Council of the European Union
General Secretariat

Brussels, 20 June 2025

DOCUMENT PARTIALLY ACCESSIBLE TO THE PUBLIC (17.07.2025)

WK 8361/2025 INIT

LIMITE

CYBER

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

WORKING DOCUMENT

From:	Presidency
To:	Delegations
Subject:	Cyber Solidarity Act: state of play - Presentation by ENISA

Delegations may find in annex the presentation given at the meeting of the Horizontal Working Party on Cyber Issues on 20 June 2025.

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

PUBLIC

SUPPORT ACTION AND THE TRANSITION TO THE CYBERSECURITY RESERVE

20 | 06 | 2025

Support Action

Transition to EU Cybersecurity Reserve

Fully evolved EU Cybersecurity Reserve

ENISA CYBERSECURITY SUPPORT ACTION

ENISA CYBERSECURITY SUPPORT ACTION

ENISA PROVIDES EX-ANTE AND EX-POST SERVICES TO INCREASE MEMBER STATES' ABILITY TO PREVENT AND RESPOND TO LARGE-SCALE CYBERATTACKS.

WHO BENEFITS? Member States' NIS2 Directive entities

PROVIDED SERVICES

Ex-post services

- incident management
- incident response
- incident coordination

Ex-ante services

- cybersecurity exercises
- cybersecurity training
- capability assessments such as infrastructure and capabilities testing

Assistance with

- threat assessments such as risk monitoring or the creation of a threat landscape and risk scenarios

Assistance with

- crisis communications

BENEFITS

- To increase your cybersecurity prevention and detection capacities
- To support your capabilities to respond to cyber threats and incidents
- To strengthen your cybersecurity situational awareness
- To build up your cyber preparedness
- To assist with your cyber capabilities' assessment

FOR WHOM?

Essential and important entities of sectors listed in NIS2 Directive

Critical entities as per critical entities resilience (CER) Directive

Highly critical sectors

- Energy
- Transport
- Banking
- Financial market infrastructure
- Health
- Drinking water
- Waste water
- Digital infrastructure
- ICT services management (B2B)
- Public administration
- Space

Other critical sectors

- Postal and courier services
- Waste management
- Manufacture, production and distribution of chemicals
- Production, processing and distribution of food
- Manufacturing
- Digital providers
- Research
- Any additional services listed by MS in national transposition measures

SERVICES OFFERED

Ex-post

Respond

Incident Response

- Information Security Incident Analysis
- Artefact and Forensic Evidence Analysis
- Cybersecurity Incident Response
- Cybersecurity Incident Coordination
- Cybersecurity Incident Recovery
- Incident-Handling Capability Development
- Incident Response Playbooks

