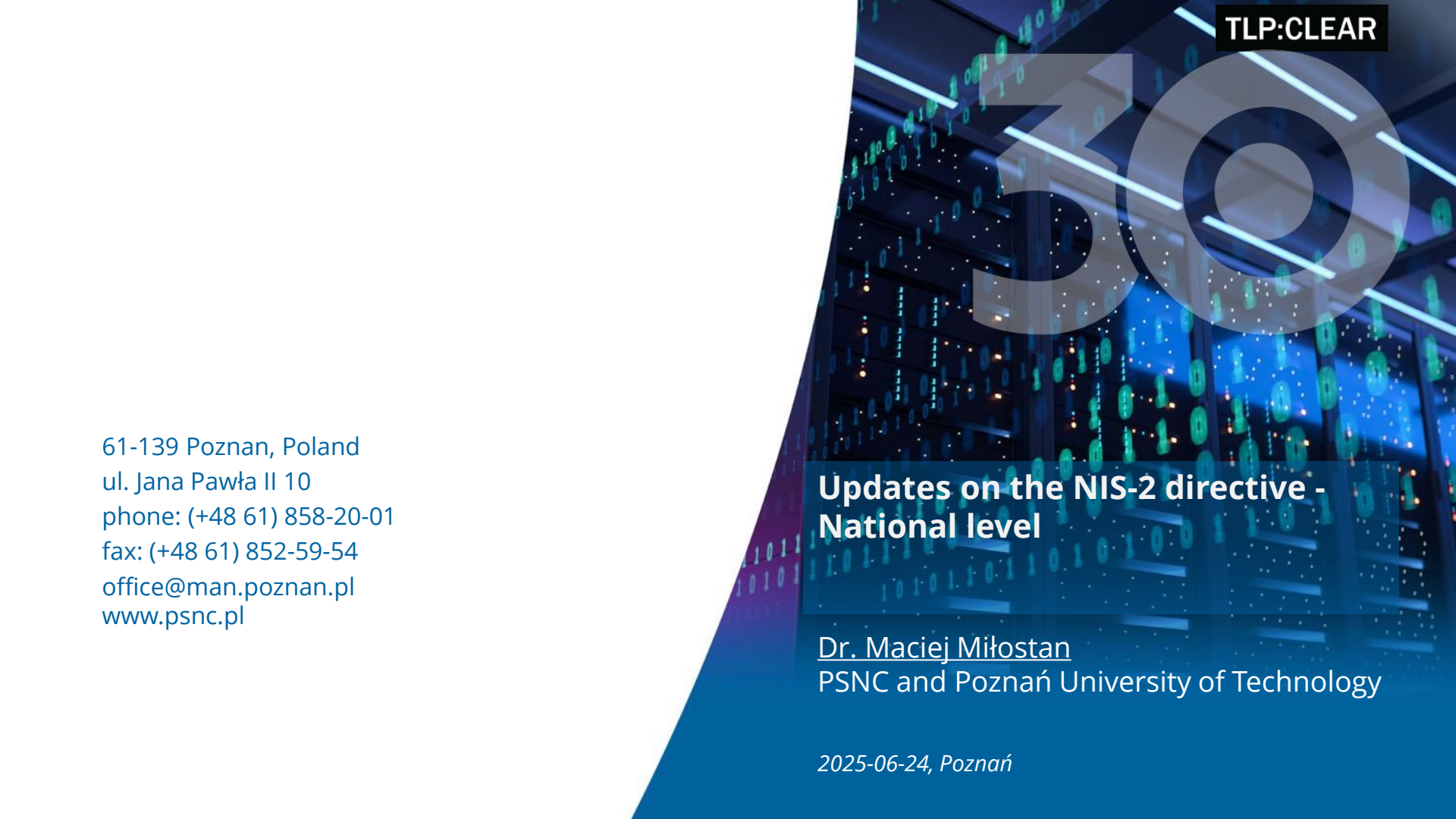
61-139 Poznan, Poland
ul. Jana Pawła II 10
phone: (+48 61) 858-20-01
fax: (+48 61) 852-59-54
office@man.poznan.pl
www.psnc.pl

