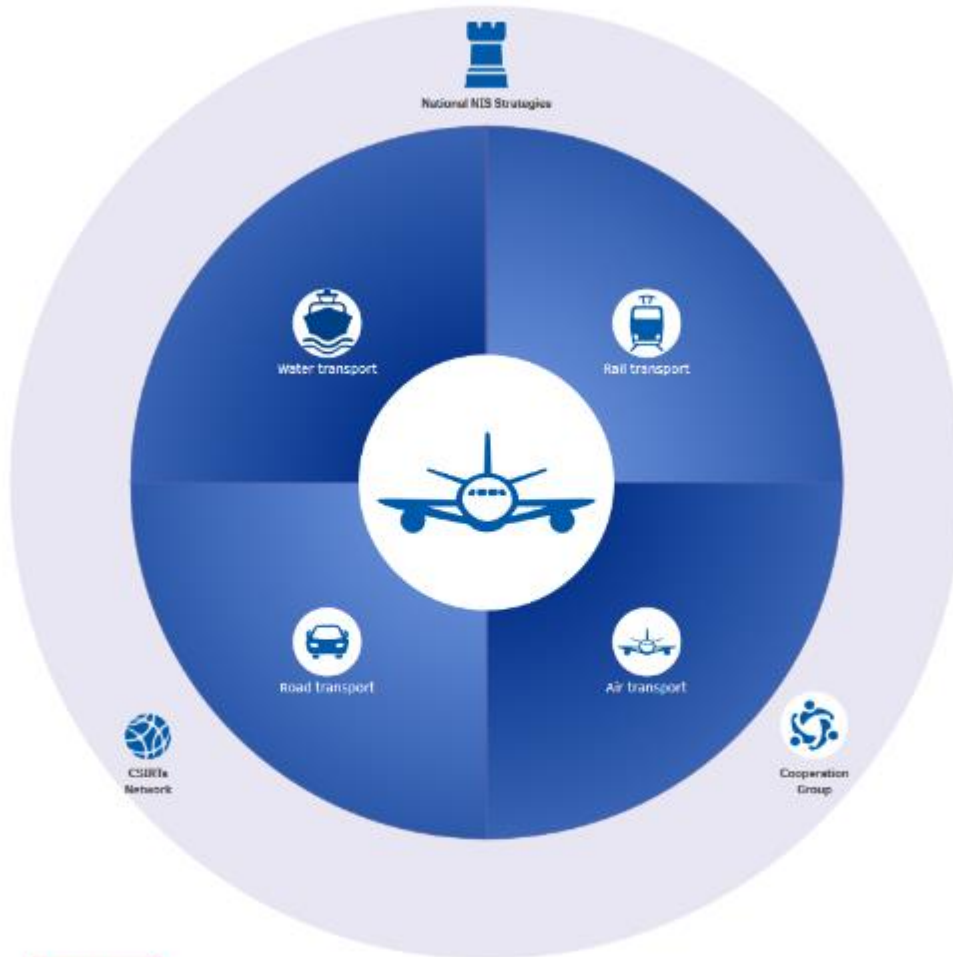
Operators of essential services and Digital Service Providers have to adopt risk management practices and notify significant incidents to their national authorities.

SECURITY MEASURES	NOTIFICATION OF MAJOR INCIDENTS

enisa

NIS DIRECTIVE TOOL

https://www.enisa.europa.eu/topics/nis-directive/nis-visualtool

National Competent Authorities for the Air transport subsector

	Austria	Federal Chancellery of Austria for the strategic transposition
		Federal Ministry of the Interior for the operative transposition
	Belgium	Federal Mobility Minister (Federal Public Service Mobility)
	Croatia	Ministry of the Sea, Transport and infrustructure
	Czechia	National Cyber and Information Security Agency (NCISA)
	Denmark	The Danish Transport, Construction and Housing Authority
	Estonia	Information System Authority (RIA)
	Finland	Finnish Transport and Communications Agency Traficom
	France	National Cybersecurity Agency ANSSI
	Germany	Federal Office for Information Security (BSI)
	Greece	National Cyber Security Authority (General Secretariat of Digital Policy - Ministry of Digital Policy, Telecommunications and Media)
	Hungary	National Directorate General for Disaster Management
	Ireland	National Cyber Security Centre (NCSC)
	Latvia	Ministry of Transport
	Lithuania	Ministry of National Defence
	Luxembourg	Institut Luxembourgeois de Régulation
	Malta	Malta Critical Infrastructure Protection Unit (CIP)

ENISA'S ROLE IN THE NISD

1 Assist MS and the EU Commission in the implementation

2 Participate in the EU NIS Cooperation Group

3 Secretariat for CSIRTs Network

4 Elaborate advices and guidelines regarding cybersecurity

5 Organize exercises

ENISA supports sectorial collaboration

- Increase awareness of sector specific threats
- EU ISACs provide a vehicle and operating model for this collaboration

enisa

THE NISD2.0 PROPOSAL - CONTEXT

- **The EU's (new) Cybersecurity Strategy for the Digital Decade**

  - bolster Europe's collective resilience against cyber threats

  - Trust and security at the heart of the digital society

  - reform the rules on the security of network

  - and information systems (NIS Directive)

  - Build operational capacity (JCU)

  - Increase cooperation (Academia, Industry, ISACs)

THE NISD2.0 PROPOSAL - HIGHLIGHTS

- **New** sectors (e.g. **manufacturing** of transport equipment)

- Entities classified based on their importance (**essential** and **important**) with different supervisory regimes.

- Air transport is considered essential.