Ex-ante

Prepare / Prevent

Capacity

- Trainings
- Exercises

Testing

- Penetration testing
- Vulnerability assessment
- Threat hunting

Threat Landscape

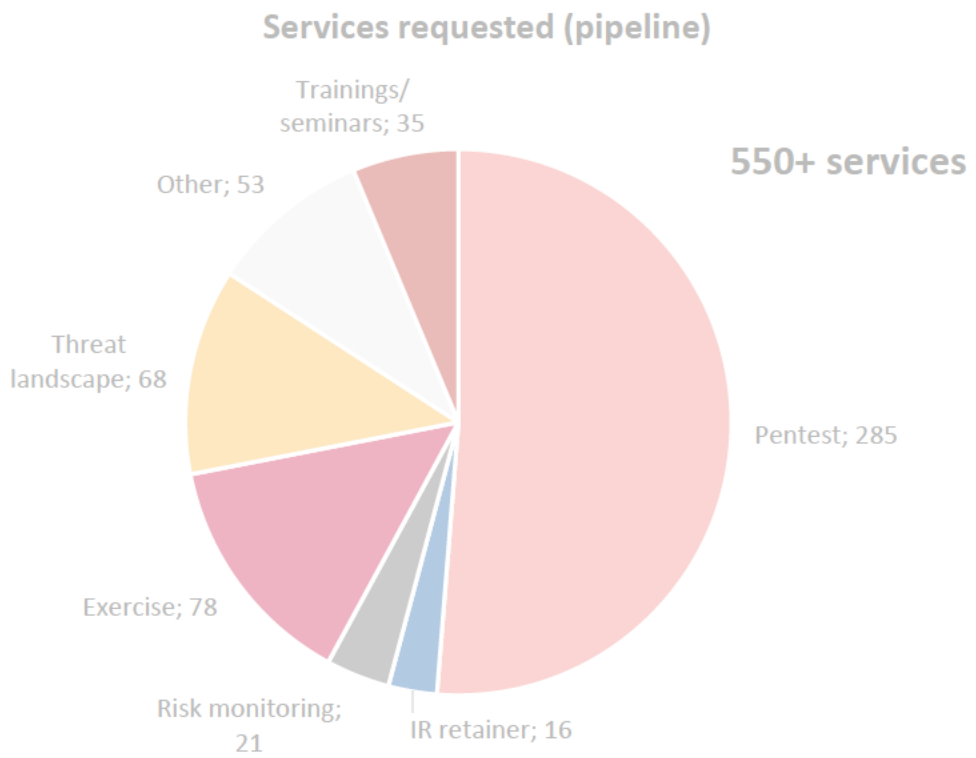
- Threat landscape
- Risk scenarios

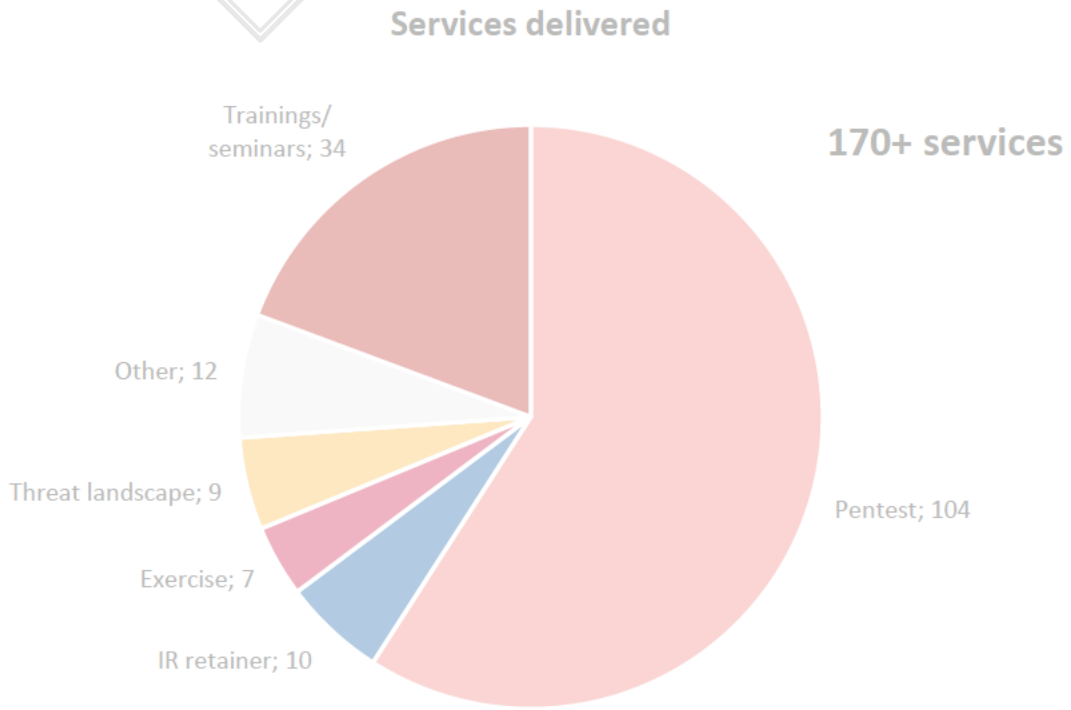
Other

- Risk monitoring
- Crisis management plan
- Maturity assessment
- NIS2 compliance
- Risk assessment