TLP:CLEAR



# Updates on the NIS-2 directive - National level

Dr. Maciej Miłostan
PSNC and Poznań University of Technology

*2025-06-24, Poznań*

# The act on National Cybersecurity System (in polish: KSC)

KSC

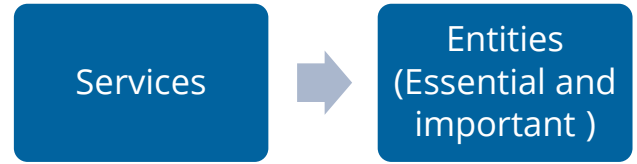
- Legal framework established in 2018 as transposition of NIS1 into Polish legal order
- Initial focus on (as in NIS) critical infrastructures (electricity, natural gas, petrol, water etc.), operators of essential services and digital service providers (not all)
- Established network of national and govermental level CSIRTs
- In 2025, *Draft law amending the Act on the national cybersecurity system and certain other acts* is on the legislation path
- The draft law transposes NIS2 directive
- Poland is already late with that legislation

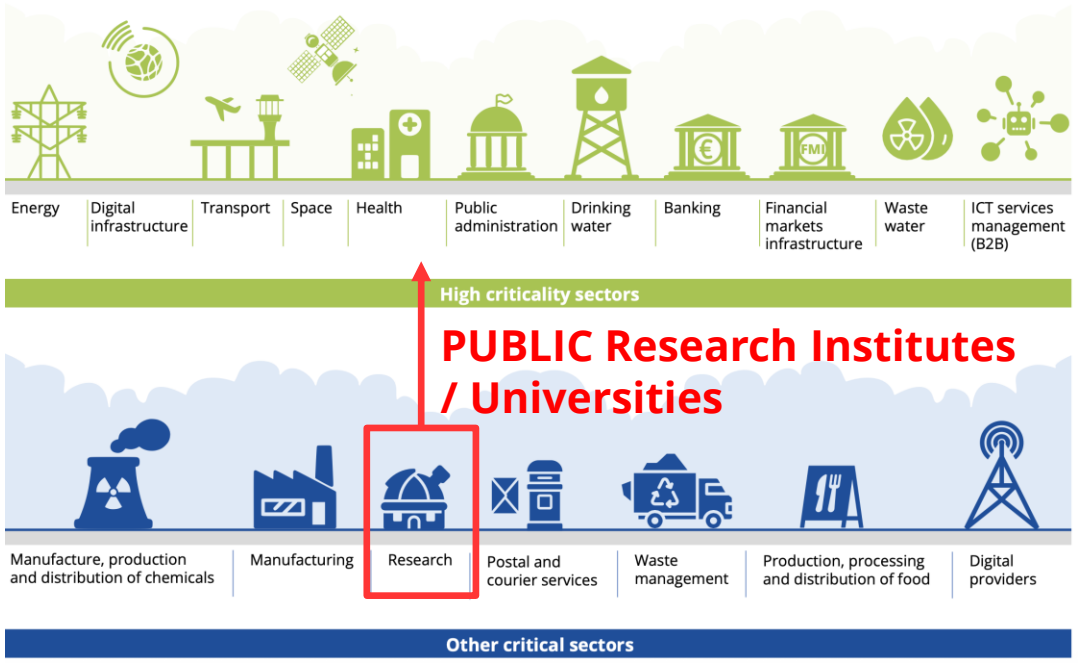
# The path of legislation of KSC amendments


https://legislacja.rcl.gov.pl/projekt/12384504

# Draft amendment - key changes to the KSC

- The proposed changes in National Cybersecurity System (KSC) are coherent with a spirit of **NIS to NIS2 evolution**
  - the emphasis is put on **entities not services**
  - the number of considered sectors is increased accordingly
- Worth to note:
  It highly influence cybersecurity operations of **public entities** including universities, research institutes and scientific institutes



