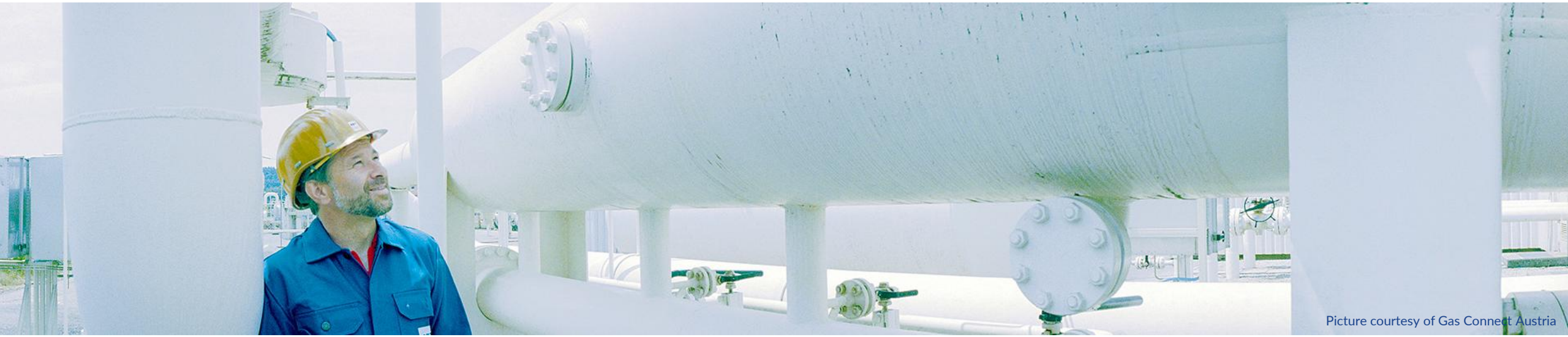
2nd October 2025



Picture courtesy of Gas Connect Austria

5th Edition: Joint ENTSOG, EASEE-Gas, GIE Workshop

DAY TWO: Cybersecurity

2nd October 2025

ENTSOG offices, Brussels

Hybrid

1. Welcome

Dr Andrea Chittaro

SNAM | Chair of the ENTSOG-GIE Joint Task Force on Cybersecurity

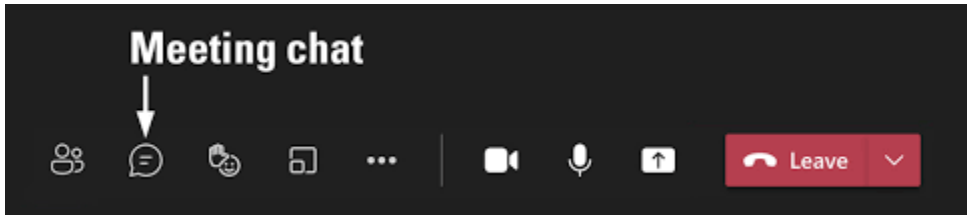
2. Agenda

Douglas Walker Hill
ENTSOG |Interoperability & Data Exchange Advisor

2nd October - Cybersecurity session 09:30-12:00

Event point	Presentation topics for Cybersecurity 2nd October 2025	Presenter	Affiliation	From	To	Duration
1	Welcome, Day 2 - Cybersecurity	Dr. Andrea Chittaro	SNAM (Chair of CS task force)	**09:30:00**	**09:35:00**	00:05:00
2	Agenda	Douglas Hill	ENTSOG	**09:35:00**	**09:40:00**	00:05:00
3	Cybersecurity Stress Tests - info session	Ricardo Figueiredo	ENISA	**09:40:00**	**09:55:00**	00:15:00
4	NIS2 updates	Konstantinos Moulinos	ENISA	**09:55:00**	**10:10:00**	00:15:00
5	Situational update energy sector	Eleni Philippou	ENISA	**10:10:00**	**10:25:00**	00:15:00
6	EC update on security issues and legislation timelines.	Felipe Castro	DG ENER	**10:25:00**	**10:40:00**	00:15:00
7	Break		ALL	**10:40:00**	**10:55:00**	00:15:00
8	NIS2 adoption experiences from National Gas UK	Sebastian Contreras	National gas (UK)	**10:55:00**	**11:10:00**	00:15:00
9	NIS2 adoption experiences from DESFA	Apostolia Angeleri	DESFA	**11:10:00**	**11:25:00**	00:15:00
10	Drill Down on Secure remote access to Industrial Control Systems (TSO Experience)	Fabrizio Zucca	SNAM	**11:25:00**	**11:40:00**	00:15:00
11	CCB updates from Belgium's National Cybersecurity Certification Authority	Johan Klykens - Director of the NCCA	CCB (NCCA)	**11:40:00**	**11:55:00**	00:15:00
12	Wrap up, Q&A	Douglas Hill	ENTSOG	**11:55:00**	**12:00:00**	00:05:00
13	Lunch		ALL	**12:00:00**	**13:00:00**	01:00:00

Questions



- *Online please ask your questions via the **Teams chat***
- *Physical attendance please ask questions at the end of each presentation*