SERVICE DELIVERY UPDATE

PUBLIC



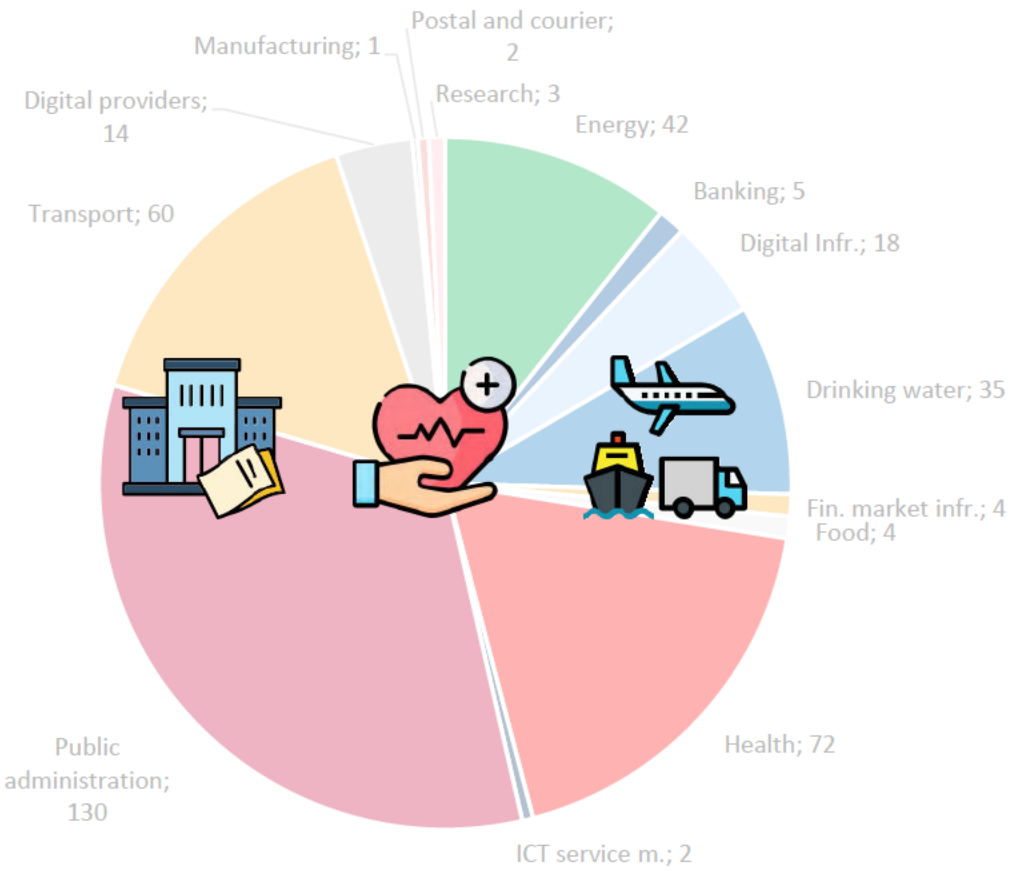


Important increase in the volume of service delivery expected as of now as work is starting with the new contractors

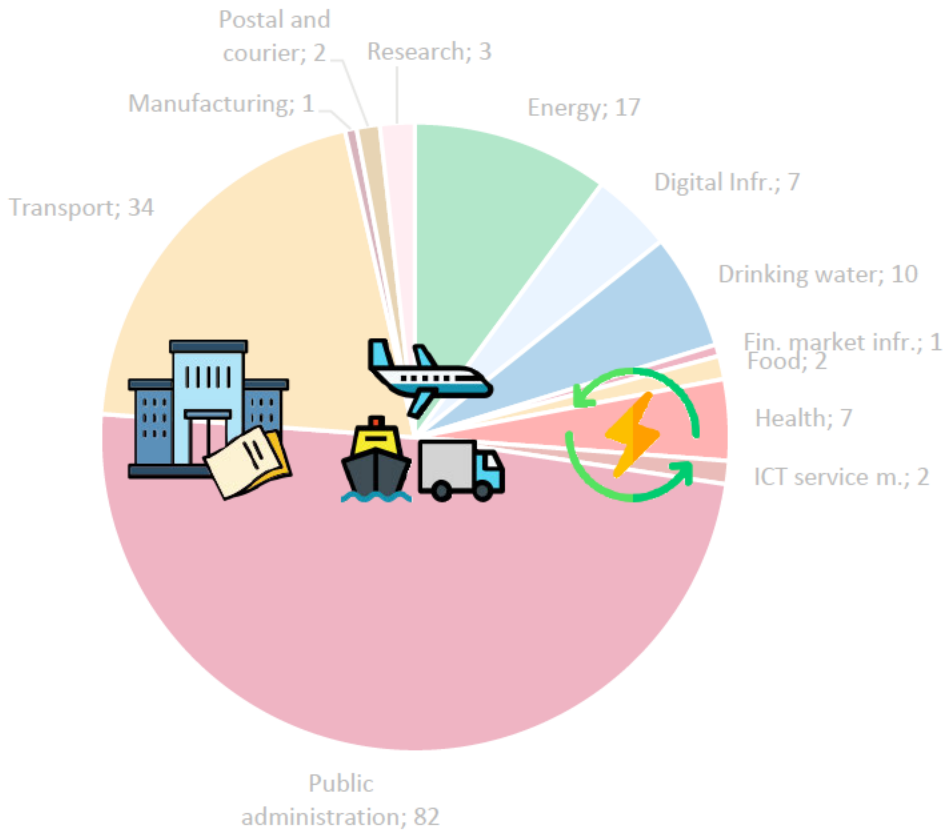
SERVICE DELIVERY UPDATE
SPLIT PER SECTOR

