The Cyber Security Policy Framework: NIS Directive and Cyber Security in Maritime

Dr. Athanasios Drougkas | Officer in NIS

Maritime Cyber Resilience Forum| Hamburg | 5th September

Positioning ENISA activities

CAPACITY

✓ Hands on activities

POLICY

✓ Support MS & COM in Policy implementation

✓ Harmonisation across EU

COMMUNITY

Mobilizing EU communities

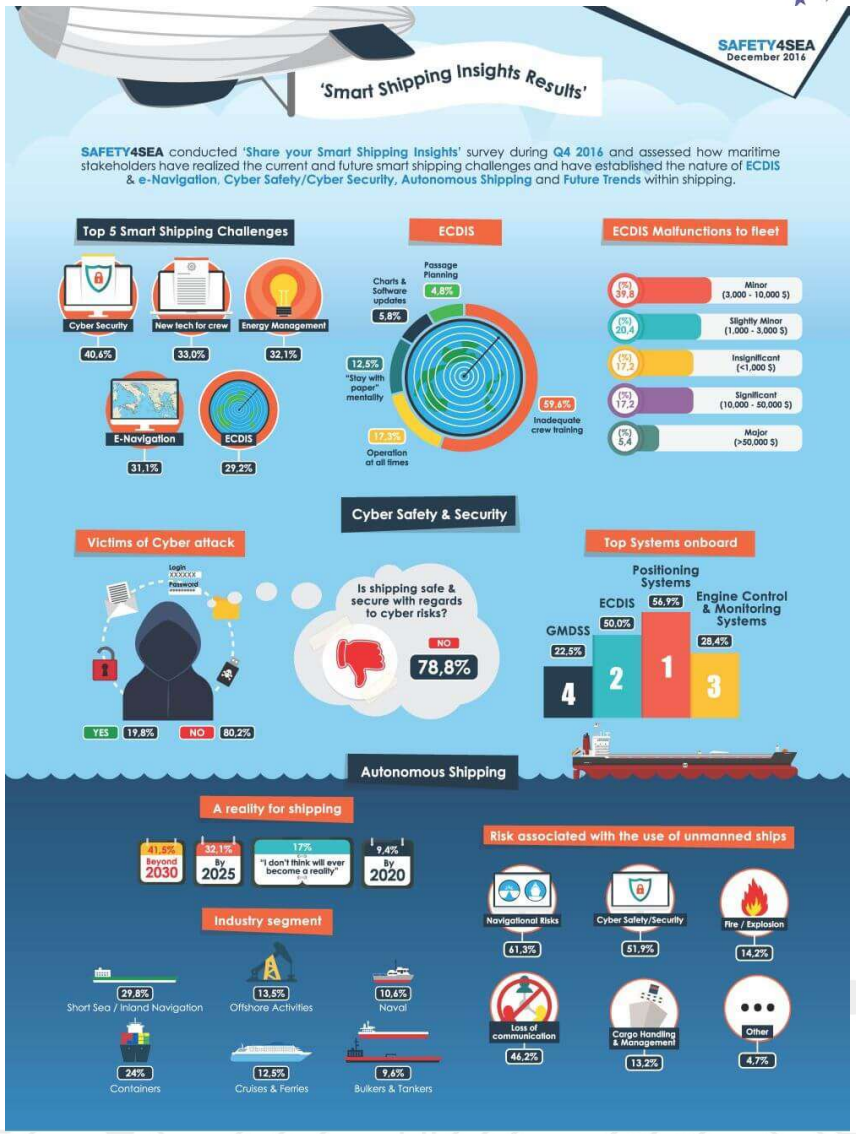
EXPERTISE

✓ Recommendations

✓ Independent Advice

Everything becomes connected

- Fundamental component of European and national Critical Infrastructures
- Passed through a significant transformation from proprietary, isolated systems to open architectures and standard technologies
- Advanced data collection and processing
- Statistics and remote control
- Convergence and interconnection with devices and services
- More functionalities



http://www.safety4sea.com/smart-shipping-survey-findings/

Increasing attack surface

- Positioning systems
- Electronic Chart Display and Information System (ECDIS)
- Engine Control and monitoring systems
- Global Maritime Distress and Safety System (GMDSS)
- Automatic Identification System (AIS)
- Maritime ICS SCADA
  - Alarms and safety
  - Bridge Systems
  - Passenger Servicing & Mgt.
  - Passenger - facing Networks
  - Cargo Management System
  - Etc…

What could possibly go wrong?