3. ENISA stress tests – an overview

Ricardo Figueiredo
ENISA | ENISA Resilience of Critical Sectors Unit

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENISA'S HANDBOOK FOR CYBER STRESS TESTS: BRIEF OVERVIEW

ENTSOG | EASEE-GAS | GIE CYBERSECURITY WORKSHOP

Ricardo Figueiredo
ENISA Resilience of Critical Sectors Unit

02 | 10 | 2025

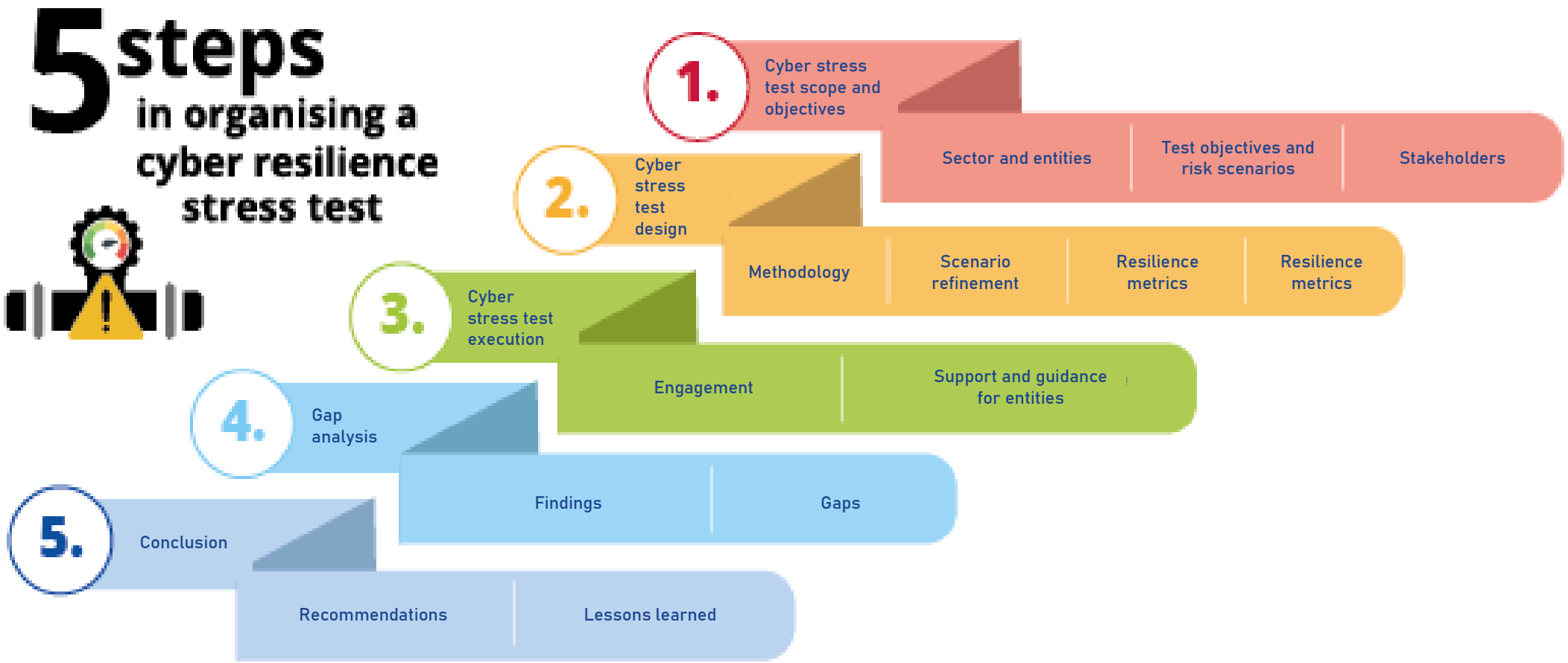
POLICY CONTEXT

- Putting the focus on EU collective situational awareness, preparedness and resilience
  - NIS2
  - Union risk assessments
  - EU 5G toolbox
  - Cyber Solidarity Act
  - CER Directive
  - Niinistö report

A HANDBOOK FOR CYBER STRESS TESTS (ENISA)

- **What is it?** – A handbook for carrying out cybersecurity and resilience stress tests
- **Who is the target audience?** – national or sectorial cybersecurity authorities and national cybersecurity agencies overseeing cybersecurity and resilience of critical sectors, at the national level, regional or EU level
- **Who is in scope of the tests?** - operators of critical infrastructure and providers of critical services under NIS2

CYBER STRESS TEST – STEP BY STEP



CYBER STRESS TEST – WHAT IS IT AND WHY IT MATTERS

Cyber stress test: a cyber stress test is a targeted assessment of the resilience of individual entities and their ability to withstand and recover from significant cybersecurity incidents, ensuring the provision of critical services, in different risk scenarios.

- Resilience focused
- Scenario-based "What-if?"
- Resilience metrics
- Stress levels
- Systemic risk view
- Individual and independent

→

- Supervision beyond auditing
- Combining cyber stress tests with other methods and tools
- Mandatory/stringent versus voluntary/exploratory approach

ADDED VALUE FOR THE EU GAS SECTOR

- Clear benefits for the sector as a whole – entities, regulator/supervisory authority
- Complement other existing cybersecurity assessment and testing methods strengthening preparedness, response and recovery
- uncover sectoral weaknesses and/or common vulnerabilities that otherwise would be unnoticeable
- Set the ground for opening a dialogue between industry and authorities about key cyber risks and threats
- improvement of technical guidance and cyber related policy frameworks

THANK YOU FOR YOUR ATTENTION

Agamemnonos 14, Chalandri 15231

Attiki, Greece

+30 693 651 3960

ricardo.desousafigueiredo@enisa.europa.eu

www.enisa.europa.eu

4. Legislation: NIS 2.0 updates

Konstantinos Moulinos

ENISA | Information security expert

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

IMPLEMENTING THE NIS2 DIRECTIVE

BUILDING UP CYBER RESILIENCE IN THE EU'S CRITICAL SECTORS

ENISA, the EU Agency for Cybersecurity

FROM NIS TO NIS2: WHAT'S NEW

IMPLEMENTATION

- 12 Member States have completed the transposition
- Need for more harmonization across the EU on various topics:
  - ✓ Incident reporting, security measures, supervision, cross border issues etc
  - ✓ On-going work on security measures for essential and important entities
- Address the interplay between NIS2 and others EU legislations
  - ✓ (CER, DORA, EIDAS, CSA, CRA, Cyber solidarity Act, GDPR, Aviation Regulation, Electricity Regulation and other sectorial legislation).
- Discussions on simplification and harmonization are ongoing
  - ✓ CSA review, Digital Omnibus*

***Call for evidence:** https://digital-strategy.ec.europa.eu/en/news/commission-collects-feedback-simplify-rules-data-cybersecurity-and-artificial-intelligence-upcoming

ADDITIONAL CHALLENGES*

- National policy specificities
- Identification of entities
- Sufficient resources for ENISA, European Commission and MS to support the additional tasks of the CG.
- Outreach and collaboration with private stakeholders (companies, industries, education, etc) and law enforcement.
- More frequent and concrete interactions with CSIRTs network, CyCLONe & CERG.

