MAIN AREAS OF WORK

- Statistics
- Electricity
- Renewable energy
- Value added tax
- Competition/state aid
- Environment
- Cyber security
- Regulator
- Gas
- Climate
- Energy efficiency
- Oil
- Security of energy supply
- General services
Legislative landscape for security in the energy sector

**SECURITY OF SERVICE**
- Directive on European Critical infrastructure [2008]
- General Data Protection Regulation (GDPR) [2016]
- Directive on the Resilience of Critical Entities

**ENERGY SECURITY**
- (Clean Energy Package) Risk Preparedness Regulation [2019]
- Security of gas supply Regulation [2017]
- Recommendations on cybersecurity in the energy sector [2019]
- Framework Guideline on cybersecurity aspects of cross-border electricity flows [2021]
- Network Code on Cybersecurity

**CYBERSECURITY**
- Directive on Security of Network and Information Systems (NIS) [2016]
- Regulation on ENISA (Cybersecurity Act) [2019]
- Directive on Cybersecurity across the Union (NIS 2)
• **ECI – Identification / Designation**
  – **Identification** – sectoral, cross-cutting, trans-boundary, **Threshold** - severity of impact
  – **Designation** – informing, **ECI** - bilateral discussions, reporting (EC), discretion principles

• **Operators’ Security Plans**
  – **Identification** of assets / threat scenarios
  – **Risk analysis** / vulnerability and potential impact / **Security measures**
  – Periodic review, **supervision**, community measures and compliance with agreed criteria

• **Security Liaison Officers**
  – **Contact point** for communication with national authority – National contact point

• **Threat assessment**
  – **Subsector-related**, reporting, common methodologies, confidentiality

• **Sectors – Energy, Transport**
  – **Oil** – production, refining, treatment, storage, transmission by pipelines
• **Sectors**: Energy (electricity, gas, oil, hydrogen, district heating), Transport, Water, Wastewater, Health, Banking, Financial infrastructure, Digital infrastructure, Public administration, Space
  - **Strategy** on the Resilience of Critical Entities (CE)

• **Identification of CE**: list – for each sector
  - **Criteria** – National Risk Assessment – infrastructure, impact - significant disruptive effects / thresholds
  - **Notification** – service providers, competent authorities, MS, reporting to EC
  - **Competent authorities** (CA) – designation, cooperation with NIS-CA,
  - **Single point of contact** – cross-border liaison function
  - **Information sharing** – confidentiality protection

• **Resilience of CE**: obligations – own (CE) risk assessment
  - Technical / organizational **Measures** to be applied – aimed to accomplish defined targets
  - **Notification** of disruption incidents (to CA) – criteria for significance, CA notifications
  - **Enforcement** of the obligations (audits, penalties)

• **Cooperation**: European significance
  - **Oversight** – advisory missions (European Commission rights and obligations)
  - **Critical Entity Resilience Group** (tasks, competences)

Providing **essential service** to the EU internal market

the role of sectoral regulatory authorities (NRA)

Promotes the role of **VOLUNTARY** form of cooperation
• Build sufficient resilience capacity at national level
  – Adopt a national **NIS strategy**
  – Designate national cybersecurity **authorities**, single **contact points** and Computer Security Incident Response Teams (CSIRTs)

• Identify **Operators of Essential Services (OES)**, and digital service providers

• Structures for cross-border cooperation and exchange of information
  – At strategic level - creating a Cooperation Group of national authorities
  – At operational level - creating a network of national CSIRTs

• Security and notification requirements imposed on OES

• Monitoring and enforcement powers

---

**Directive on security of Network and Information Systems (NIS) (EU) 2016/1148**

- **a)** an entity provides a service which is essential for the maintenance of critical societal and/or economic activities;
- **b)** the provision of that service depends on network and information systems; and
- **c)** an incident would have significant disruptive effects on the provision of that service.
### Challenges of existing NIS Directive (implementation)

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not all sectors that may be considered critical are in scope</td>
<td>Great inconsistencies and gaps due to the NIS scope being <em>de facto</em> defined by MS (case by case OES identification)</td>
</tr>
<tr>
<td></td>
<td>Diverging security requirements across MS</td>
</tr>
<tr>
<td>Diverging incident notification requirements</td>
<td>Ineffective supervision and limited enforcement</td>
</tr>
<tr>
<td></td>
<td>Voluntary and ad-hoc cooperation and info sharing between MS and between operators</td>
</tr>
</tbody>
</table>