Shipping industry vulnerable to cyber attacks and GPS jamming

Luke Graham | @LukeWGraham
Wednesday, 1 Feb 2017 | 8:32 AM ET

CNBC

The shipping industry is increasingly at risk from cybersecurity attacks and a gap in insurance policies is leaving them vulnerable, industry experts have told CNBC.

Cybersecurity has come into focus
become more capable. Meanwhile,
electronic devices to operate.

"This includes software to run the e
systems, automatic identification sy
systems (GPS) and electronic chart
(ECDIS)," explained Matthew Montg
international law firm Holman Fenw

"The added incentive for a hacker is
high value assets and the movemer

Homeland Security

National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Critical Infrastructure Security and Resilience Note

CONSEQUENCES TO SEAPORT OPERATIONS FROM MALICIOUS CYBER ACTIVITY

March 3, 2016; 1300 EST

PREPARED BY: OPERATIONAL ANALYSIS DIVISION

SECURITY

Home News Columns Management Physical Cyber

Home » Maritime Companies Warned of Cyber Attacks

Cyber Security News | Security Newswire | Ports: Sea, Land, & Air

Maritime Companies Warned of Cyber Attacks

Ships are already under cyber attack

Tue 18 Apr 2017 by Martyn Wingrove

Indicative list of incidents

- July 2018: **COSCO Shipping Lines falls victim to cyber attack** - ransomware disrupts electronic communications.
- June 2017: **Maersk hit by NotPetya**. Revenue losses estimated at over $300 million.
- February 2017: **Hackers took 'full control' of container ship's navigation systems for 10 hours**. Presumably a piracy attempt.
- November 2017: **Global shipping firm warns that hackers may leak confidential information** as a result of a "cybersecurity incident".
- June 2011 and for an estimated 2 years: **Cyber-attack on the Belgian port of Antwerp**. Drug traffickers recruited hackers to breach IT systems that controlled the movement and location of containers.
- A survey by Danish Shipping of its CEO panel showed that **69% of companies had been hit by cyber crime last year**