ENERGY CYBERSECURITY FORUM

Stanhope Hotel

REGISTER

https://www.eventbrite.co.uk/e/8th-edsoee-isacencsenisa-cybersecurity-forum-tickets-1414735504979?aff=oddtdtcreator

Q&A

INPUT, IDEAS, SUGGESTIONS VERY WELCOME – ALSO VIA EMAIL OR LINKEDIN

Connect on Linkedin

ENISA-NIS-Directive@enisa.europa.eu

5. ENISA Cybersecurity landscape threat assessment

Dr. Eleni Philippou

ENISA | Information security expert

TLP GREEN

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENERGY SECTOR
BI-MONTHLY SITUATIONAL AWARENESS UPDATE

5TH JOINT DATA EXCHANGE AND CYBERSECURITY WORKSHOP
ENTSOG, EASEE-GAS AND GIE

Eleni Philippou
ENISA, Resilience of Critical Sectors Unit

02 10 2025

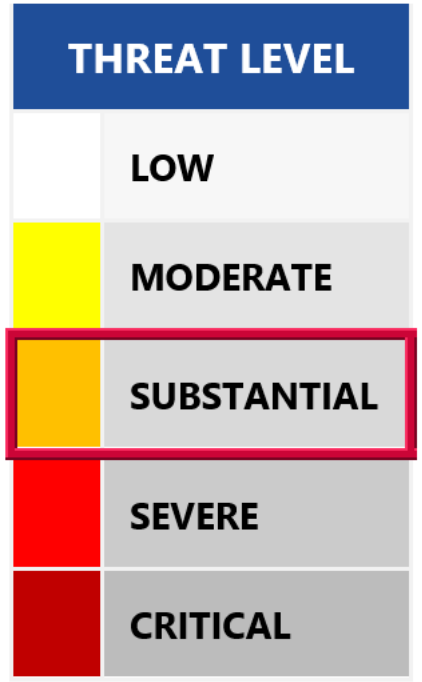
DISCLAIMER

- ✓ *Based on publicly available data, compiled from open sources.*
- ✓ *For **Situational Awareness** purposes only.*
- ✓ *Sources verified on a **best-effort** basis at the time of reporting.*
- ✓ *Referenced opinions **do not represent** an official **ENISA** position*

ENERGY SECTOR
EU - THREAT ASSESSMENT

Reporting period: 01 July – 31 August 2025

The **EU** threat level has been maintained at **SUBSTANTIAL**.



Predominantly opportunistic targeting of the sector:

- Entities reportedly affected across numerous MS by either intrusions or ransomware attacks.

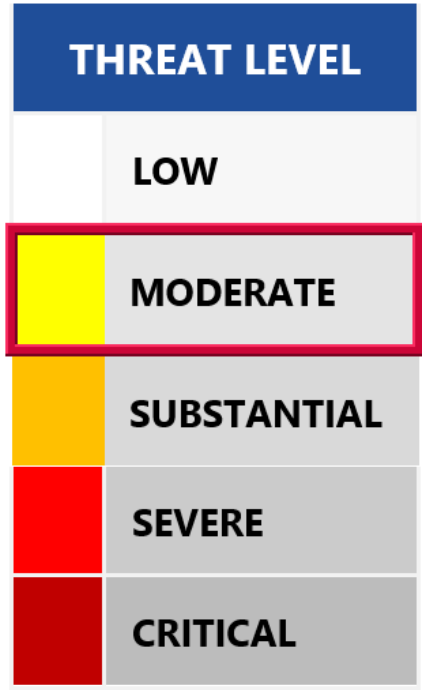
Public reporting during the period:

- *Russia-nexus attackers target Norwegian dam*

ENERGY SECTOR
GLOBAL - THREAT ASSESSMENT

Reporting period: 01 July – 31 August 2025

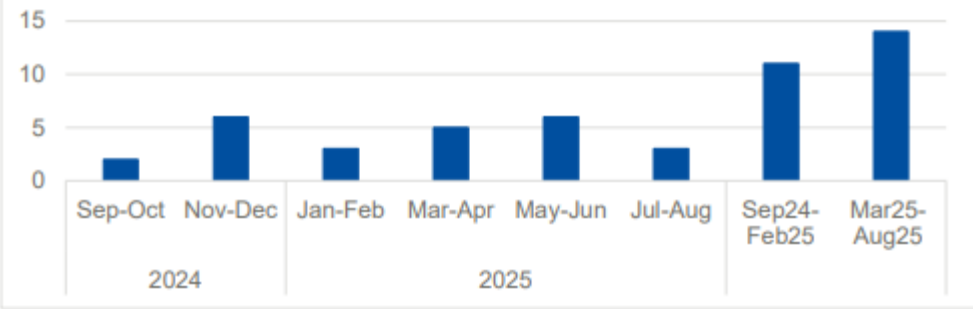
The **Global** threat level has been maintained at **MODERATE**.