- Strengthens **security requirements** (risk management approach, minimum list of basic security elements)

- More precise provisions on the process for **incident reporting**, content of the reports and timelines.

enisa

THE NISD2.0 PROPOSAL - HIGHLIGHTS

- **Security of supply chains** and supplier relationships (supply chain cybersecurity for key ICT (see 5G), coordinated risk assessments of critical supply chains)

- Coordinated **vulnerability disclosure**

- More **information sharing** mechanisms (also at national level)

- Clarifies link with sectorial regulations (*lex specialis*)

NISD & AVIATION

ANNEX II OF THE NIS DIRECTIVE:

- Air carriers
- Airport managing bodies, core airports and entities operating ancillary installations contained within airports
- Traffic management control operators providing air traffic control (ATC) services
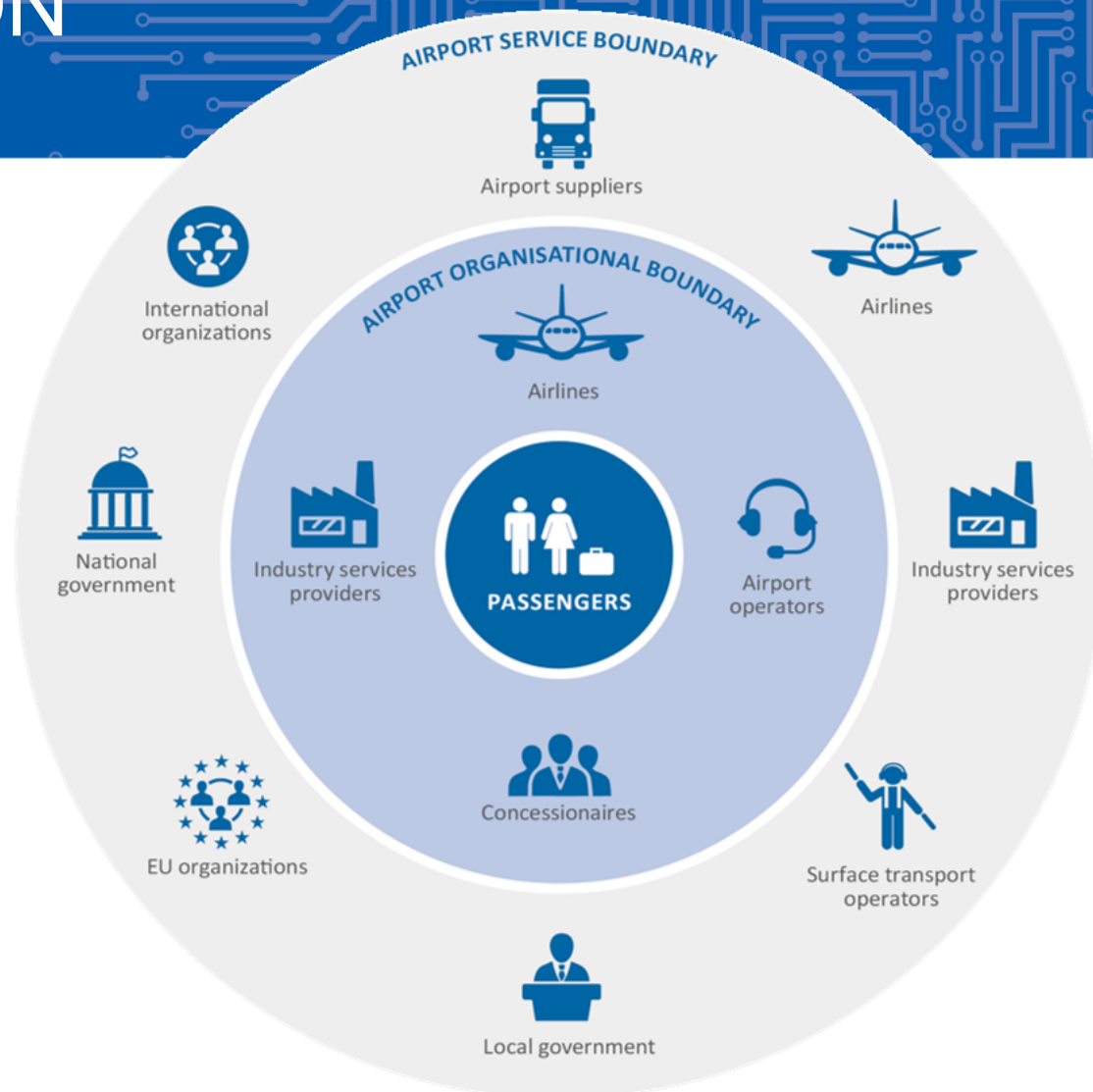
ENISA EFFORTS IN AVIATION

- **Securing smart airports study (2016)**
- **Support of the implementation of the NIS Directive**
- **Support of the review of the NIS Directive and the proposal of NISD2.0**
- **Support of the ESCP**
- **Collaboration with EASA & Eurocontrol**

CONCLUSIONS

NIS Directive – enabler of higher level of security for Europe's Infrastructure

ENISA as catalyst for collaboration and exchange

- Foster sharing about experiences, threats, incidents

- Collecting, consolidating, disseminating good practices

- Work with authorities to achieve EU-wide harmonization

"Collaboration is Everything"

ENISA TRANSSEC Expert Group

Join us:

**https://resilience.enisa.europa.eu/
intelligent-public-transport-
security-and-resilience**

enisa

THANK YOU FOR YOUR ATTENTION

European Union Agency for Cybersecurity

Agamemnonos 14 Str., 15231 Chalandri Attiki,

Greece

📱 +30 28 14 40 9711

✉ info@enisa.europa.eu

🌐 http://www.enisa.europa.eu