**Directive on security of Network and Information Systems (NIS)** (EU) 2016/1148
NIS 2 Main Objectives

1. Cover a larger portion of economy and society (more sectors)

2. Within sectors: systematically focus on bigger and critical players (replace current identification process)

3. Align security requirements (incentivize investments and awareness including by mandating board-level accountability), expand supply chain and supplier relationships risk management

4. Streamline incident reporting obligations

5. Align provisions on national supervision and enforcement

6. More operational cooperation approach including on crisis management

7. Align with proposed Resilience of Critical Entities Directive
**Entities:** scope – categories of ESSENTIAL (same sectors/services as for Critical entities) and IMPORTANT (postal, waste, chemical, food production, manufacturing essential equipment, digital services)

- National Cybersecurity Strategy / crisis management framework / EU Vulnerability Registry
- Authorities – Competent Authorities (CA), single points of contact, CSIRTs

**Cooperation:** structures

- National level – cross-sectoral (CA, Resilience authorities), notifications (incidents, threats)
- Union level – Cooperation Group / CSIRTs network / CyCLONE network (large-scale incidents), Biennial review (ENISA – capabilities, resources, maturity level), Peer-reviews (EC / independent experts)

**Risk management:** entity requirements

- Measures – technical / organizational, MS - governance, EU - coordination (supply chain)
- Reporting – incident / threat notification (CA, CSIRT, recipients – other authorities)

**Sharing of information:** mechanisms (scope, targets, rules) – ISAC forms of cooperation (voluntary notifications)

**Supervision and enforcement:** for each category separately

- Powers of Competent Authorities /
- Administrative fines for infringement on obligations / penalties for infringements on data breach

**Applied to ALL (public and private) entities of the category**

**SME not included, exceptions and special cases are defined**

**ENISA to create and maintain a REGISTRY for both categories**
Cybersecurity – EC Recommendations on Cybersecurity in energy

### Real-time Requirements
- Use international standards
- Apply physical measures
- Classify / manage your assets
- Consider privately owned communication networks, or consider specific measures
- Split system into logical zones
- Choose secure communication and authentication

### Cascading effects
- Evaluate interdependencies
- Ensure communication framework for early warnings and to cooperate in crisis
- Ensure level of security for new devices
- Consider cyber-physical spill overs
- Establish design criteria for a resilient grid

### Technology mix
- Follow a cybersecurity-oriented approach when connecting devices
- Use international standards
- Establish monitoring and analysis capabilities
- Conduct specific cybersecurity risk analysis for legacy installations
- Collaborate with technology providers
- Update hardware and software
Cybersecurity – technology mix in the energy sector
Cybersecurity – Information Security (ISMS) standards

ISO/IEC 27000
- Information technology security Techniques - 49 items

Other security standards:
- ITU - International Telecommunications Union
- ANSI - American National Standards Institute (USA)
- NIST – National Institute of Standards and Technology (USA)

• Information Security Management Systems (ISMS)
  - ISO/IEC 27000:2018 - Overview and vocabulary
  - ISO/IEC 27001:2013 - Requirements
  - ISO/IEC 27005:2013 - Information security risk management
  - ISO/IEC 27019:2017 - Information security controls for the energy industry

• Other relevant ISO/IEC standards
  - ISO/IEC 15408-1:2009 - Evaluation criteria for IT security
  - ISO/IEC 18045:2008 - Methodology for IT security evaluation
  - ISO/IEC 30111:2019 - Vulnerability handling processes

12 │ The Energy Community Secretariat │ 13th OIL FORUM – 12 October 2021
Cybersecurity standard relevant for OT infrastructure - ISA/IEC 62443 series