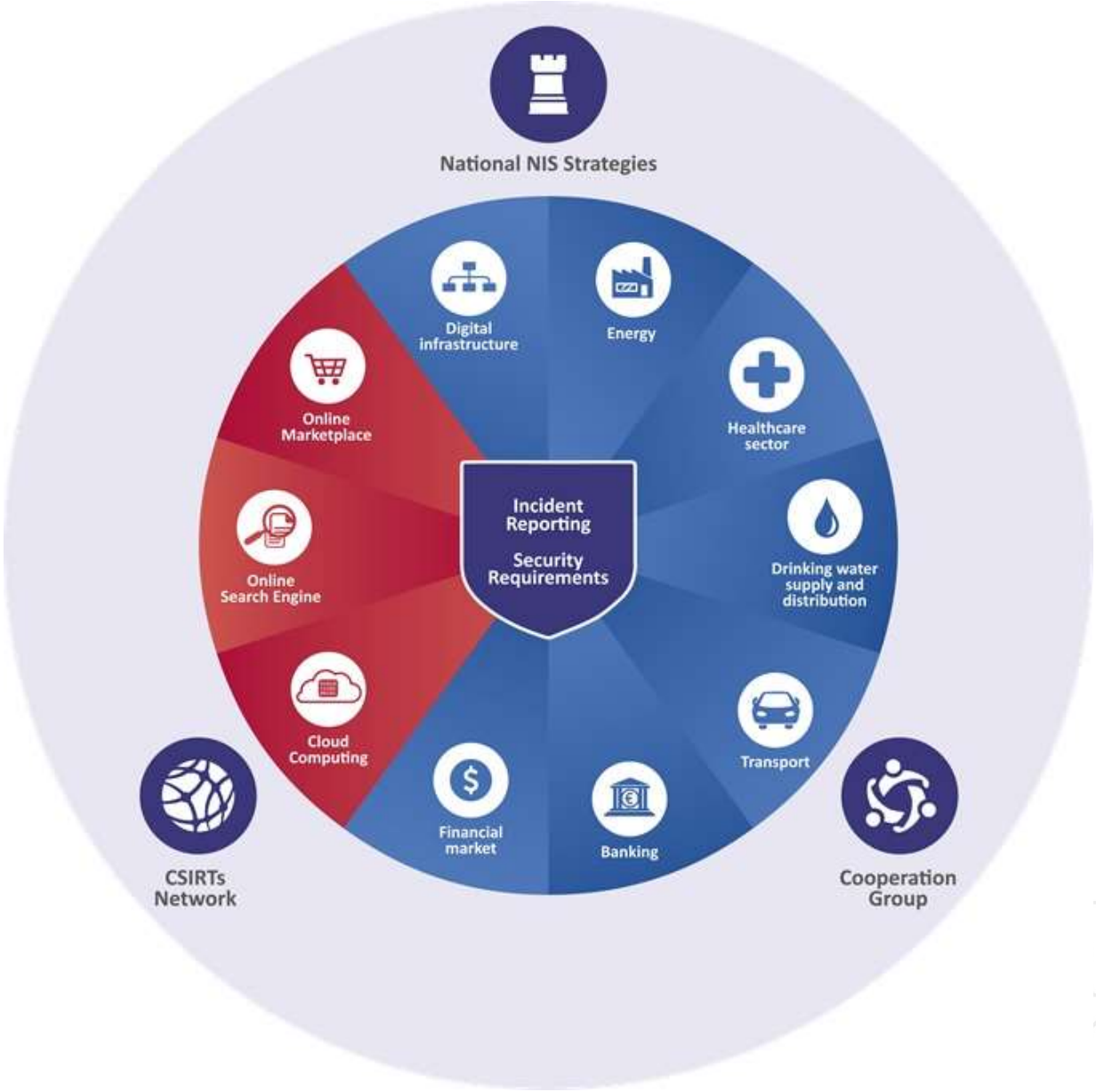
…and that's not all

- Popular **ship communication system diagnosed with 2 critical vulnerabilities** that allow compromise of the system.
- **Ship loading and container load plans are vulnerable to hack** because are created without using a secure messaging system. Integrity violation of BAPLIE.
- Research exposes vessel vulnerabilities to cyber attack. InfoSec company was able to **shift the vessel's reported position and mislead the radar display**.
- Penetration testing experts highlighted how **hackers could sink a bulk carrier** by manipulating the loading data of its hull stress monitoring systems (HSMS) to deliberately cause an imbalance of cargo on the vessel without the crew being aware
- InfoSec experts demonstrate **multiple methods to interrupt and disrupt the shipping industry** at a demo, including hacking the ECDIS to crash the ship (e.g. via GPS offset and reconfiguration to make ship appear much larger) or by exploiting plain text messages of OT systems controlling the steering gear, engines, ballast pumps and more.