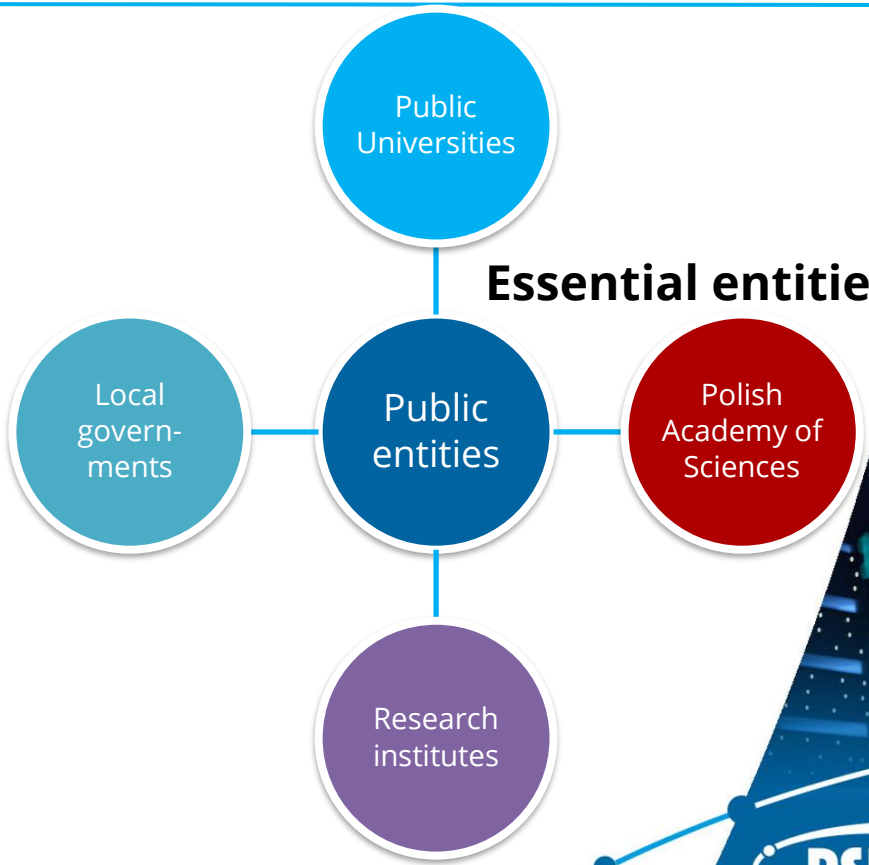



# Essential and important entities

**A public entity**, regardless of its size, is **an essential entity according to draft of Polish bill** (in polish: *podmiot kluczowy*)

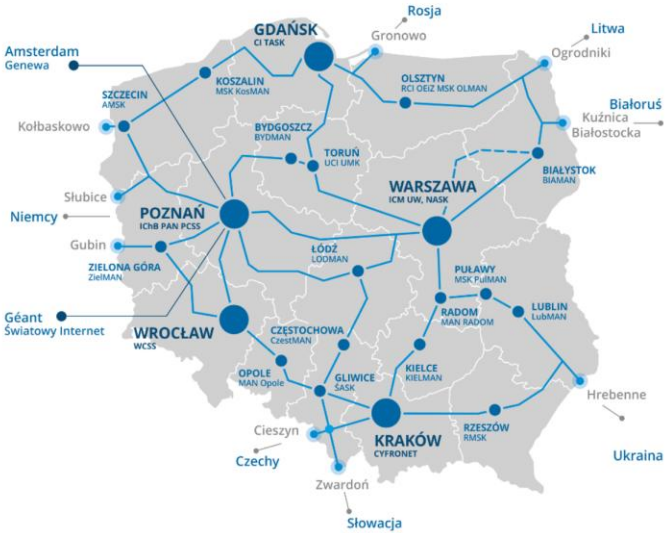
# Essential and important entities

- **Public entities** include, among others, public universities, Polish Academy of Sciences (PAS), Public Research Institutes.
- **Remaining research entities (e.g. non-public universities)** are considered as belonging to less critical sector (the other critical sectors group in NIS2 directive) and group of important entities.
- Research sector in Poland is defined by the Law of Higher Education and Science, private research institutes (besides universities) are not mentioned there
- **Universities** and institutes of **PAS** are **both essential and important entities.**