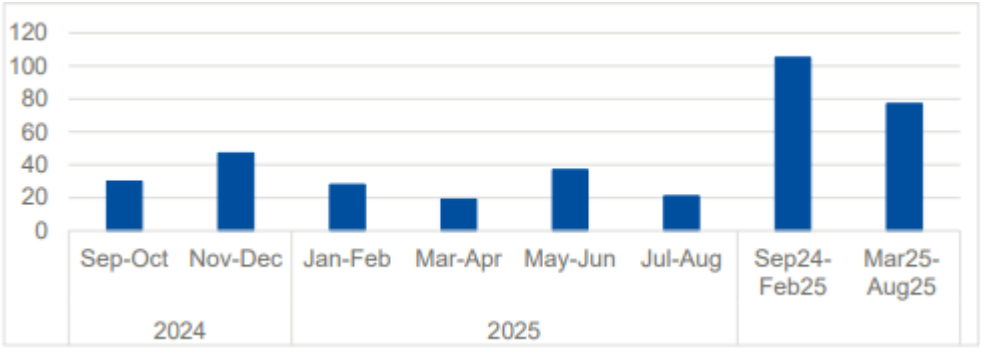
- **Sector entities remain targeted:**
  - *Exploitation of public-facing software products continues to affect critical infrastructure entities.*
    - *Microsoft SharePoint vulnerabilities.*
  - *Russia-nexus threat actor targets Moldovan energy firm.*
  - *Nova Scotia Power reports continued disruption to ICS infrastructure since April's incident.*

SPOTLIGHT ON RANSOMWARE

EU Energy Sector Ransomware Listings Sep 2024 – Aug 2025



Global Energy Sector Ransomware Listings Sep 2024 – Aug 2025



Reporting period operator listings:

- EU: Jul-Aug 2025 ↓
- Global: Jul-Aug 2025 ↓

Past six months vs. six months prior

- EU ~ 27% ↑
- Global ~ 27% ↓

SPOTLIGHT ON VULNERABILITIES

Date Disclosed	**19/07/2025**
Product Affected	**All supported versions of on-premises Microsoft SharePoint servers**

Summary	• The vulnerabilities include:
	  • EUVD-2025-21981 and EUVD-2025-22040 which are variants or bypasses of
	  • EUVD-2025-20554 and EUVD-2025-20552
	• These last two comprise a chain of deserialization vulnerabilities –> “PoC” available known as ToolShell

Observed Usage	• **Initial ‘ToolShell’ chain exploited since 07 July 2025 (patch available since 08 July)** • **Out-of-band patch released for follow-up vulns on 22 July 2025** • **Exploited by Linen Typhoon, Violet Typhoon and Storm-2603 (Chinese state-nexus actors) against internet-facing SharePoint servers** • **Unit42 suggests exploitation of the follow-up vulns since 17 July 2025.**
CVSS 3.x	**6.5 MEDIUM – 9.8 CRITICAL**

SPOTLIGHT ON VULNERABILITIES

Date Disclosed	**24/07/2025**
Product Affected	**Honeywell Experion PKS Bundle**
Summary	• Six vulnerabilities impacting Honeywell Experion Process Knowledge System, a DCS platform for industrial automation and process control used in the energy sector. • The most critical vulnerability amongst those EUVD-2025-21063, could be exploited by a remote unauthenticated attacker to achieve communication channel manipulation, which could result in a failure during subtraction, allowing remote code execution.
Observed Usage	**None**
CVSS 3.x	**9.4 CRITICAL**

SPOTLIGHT ON VULNERABILITIES

Date Disclosed	**19/08/2025**
Product Affected	**Tigo Energy Cloud Connect Advanced -**
Summary	• Three vulnerabilities impacting Tigo Energy Cloud Connect Advanced, a solar photovoltaic (PV) data logger and gateway for module-level monitoring and control. • EUVD-2025-23883, the critical severity vulnerability could allow unauthorised users to gain administrative access due to hard-coded credentials → escalate privileges → full control of device (modifying system settings, disrupting solar power production, interfering with safety mechanisms).
Observed Usage	**None*** although a proof-of-concept exploit is reportedly available for EUVD-2025-23875, thus increasing the likelihood of potential exploitation of unpatched PV units
CVSS 3.x	**9.8 CRITICAL**

SPOTLIGHT ON INCIDENTS

JUL
08

SECTOR16 claims access to Hungary-based geothermal system

particularly to multiple components including fans, compressors, emergency protocols, pressure and temperature sensors.

- SECTOR16 is a pro-Russia hacktivist group
- First observed in January 2025
- Emerged as collaborators of Z-PENTEST
- Primarily claims intrusions against oil, gas and water sectors.
- Posts include videos & images to amplify credibility of claims.

JUL
12

SafePay lists BARTEC

- BARTEC is a German company that operates in the manufacturing of explosion protection and safety technology products used in the energy industry.
- 21GB of data allegedly exfiltrated (operational and employee data including sales orders, invoices and meeting notes).
- BARTEC has published a press-release to inform of unauthorized access to the servers of BARTEC Pte (Singapore) resulting in the leakage of certain data.

SPOTLIGHT ON INCIDENTS

JUL 28

Darkforums user advertises access to Lukoil Bulgaria fuel tank telemetry

- Darkforums user ‘TCMSecurity’ advertised alleged real-time access to Lukoil Bulgaria’s fuel tank telemetry.
  - *No confirmation and user has low reputation and only a few prior posts.*
- In the listing, the actor claims they can provide access to Lukoil’s Rosemount TankMaster system, that monitors fuel storage tank metrics.

JUL 28

WorldLeaks lists Acea group

- Worldleaks ransomware group lists Acea, an Italian group that manages integrated water, electric, gas and waste management utility services.
- The listing claims the actor’s purported access to 2.9TB of exfiltrated data.
- *No confirmation from Acea*

SPOTLIGHT ON INCIDENTS

JUL
18

Gazprom allegedly disrupted by Ukraine's HUR

- According to a representative of Ukraine's military intelligence agency (HUR), the HUR conducted a large-scale cyberattack against Gazprom.
- The operation allegedly took place on July 17th and reportedly impacted 390 of Gazprom's subsidiaries and branches.
- Involved the deployment of custom malware to disable 20K system administrators, exfiltrated and wipe backups (contract records, tarrifs, payment records etc.)
- *Gazprom has not publicly acknowledge the incident.*

ON ANOTHER NOTE

*Only **a few days left***

to contribute to the 2025 ENISA NIS360!