<table>
<thead>
<tr>
<th>Category</th>
<th>Standard Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>ISA-62443-1-1</td>
<td>Terminology, concepts and models</td>
</tr>
<tr>
<td></td>
<td>ISA-TR62443-1-2</td>
<td>Master glossary of terms and abbreviations</td>
</tr>
<tr>
<td></td>
<td>ISA-62443-1-3</td>
<td>System security compliance metrics</td>
</tr>
<tr>
<td></td>
<td>ISA-TR62443-1-4</td>
<td>IACS security lifecycle and use-case</td>
</tr>
<tr>
<td>Policies &amp; procedures</td>
<td>ISA-62443-2-1</td>
<td>Requirements for an IACS security management system</td>
</tr>
<tr>
<td></td>
<td>ISA-TR62443-2-2</td>
<td>Implementation guidance for an IACS security management system</td>
</tr>
<tr>
<td></td>
<td>ISA-TR62443-2-3</td>
<td>Patch management in the IACS environment</td>
</tr>
<tr>
<td></td>
<td>ISA-62443-2-4</td>
<td>Installation and maintenance requirements for IACS suppliers</td>
</tr>
<tr>
<td>System</td>
<td>ISA-TR62443-3-1</td>
<td>Security technologies for IACS</td>
</tr>
<tr>
<td></td>
<td>ISA-62443-3-2</td>
<td>Security levels for zones and conduits</td>
</tr>
<tr>
<td></td>
<td>ISA-62443-3-3</td>
<td>System security requirements and security levels</td>
</tr>
<tr>
<td>Component</td>
<td>ISA-62443-4-1</td>
<td>Product development requirements</td>
</tr>
<tr>
<td></td>
<td>ISA-62443-4-2</td>
<td>Technical security requirements for IACS components</td>
</tr>
</tbody>
</table>
Cyber Resilience in oil and gas industry – WEF methodology

- **Cyber resilience governance** – Cybersecurity efforts count on broad participation within an organization. Aligning efforts and setting clear accountability are fundamental to success.

- **Resilience by design** – Including cybersecurity as a design parameter and as part of corporate culture helps improve outcomes.

- **Corporate responsibility for resilience** – Recognizing that sophisticated, frequent threats are likely to continue or escalate, organizations should be examining their cyber risks, and taking responsibility for managing those risks.

- **Holistic risk management approach** – As with other risks, managing cyber risks requires a mandate, funds, resources and accountability. In the oil and gas sector, it’s especially important to discover and mitigate risks to all parts of the value chain, so that one weak link doesn’t bring production to a halt.

The WEF’s cyber resilience principles for oil and gas infrastructure are drawn from the shared real-world experience of leading companies in the oil and gas sector. (13.08.2021)
Cyber Resilience in oil and gas industry – WEF methodology

- **Ecosystem-wide collaboration** – Weak links in defences may lie outside of an organisation. Intentional efforts to share cyber threat information, use best practices and improve cybersecurity maturity across the whole sector help industry-wide stability.

- **Ecosystem-wide cyber resilience plans** – Recognizing that cyber attacks will continue to occur, organizations should build resilience plans to help mitigate damage from those that succeed in whole or in part. Cybersecurity exercises enable defenders to test and improve defences – including how they will cooperate with other industry partners.
Cyber Resilience in oil and gas industry – manufacturing

- Identification of Critical Information Infrastructure (ICT) and Operational Technology (OT) assets (segmented)
- Planning / financing of cyber protection – “smart greenfield” / “phased brownfield” methodologies
- Mechanisms for deterrence, defense and recovery from cyber incidents,
- Redundancies / contingencies / backups / unidirectional protection - in IT and OT critical environments
- Human capacity and cybersecurity culture – training, education
- Internal / dedicated professional team for computer security incident response (CSIRT)
- Programs / methodologies for threat identification / risk assessment on company and industry level
- Information Security Management System (ISO/IEC 27000 series) / OT security system (IEC 62443 series)
- Participation in a voluntary, confidential platform for information sharing (ISAC)
THANK YOU
FOR YOUR KIND ATTENTION

simon.uzunov@energy.community.org

www.energy-community.org
Ener_Community
/company/energy-community
/Ener.Community
/EnergyCommunityTV
Tasks of the Contracting Parties

- establish administrative and operational environment (focal points / liaison officers)
- communicate information (reports / strategies / measures) and knowledge (training / research and development / public awareness)
- Develop and apply EU-coherent methodologies for risk assessment / security criteria / identification and designation of essential services and critical infrastructures,
- apply EU technical standards on information security and relevant technologies,
- establish a CSIRTs network (security incidents and threats / capacity building / blueprint for cooperation and early warning / mutual assistance)
- facilitate cooperation with EU MSs / gaining observers’ status in ENISA