# Polish Optical Internet (PIONIER NREN) vs National Cybersecurity System

- The **research institutes, universities and local governments are using** (to large extent) networks and resources provided by Polish Optical Internet (**PIONIER**) Consortium
- **The consortium members** (universities and research institutes) operate **data centres** and provide **services in digital infrastructure** sector, in particular, internet **exchange points**, date centre services, cloud computing services, **trust services**
  - **Therefore, that institutions will probably belong to essential entities**
- Requirements for both types of entities are very similar




21 MAN Networks
5 HPC Centres

PSNC is the operator of PIONIER

# Requirements and obligations (1/2)

- The act specifies requirements for entities and their managers
- A **public entity** shall **fulfil** the defined **set of legal obligations**, if it **operates** an **information system** in order to **perform** a **public task**
- The entity shall **establish internal** structures responsible for **cybersecurity** or shall **conclude an agreement with a provider of managed services** in the field of cybersecurity
- It shall prepare, apply and update documentation concerning the **security of the information system** used in the process of providing the service
- It shall **implement an information security management system** in the information system; including, among others,
  - estimating **the risk** of an incident,
  - **physical security**,
  - continuous **monitoring** of services,
  - collecting information on **vulnerabilities**;

  **detailed requirements may be specified by the Council of Ministers**, by way of a regulation, separately for a given type of activity performed by essential entities or important entities

# Requirements and obligations (2/2)

Entity:

- **updates** data in the Polish **registry** of essential and important entities
- carries out a security **audit** of the information system used for the service provisioning at least once **every 3 years** (essential entities)
- **reports early warnings** of serious incidents **within 24 hours** of their detection to the appropriate CSIRT teams
- **reports serious incidents immediately**, no later than 72 hours from the moment of their **detection to the appropriate CSIRT** teams
- **informs users** of its services **about cyber threats** that may affect them, including possible preventive measures, provided that this does not increase the level of risk to the security of information systems
- **informs users about serious incidents**

# CSIRT Teams in Poland

- **National level**
  - CSIRT MON
  - CSIRT GOV
  - CSIRT NASK
- **Sectorial CSIRTs**
  - Under jurisdiction of appropriate Ministry
    - CSIRT KNF – financial sector
    - CSIRT CeZ – health sector (CeZ = Centre of eHealth)
    - CSIRT Cyfra (established this month) – digital infrastructure, only operators of key services (DNS, IXP, TLD)
- **Other CSIRTs – not directly regulated**
  - Critical infrastructures operators
  - Telecoms
  - Network operators (e.g. PIONIER CERT)