Survey closes 6th Oct 2025 - EOD

enablor.dk/auth/register/survey/e900d95d70cc424e9018b791ef66f469?lang=en&enisa=true

Give us a real-world insight of what's going on in your sector!

THANK YOU

Agamemnonos 14, Chalandri 15231
Attiki, Greece

+30 28 14 40 9711

info@enisa.europa.eu

www.enisa.europa.eu

7. EC Update On Security Issues Plus Overview On Legislation And Timelines.

Felipe Castro
DG ENER

DG ENER update on cybersecurity. Overview on legislation and timelines.

5th Joint Data Exchange and Cybersecurity workshop

Felipe Castro. European Commission. DG ENERGY

Unit F4: Energy security and safety

2 October 2025

European Commission

Network Code on network code on sector-specific rules for cybersecurity aspects of cross-border electricity flows

Status update

Designation of Competent Authorities (Art.4)

State of play:

- 10 MS designated a competent authority, 17 competent authorities have not yet been designated (but 6 MS communicated with COM/ACER temporal arrangements)
- The deadline for designating was 14/11/2024 and notifying 13/12/2024.

NCCS Methodologies

State of play for some key deliverables

- Cybersecurity risk assessment methodologies: approved by All TSOs and DSO Entity Board
- Cyber-attack Classification Scale Methodology: approved by All TSOs and DSO Entity Board
- Recommended provisional electricity cybersecurity impact index ('ECII'): published
- Recommended provisional list of European and international standards and controls: published
- Guide on benchmarking the costs and effectiveness of cybersecurity investments: issued by ACER

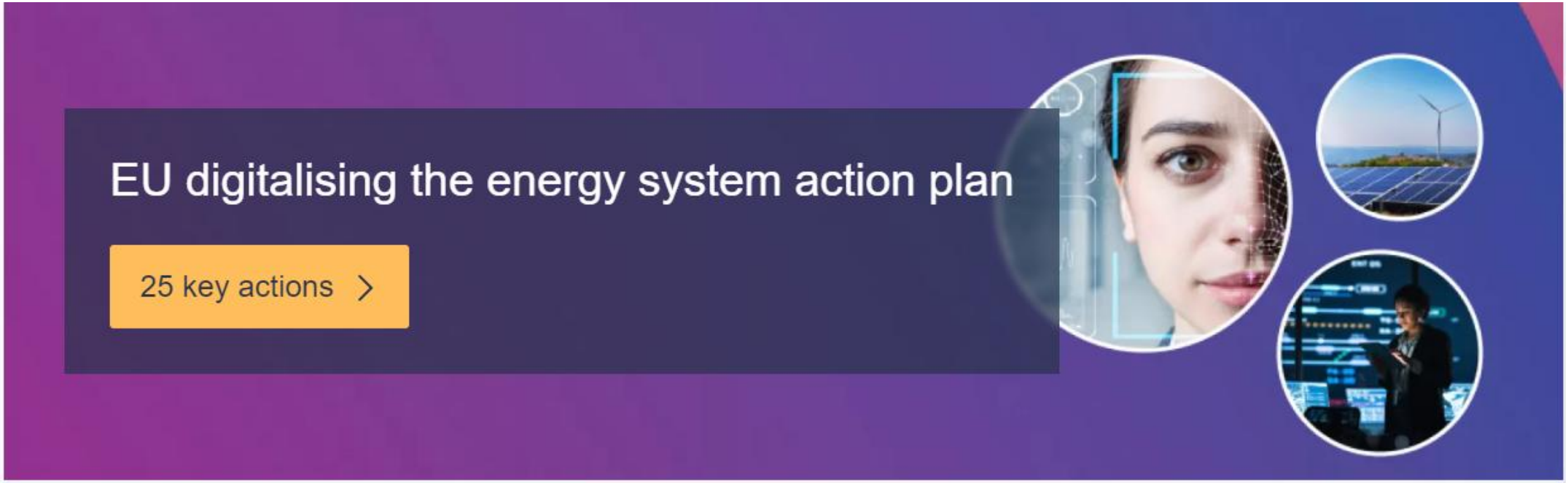
All relevant Competent Authorities have received the proposal for the Risk Assessment Methodologies. The last proposal submission was reported on 14 July. The Commission stresses the importance of all Competent Authorities deciding as soon as possible on those methodologies so that they can be used for the next steps

Smart Energy Expert Group (SEEG)

Status update

The Smart Energy Expert Group (SEEG) 1/2

The creation of the Smart Energy Expert Group (SEEG) was outlined in the Digitalisation action plan and it was formally established by Decision C/2023/6121, adopted on 18 September 2023.



©iStock_metamorworks/AdobeStock_Gorodenkoff/AbobeStock_Ovelyday12

The Smart Energy Expert Group (SEEG) 2/2

- The Smart Energy Expert Group replaces the Smart Grids Task Force.
- It will advise the Commission on initiatives and actions to coordinate and accelerate the digital and sustainable transformation of the EU's energy system, namely on the development and deployment of smart energy solutions, cybersecurity and consumers empowerment and protection.
- The Commission has established 3 subgroups under the SEEG to cover:
  - Data for Energy (D4E)
  - Consumer Empowerment and Protection
  - Cybersecurity

Smart Energy Expert Group (SEEG)

Work programme. Topics for research:

1. Recommendations to address cybersecurity risks in Photovoltaic
2. Continuation of previous SGTF EG2 work on existing EU legislation and standards in the energy sector
3. Requirements of a reference architecture for energy grids
4. Cybersecurity Information Exchange in the European Energy Sector