Cyber security the maritime sector – Situational Analysis

- **Low awareness** and focus on maritime cyber security
- **Complexity** of the maritime ICT environment including SCADA and emerging IoT usage
- Fragmented maritime **governance context**
- No holistic approach to **maritime cyber risks**
- Overall **lack of direct economic incentives** to implement good cyber security in maritime sector

The Network and Information Security Directive



Obligations for MSs on OESs

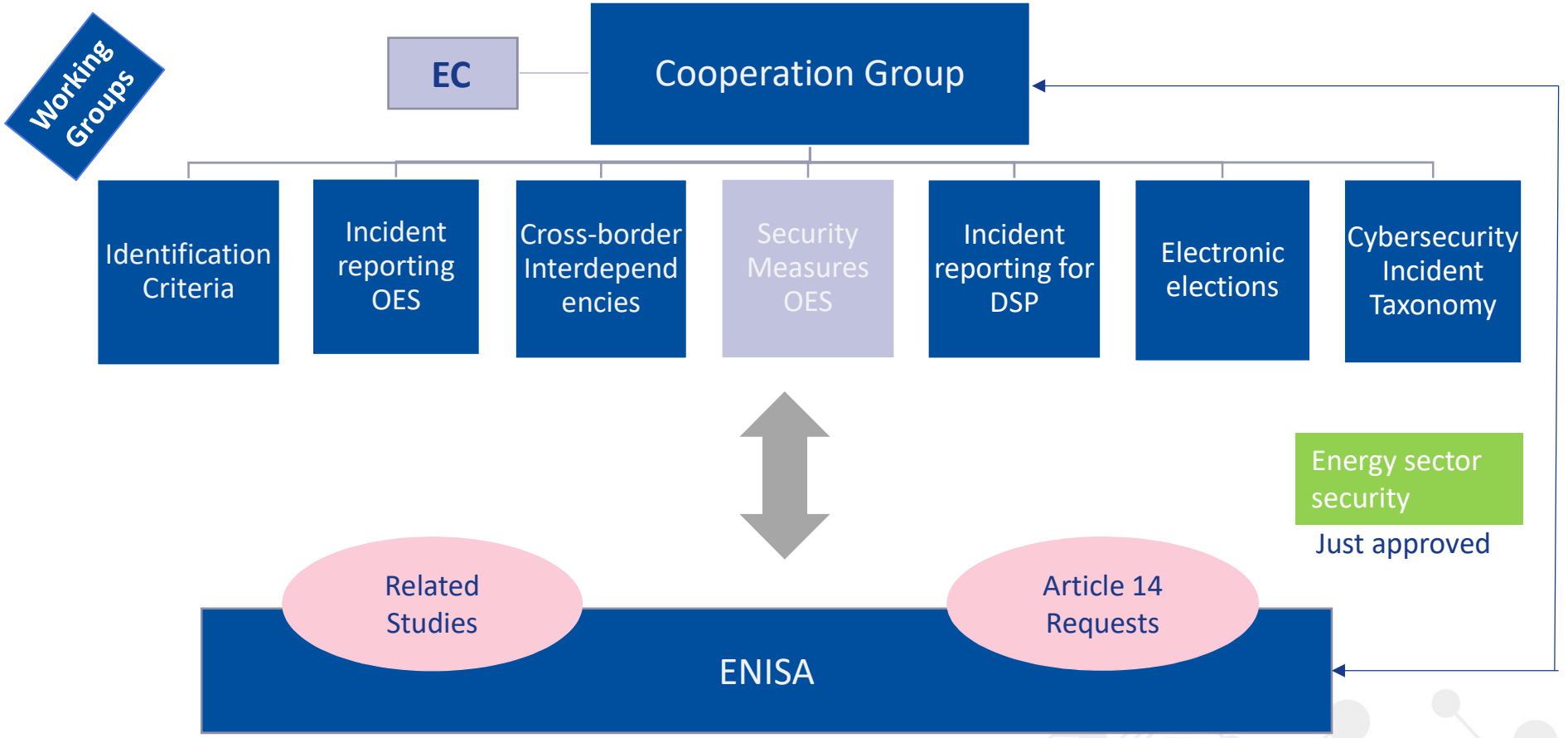
- Identification of operators of essential services
- Minimum security measures to ensure a level of security appropriate to the risks
- Incident notification to prevent and minimize the impact of incidents on the IT systems that provide services
- Make sure authorities have the powers and means to assess security and check evidence of compliance for OES