# TI – 40 teams in Poland (fast growing community)

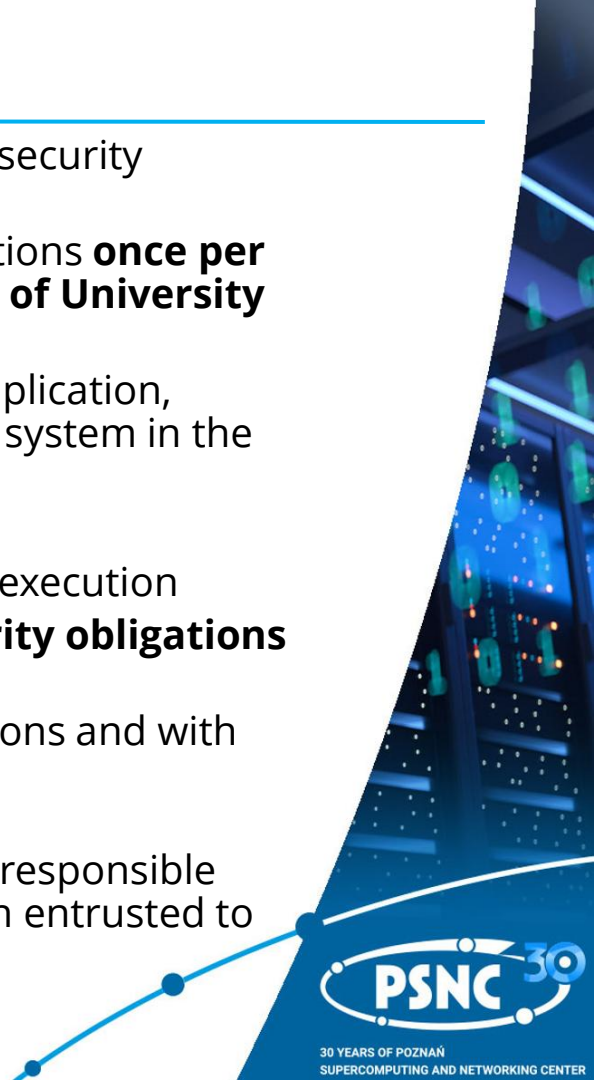
Poland

| | |
|---|---|
| CERT ACL (PL) | Accredited (since 22 Jun 2023) |
| CERT Alior | Accredited (since 26 Aug 2019) |
| CERT ALLEGRO | Accredited (since 21 Oct 2019) |
| CERT Atos (PL) | Listed (since 09 Sep 2024) |
| CERT BIK | Accredited (since 20 Nov 2020) |
| CERT ENEA (PL) | Accredited (since 13 Dec 2022) |
| CERT IT-PKP (PL) | Accredited (since 22 Nov 2022) |
| CERT mBank | Accredited (since 03 Nov 2017) |
| CERT OPL | Certified (since 14 Mar 2016) |
| CERT ORLEN | Accredited (since 26 Feb 2021) |
| CERT PKO BP | Certified (since 28 Jan 2020) |
| CERT Pocztowy (PL) | Re-Listing Candidate (since 24 Apr 2025) |
| CERT POLSKA | Certified (since 23 Sep 2020) |
| CERT PSE | Re-Certification Candidate (since 10 May 2022) |
| CERT TMPL | Accredited (since 31 Aug 2018) |
| CERT.NETWORKS.PL (PL) | Accredited (since 14 Sep 2023) |
| ComCERT.PL | Accredited (since 02 Jun 2016) |
| CSIRT GOV (PL) | Listed (since 19 Oct 2022) |
| CSIRT KNF (PL) | Accredited (since 07 Jul 2021) |
| CSIRT MON (PL) | Listed (since 04 Apr 2025) |
| CSIRT MR (PL) | Listed (since 18 Dec 2024) |
| CSIRT-BOS (PL) | Accredited (since 27 Jun 2023) |
| CSIRT-CEZ (PL) | Listed (since 23 Dec 2024) |
| E.ON CERT PL | Accredited (since 31 Aug 2021) |
| Eurofins SOC (PL) | Accredited (since 14 Nov 2023) |
| ExaCERT (PL) | Accreditation Candidate (since 22 Apr 2025) |
| EY CSIRT (PL) | Listed (since 22 May 2022) |
| GAZ-SYSTEM CERT | Re-Certification Candidate (since 02 Sep 2024) |
| NASK IRT (PL) | Listed (since 27 Oct 2023) |
| Netia SOC (PL) | Listing Candidate (since 24 Apr 2025) |
| NSOC (PL) | Listed (since 01 Apr 2025) |
| PGE-CERT (PL) | Re-Certification Candidate (since 10 May 2022) |
| PIONIER-CERT (PL) | Accredited (since 09 Feb 2024) |
| REDTEAM.PL (PL) | Listed (since 01 Aug 2023) |
| RTFS.PL (PL) | Listed (since 11 Aug 2022) |
| SmartSOC (PL) | Accredited (since 18 Dec 2024) |
| SOC Trecom (PL) | Accredited (since 03 Apr 2024) |
| SOC24.PL | Accredited (since 28 Jan 2019) |
| StillSec iSOC (PL) | Listed (since 18 Aug 2023) |
| VPOL-SOC (PL) | Listed (since 17 Apr 2025) |