Preparative Study for the development of a Delegated Act/Policy Initiatives on Gas, Hydrogen and Oil Cybersecurity

Status update

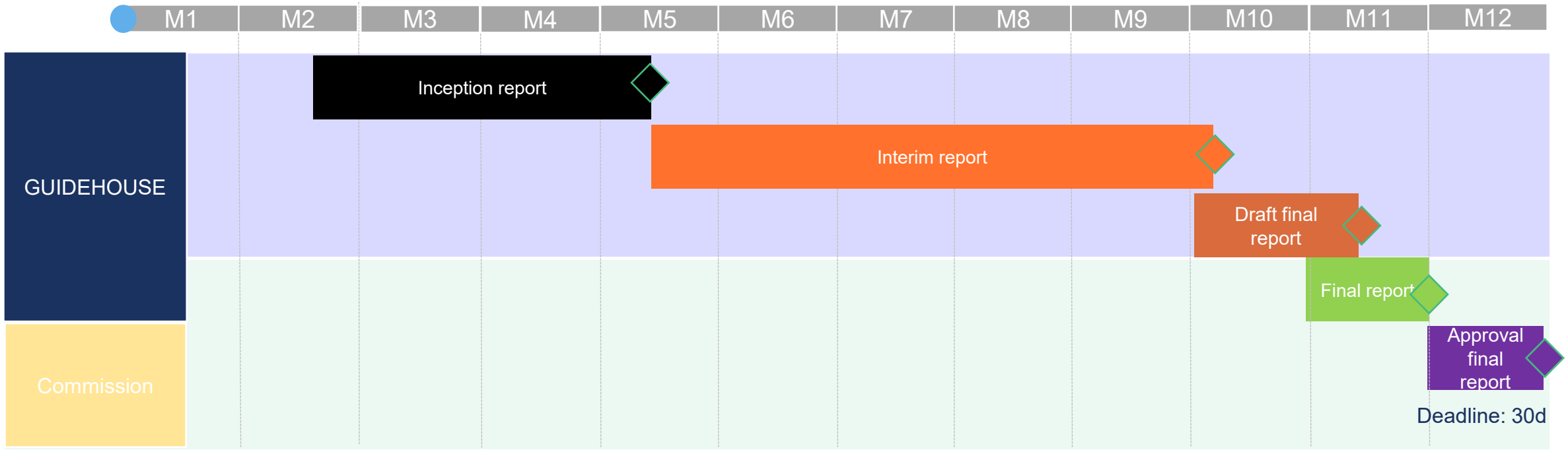
Background and objectives

The mandate requires an upfront analysis of possible needs, objectives and impacts.

Objective of the study:

- risk assessment of cyber threats in the gas, hydrogen and oil sectors: identification of existing regulatory gaps, analysis of needs to mitigate these risks, estimation of implementation resources and operational costs of respective measures to address those risks
- common understanding of cyber risks in these energy sub-sectors and regulatory measures to address them
- Inputs for the discussion with Member States, National Regulatory Authorities, National Competent Authorities, and stakeholders on additional policy actions in the area of cybersecurity in the gas, hydrogen and oil sector

Next steps



- Inception report
- Interim report
- Draft final report
- Final report
- Approved Final report