Identification of OES in the water transport sector

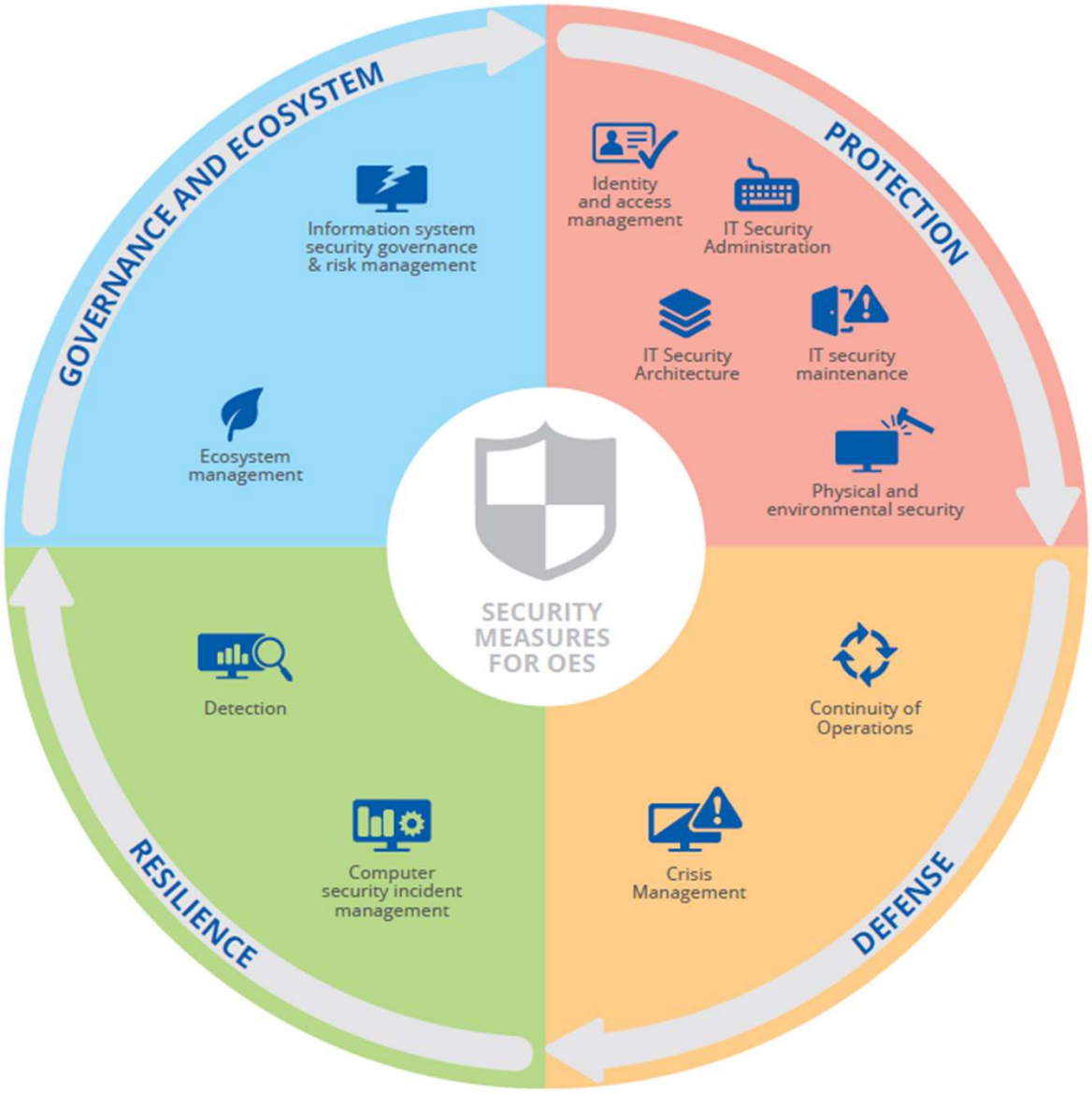
MS shall define the criteria for the identification of operators of essential services and identify the OES among the following:

- Inland, sea and coastal passenger and freight water transport companies (Annex I to Regulation (EC) No 725/2004)
- Managing bodies of ports (point (1) of Article 3 of Directive 2005/65/EC), including their port facilities (point (11) of Article 2 of Regulation (EC) No 725/2004), and entities operating works and equipment contained within ports.
- Operators of vessel traffic services (point (o) of Article 3 of Directive 2002/59/EC)

Working groups under the NISD



Security Measures for OES



NIS directive - TIMELINE

August 2016	-	Entry into force
February 2017	6 months	Cooperation Group starts its tasks
August 2017	12 months	Adoption of implementing on security and notification requirements for DSPs
February 2018	18 months	Cooperation Group establishes work programme
9 May 2018	21 months	Transposition into national law
November 2018	27 months	Member States to identify operators of essential services
May 2019	33 months (i.e. 1 year after transposition)	Commission report - consistency of Member States' identification of OES
May 2021	57 months (i.e. 3 years after transposition)	Commission review

ENISA supporting Cybersecurity in Transport

Sectorial Work

- Support the implementation of NIS-D
- New TRANSSEC Expert Group
- Stakeholder Engagement
- Collaboration with other Agencies and European Commission
- Sectorial ISACs

IoT – Smart Transport

Automotive & Transport

Aviation

- IoT Expert Group - IoTSEC
- Baseline IoT security recommendations
- Vertical IoT Sectors

ENISA and IoT cybersecurity

- Baseline Security Recommendations for IoT
  - Map existing IoT security initiatives
  - Address the problem holistically engaging with wider community
  - Utilize sectorial knowhow
  - Provide horizontal cybersecurity recommendations and security measures
  - One stop shop for IoT cybersecurity in Europe

https://enisa.europa.eu/iot

IoT Security Measures

Policies

- Security by design
- Privacy by design
- Asset Management
- Risk and Threat Identification and Assessment

Organizational, People and Processes

- End-of-life support
- Proven solutions
- Management of security vulnerabilities and/or incidents
- Human Resources Security Training and Awareness
- Third-Party relationships

Technical

- Hardware security
- Trust and Integrity Management
- Strong default security and privacy
- Data protection and compliance
- System safety and reliability
- Secure Software / Firmware updates
- Authentication
- Authorization
- Access Control - Physical and Environmental security
- Cryptography
- Secure and trusted communications
- Secure Interfaces & network services
- Secure input and output handling
- Logging
- Monitoring and Auditing

ENISA and IoT cybersecurity

CONFERENCE

2nd Europol-ENISA IoT Security Conference

The 2nd Europol-ENISA IoT Security Conference focuses on the cybersecurity of the entire IoT ecosystem by providing a platform for all relevant stakeholders to exchange insights and discuss pertinent topics and open challenges.

Time October 24, 2018 10:00 to October 25, 2018 16:30

ENISA supporting Cybersecurity in Maritime

- Support the implementation of the NIS Directive in the Maritime sector
- Mapping of NIS-D requirements with existing standards/guidelines (e.g. IMO)
- Stakeholder Engagement (e.g. SAGMAS, Associations, industry, etc.)
- Collaboration with EMSA and DG MOVE
- **Maritime Work Stream in ENISA TRANSSEC Group – New call for applications has just been announced!**

Next Steps for Maritime Security in ENISA

- Implementation of the NIS Directive
- Stakeholder Engagement
- Raise awareness via workshops and meetings
- Cybersecurity aspects of maritime
  - Guidelines & Standards (e.g. IMO)
  - Regulatory framework
  - Assets / Threat landscape
  - Good Practices
- Use cases (Port security / IoT)

The ENISA TRANSSEC Group is looking for Experts!

Share you expertise and contribute to promoting cybersecurity in maritime!

Join us:

https://resilience.enisa.europa.eu/transport-security

Thank you

PO Box 1309, 710 01 Heraklion, Greece

Tel: +30 28 14 40 9710

info@enisa.europa.eu

www.enisa.europa.eu