PIONIER-CERT is the only team from research and education sector in Poland (besides NASK fulfilling National level CSIRT obligations)
We, in Poland, do not have CSIRTs affiliated to the universities

# Managers' obligations

- **The manager is directly responsible** for the fulfilment of cybersecurity obligations by an essential entity or an important entity
- **The manager attends training** on the above-mentioned obligations **once per year**. Participation in the training must be documented. (**In case of University the manager is Rector**.)
- **Makes decisions** regarding the preparation, implementation, application, review and supervision of the information security management system in the entity
- **Plans** adequate **financial resources**
- **Assigns tasks** in the field of cybersecurity **and supervises** their execution
- **Ensures** that the entity's **personnel is aware of the cybersecurity obligations** and familiar with the entity's **internal regulations** in this area
- **Ensures compliance** of this entity's operations with legal provisions and with the entity's internal regulations
- **The manager cannot wave responsibility**
  The manager of an essential entity or an important entity is also responsible when some of the obligations, or all of the obligations, have been entrusted to another person with their consent.



# Penalties for failure to fulfil obligations

- The detailed list of actions and omissions being subject to a financial penalty imposed on a given entity is specified in Article 73 of the legal act (it includes **lack of incident risk management** among others)
- The amount of the financial **penalty** may not exceed **10,000,000 EUR or 2% of revenues**, but **not less than 20,000 PLN**
- The **penalty may also be imposed on the manager** of the entity in an amount **not exceeding 600% of the remuneration received by the punished person**, calculated according to the rules applicable to determining the financial equivalent for leave

# Information sharing

- Essential and important entities should be granted access to the **system** specified in Article 46 and called **S46** (provided by CSIRT NASK) and be able to **exchange information on cybersecurity**,
- **Entities will also be able to exchange information through mutual agreements**

- The exchange of information is regulated by Article 8h of the draft act

# Restrictions on the use of certain ICT products

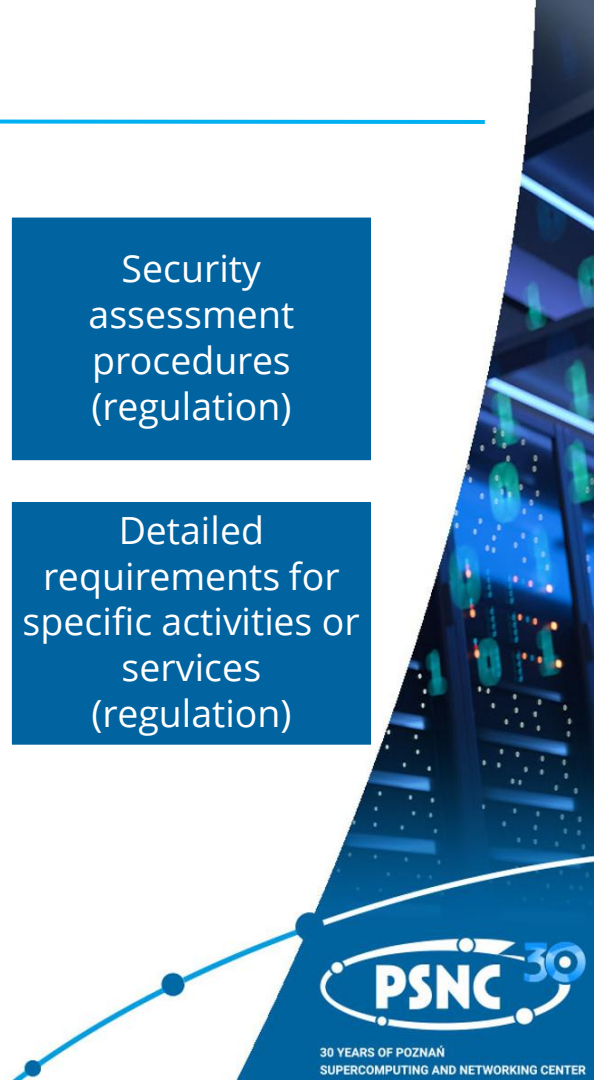
- Under Chapter 12a, **restrictions** may be imposed **on the use of specific ICT products**, services and processes
- Hardware and software from suppliers listed as **high-risk suppliers must be phased out within 4 years**
- This restrictions could be taken into account during public procurements, e.g., allowing to reject offer that include the equipment or software from banned vendors
- It could impact operations of the data centres using equipment of certain Chinese vendors


