Significant increase in cyber threats to critical services and infrastructures calls for enhanced cooperation among private and public sector stakeholders

With its study on critical information infrastructures (CIIs), ENISA analyses current CIIP practices and governance models deployed across EU Member States. This study contributes to the promulgation and future implementation of the NIS Directive.

Citizens and businesses depend on information and communications infrastructure to support online critical services (e.g. energy, telecommunications, healthcare). Increased cyber threats can impact greatly the provision of services and result in loss of money and reputation damage for businesses.

EU Member States and the private sector alike need to co-operate with each other if they want to effectively address these threats today. Yet, only half of the examined countries have established such cooperation models as public–private partnerships, working groups and contact forums.

As some sectors, like finance, telecommunications, and energy are more tightly regulated than others, security requirements differ greatly across sectors and for different types of CII operators. Just a small number of countries have implemented mandatory security requirements across sectors.

This study points out that a few countries, especially the ones with a more decentralised CIIP approach, delegate their national risk assessment to sector-specific authorities or to operators of CIIs. Some countries believe that market pressure will give CII operators sufficient incentives to invest in additional security measures. However, almost none of the examined Member States have implemented incentives to invest in CIIP-related security measures for operators of CII.

Following the validated results of the study ENISA proposes Member States and EU Commission to:

- conduct a thorough national risk assessment
- establish cooperation between public and private stakeholders
- define baseline security requirements to support CIIP development in the MS
- implement incentives that could motivate CII operators to invest more on security measures

Udo Helmbrecht, Executive Director of ENISA, said: ***"Emerging threats to critical information infrastructure constitute a clear and present danger. One which can only be mitigated by coordinated efforts. ENISA works with public as well as private stakeholders to make sure that CIIP is a priority at EU level".***

ENISA provides advice, recommendations and assistance to the EU Member States in implementing relevant EU legislation. The agency engages stakeholders and the industry in exchanging good practices, information and ideas towards the improvement of CIIP in Europe.

In the light of the upcoming NIS Directive and based on the findings of this report, ENISA will continue working on CIIP matters by engaging public and private stakeholders to define baseline security requirements and a harmonised approach to incident reporting.

Full report: More findings and additional information about the study
For technical information: Anna Sarri, Officer in NIS, Anna.sarri@enisa.europa.eu
For interviews and press enquiries please contact **press@enisa.europa.eu, Tel:** +30 2814 409576