Review energy security framework

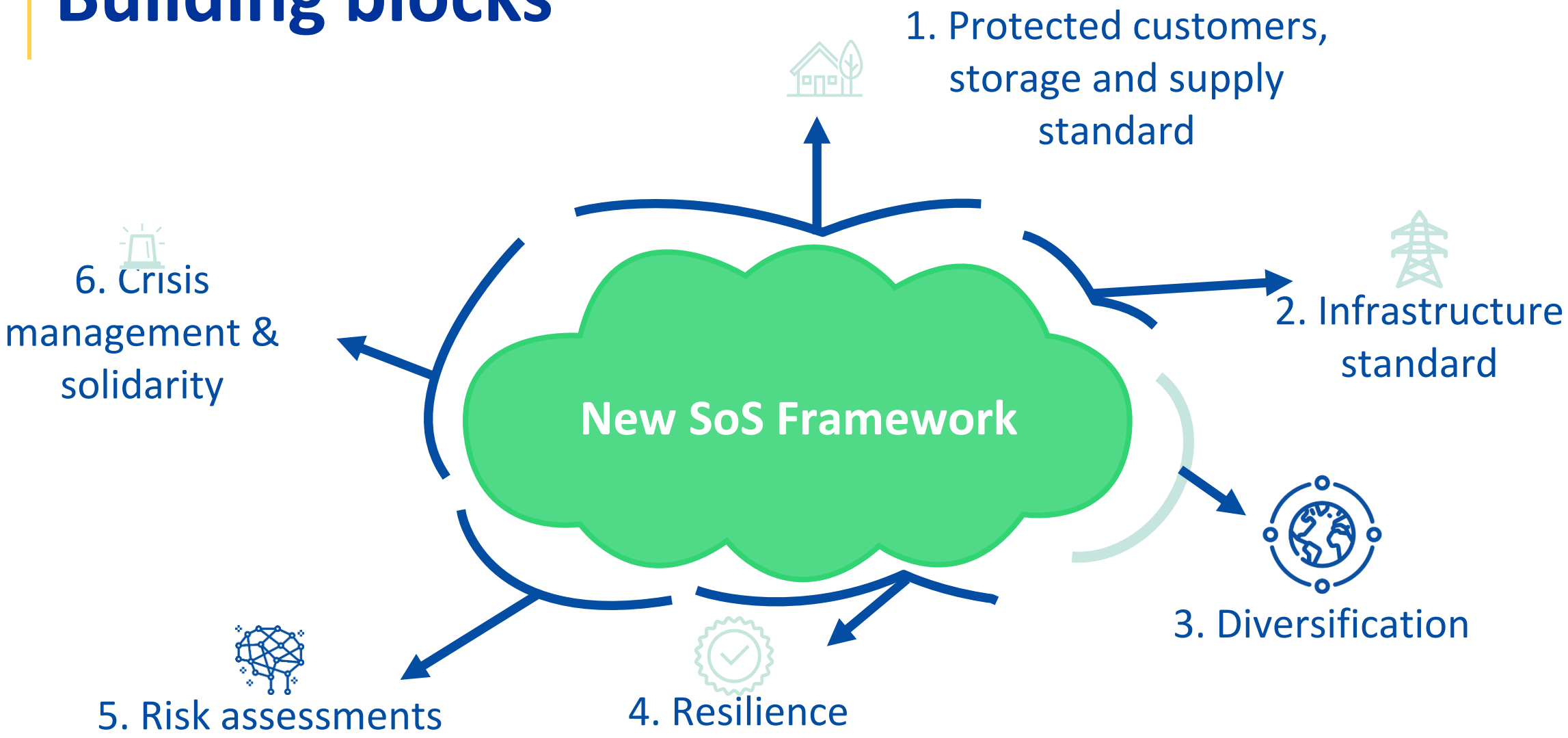
Status update

Why a revision?

Main reasons to act: emerging challenges and weaknesses

- → Competitiveness
- → Cumbersome framework
- → Lack of cross-sector interaction
- → Limited cross-border cooperation
- → A changing energy system
- → Climate change adaptation
- → New threats (cyber and physical)
- → Dependencies and geopolitical turbulences

Building blocks



Timeline

Sep-Nov 2024

Fitness check - Public consultation

Call for evidence for legislative proposal

Sept - Oct 2025

29 Sept 2025

Stakeholder workshop

We are here.

Joint ECG-GCG on the revision

9 Oct 2025

Oct 2025

End of consultant's study

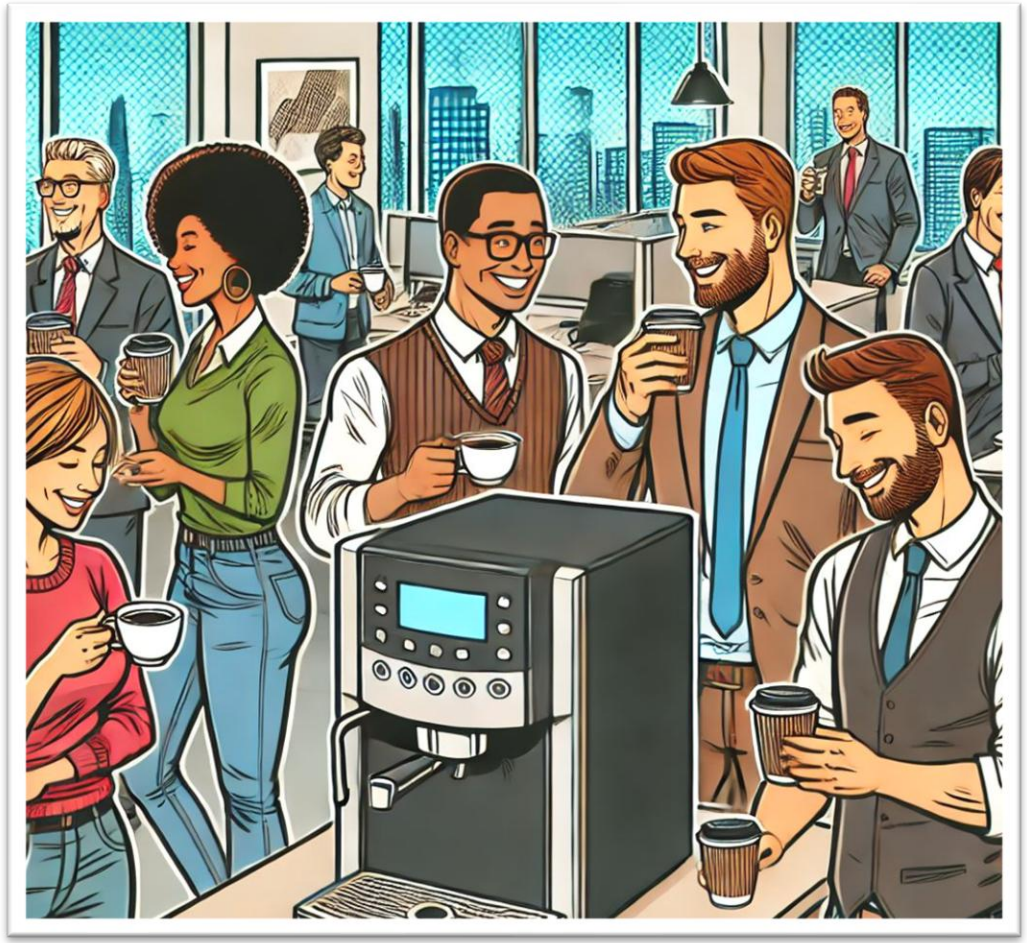
Adoption of the legislative proposal

1st half 2026

Fill in copyright information.

Thank you

7. Short break



8. Cyber/physical legislation interplay

Sebastian Contreras
National Gas | Policy Manager

Slides to come

9. NIS2 Adoption Experiences From DESFA

Apostolia Angeleri
DESFA

NIS2 Directive: DESFA's response and initial actions

*Following the adoption of the NIS2 Directive at the EU level, DESFA promptly took action to **assess its impact** and align internal cybersecurity practices with the new requirements. The Company has demonstrated a **proactive commitment** to meeting both European and national regulatory obligations.*

Initial notification to NCSA: in line with the instruction from the Greek National Cybersecurity Authority (NCSA), DESFA submitted the required information (including CISO contact details, public IP ranges, and registered domains) to register.ncsa@cyber.gov.gr.