**Vendor ban will be legal, possible and binding for essential and important entities**

# Additional regulations and resolutions

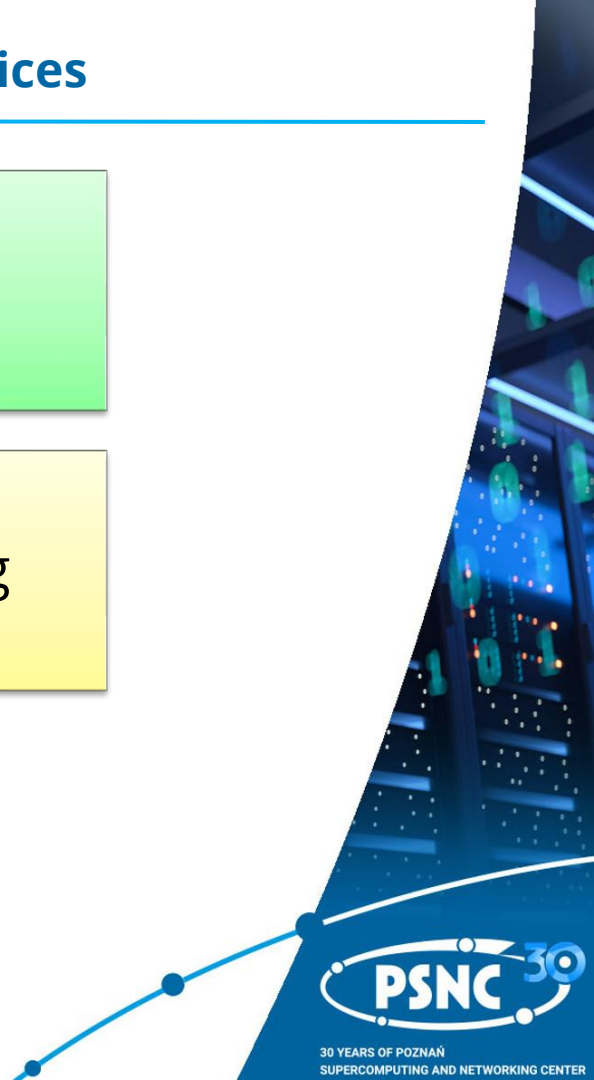
- The Act is accompanied by a number of implementing acts – regulations, some of which will require re-enactment.
- The Council of Ministers may specify detailed requirements for the information security management system for each type of activity conducted by essential entities or important entities,
- The regulation regarding the list of certificates authorizing the conduct of an audit remains in force – no changes are proposed
- The Council of Ministers may specify, by means of a regulation: the procedure and conditions for conducting a security assessment (...)
- The Council of Ministers adopts, by resolution, National Cybersecurity Incident and Crisis Response Plans

| | |
|---|---|
| Requirements for auditors (regulation) | Security assessment procedures (regulation) |
| National Cybersecurity Incident and Crisis Response Plans (resolution) | Detailed requirements for specific activities or services (regulation) |



# Areas of national cooperation and cybersecurity services

- Exchange of CTI
- Situational awareness
- Audits
- Monitoring / SOC services
- Vulnerability management
- Training
- Forensics
- Incident handling support



# Summary

- Poland is working on amendments to National Cybersecurity System (KSC) to adapt it to NIS2
- The draft legislation looks promising but rises also a lot of concerns especially among universities and small research institutes (issues with continuous monitoring and short reaction times, costs of audits etc.)
- Community driven efforts are on the way
- We can expect rise of commercial offerings around cybersecurity managed services targeting various stakeholders
- Establishment of additional sectorial CSIRT teams is highly probable


Sectorial CSIRTs

# Questions

**Dr. Maciej Miłostan**
Maciej.Milostan@psnc.pl