



REPUBLIC OF ESTONIA  
INFORMATION SYSTEM AUTHORITY

# Drafting a Cyber Security Act in Estonia

**Elsa Neeme**

Information System Authority

# Draft Cyber Security Act

- Legal analysis November 2016
- Inter-ministerial working group December 2016
- Legislative intent March 2017
- Draft Act proposed for public consultation September 2017
- Submission to Parliament January 2018

# Objectives

- 1) List of the vital/essential services;
- 2) Setout of the General Principles for the stakeholders in ensuring cybersecurity;
- 3) Competence and powers of EISA;
- 4) Preventive and active measures for handling cyberincidents

# Requirements to OES

- risk assessment;
- security measures for network and information systems and related information assets;
- monitoring and sharing;
- restrict usage/access in case of an incident;
- incident reporting

# Incident handling instruments

- the ISPs are required to
  - pass on to EISA the data of Internet session to determine the cause/impact of incident;
- EISA may restrict the usage/access of the network and information systems if
  - *ultima ratio*
  - the possessor is unable to counter the threat or is unable to do so in a timely manner
  - the threat is significant

# Challenges?



# Incident Reporting

Cyberincident must have **significant disruptive effect**

- dependencies of other sectors/entities are often not recognized
- the significant disruptive effect/impact can not be assessed timely nor foreseen
- assessing the cross-border impact can be difficult



REPUBLIC OF ESTONIA  
INFORMATION SYSTEM AUTHORITY

# Thank you!

Elsa Neeme

[Elsa.neeme@ria.ee](mailto:Elsa.neeme@ria.ee)