Greek Legal Transposition (Law 5160/2024 & Joint Ministerial Decision 1689/2025): the Directive was transposed into Greek law with specific cybersecurity obligations for essential and important entities. Despite the increased specificity and stringency of the requirements, DESFA already maintains a strong cybersecurity maturity.

Early Gap Analysis: DESFA conducted a comprehensive gap analysis against the NIS2 requirements to identify improvement areas, and relative initiatives.

Greek NCSA Launches new Compliance Assessment Tool

*The National Cybersecurity Authority of Greece (NCSA) has introduced a **comprehensive compliance assessment tool** for all essential and important entities that fall under Law 5160/2024, implementing the new national cybersecurity legislative framework.*

Development: Developed with the support of ENISA and the "Support Action" initiative, this tool helps essential and important entities perform gap analyses and meet evolving regulatory obligations.

Tool Structure: Features 169 control points organized into 24 thematic areas—covering all legal, technical, and organizational requirements of Law 5160/2024 and supporting ministerial decisions (1689/2025 & 1899/2025).

Key Capabilities:

- Compliance Evaluation: Assess alignment with cybersecurity legal obligations.
- Risk Identification: Highlight gaps and security risks.
- Maturity Assessment: Evaluate the effectiveness of cybersecurity measures.
- Guidance for Improvement: Support planning and implementation of improvement opportunities for further compliance.

*Additionally, **Ministerial Decision 1899/2025** establishes the qualifications, duties, incompatibilities and obligations for the Chief Information Security Officer (CISO) - ensuring that every covered entity designates a qualified CISO with clear authority and accountability.*

ISMS Implementation & NIS2 Alignment

*The implementation of the **Information Security Management System** (ISMS), according to the **ISO/IEC 27001:2022 standard**, served as the foundation for **NIS2 compliance**, enabling a structured and risk-based approach to cybersecurity across critical domains:*

- **Risk-Based Foundation**: the ISMS introduced a structured risk assessment methodology, aligning naturally with NIS2 focus on proportionality and asset protection.
- **Policy and Operating Instructions Framework**: Operating Instructions developed under the ISMS directly supported NIS2 requirements across areas such as incident handling, asset management, and disaster recovery.
- **Governance & Ownership**: the ISMS helped clarify roles and responsibilities for security-related processes, strengthening accountability as required by the NIS2 Directive.
- **Audit-Driven Maturity**: the ISO audit process fostered a culture of continuous improvement, reinforcing NIS2 principles on effectiveness review and gap closure.
- **Tool-enabled enforcement**: technologies like ServiceNow, Microsoft Defender, Active Directory, and SIEM platforms were embedded within ISMS controls to meet NIS2 expectations.

DESFA Cybersecurity Posture according to NIS2 Directive

*The Company has reached a **strong level of cybersecurity maturity**, with structured controls in place across all key NIS2 areas. The ISMS implementation and ISO/IEC 27001:2022 certification achievement have led to well-defined policies, operating instructions, and technical safeguards in every critical domain:*

- **Risk Analysis & Information System Security**: a wide range of Operating Instructions has been established and aligned with ISO requirements, supporting a robust risk-based security framework.
- **Incident Handling:** Event & Incident Management Operating Instructions, supported by SOC monitoring and SIEM capabilities, ensure a systematic and timely response to cybersecurity events.
- **Business Continuity:** Disaster Recovery and Backup Procedures are defined, and Business Continuity Plans have been implemented for key operational units.
- **Supply Chain Security:** comprehensive controls are enforced through tender procedures, contractual clauses, and cybersecurity checklists.
- **Secure System Development**: security is embedded into the development lifecycle with documented technology requirements.
- **Effectiveness of Risk Measures**: a formal methodology and supporting documentation are in place to continuously assess and improve the effectiveness of cybersecurity controls.
- **Cyber Hygiene**: strong technical hygiene practices are enforced, including regular backups, endpoint protection, firewall configuration, password policies, and patch management.
- **Cryptography & Encryption**: encryption is enforced on a wide range of IT assets. Cryptography policies have been defined.
- **Access Control & Asset Management**: Access and asset management are formalized and supported by enterprise-grade tools like Active Directory, MFA, VPN, and ServiceNow, ensuring secure and controlled operations.
- **Multi-Factor Authentication & Secure Communication:** MFA and conditional access are enforced, supporting secure access and communication practices.

Insights from NIS2 Implementation

*The implementation of the NIS2 framework provided **valuable insights** into our existing cybersecurity practices. While the overall maturity level is high, the compliance journey revealed specific areas that could benefit from further refinement. The prioritization of **targeted improvement actions** contributed to the continuous enhancement of our security posture.*

- **Vulnerability & Patch Management**: the NIS2 highlighted the need to formalize and consolidate vulnerability handling and patching procedures into a dedicated Operating Instructions. Existing practices were embedded within other documents, requiring process visibility.

- **Supply Chain Risk Management**: the review of contractual clauses showed the need to define more specific obligations for third-party management to align with NIS2 expectations.

- **Incident Response:** while high-level guidelines exist, NIS2 compliance expedited already planned initiatives like detailed incident playbooks, including clearer roles, escalation paths, and coordination across technical and business teams.

10. Drill Down on Secure remote access to Industrial Control Systems (TSO Experience)

Fabrizio Zucca
Snam

11. CCB updates from Beligium's National Cybersecurity Certification Authority

Johan Klykens – Director of the NCCA (CCB)

12. Wrap-up and goodbye

Douglas Walker Hill
Interoperability & Data Exchange Adviser
ENTSOG

Thank you for your attention & being an active part of this event, see you in 2026!

Douglas Walker Hill, Interoperability & Data Exchange Adviser

douglas.hill@entsog.eu

ENTSOG - European Network of Transmission System Operators for Gas

Avenue de Cortenbergh 100, 1000 Bruxelles

www.entsog.eu | info@entsog.eu