PUBLIC

Services requested (pipeline) – split per sector



Services delivered – split per sector




PUBLIC

PARTIES INVOLVED

MEMBER STATE (MS)

- Point of contact (PoC): liaison between ENISA and beneficiaries; assessing national needs; defining pipeline of services
- Beneficiaries: direct addressees of support services

ENISA

- Ensuring timely and efficient service provision
- Service manager for MS: contact with PoC; advise on available services; support for requests submission
- Governance

SERVICE SUPPORT PROVIDER

- Provides support as per tender requirements: technical support to ENISA
- Scoping of services: in agreement with ENISA, PoC and beneficiaries
- Provision of deliverables: responsible in front of ENISA

EUROPEAN COMMISSION (DG CNECT)

- Consultation: for borderline requests potentially falling outside of scope
- Reporting: ENISA provides regular and ad-hoc reports to the Commission

SUPPORTING PARTNERS VIA PUBLIC TENDER (2024)

- Support ENISA in the delivery of the services
- Public tender procurement
- 27 lots + 1 pan-EU lot
- Framework contract for 3 years with cascade
- **DEP Art 12.5 – OCA Requirements**

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

Ref. Ares(2024)6224838 - 03/09/2024

OPEN CALL FOR TENDERS

*concludes with **Framework service contracts in cascade***

Tender Documentation

Supporting ENISA for the provision of cybersecurity services to European Union Member States

ENISA F-OCU-24-T10

LOTs 1 – 27

SUPPORT ACTION BUDGET

- Current budget envelop over 2024-2026 – Contribution Agreement 2023
  - **Per Member State: 525.926 EUR over the three years**
  - Pan-EU lot: 890.000 EUR over the three years
- New Contribution Agreement(s) follow the Cybersecurity Reserve model
- Current status
  - **Some MS have (almost) exhausted their assigned budget**
  - Some MS have used little/no budget
  - Budget consumption in some cases stalled because of new procurement / OCA
  - New Contribution agreement for the period of 2025-2027 under preparation (possible signature July 2025)

Support Action

Transition to EU Cybersecurity Reserve

Fully evolved EU Cybersecurity Reserve

TRANSITION TO THE CYBERSECURITY RESERVE

CSOA - CYBERSECURITY EMERGENCY MECHANISM

Cybersecurity Emergency Mechanism

Preparedness Actions:
- **Coordinated preparedness testing** of NIS2 entities (e.g. pen-testing, threat assessment)
- **Other preparedness actions** for NIS2 entities (e.g. vulnerability monitoring, risk monitoring, exercises and training

EU Cybersecurity Reserve:
- **Trusted providers / MSSPs**
- **Response services**
- Unused pre-committed services **convertible into preparedness services** related to incident prevention and response

Mutual Assistance

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

WHO

Stakeholders list	
Who can request services?	• **NIS2 SPOC*** • CERT-EU • DEP-associated third country SPOC
Who are the users of the Reserve?	• **MS crisis management authorities*** • **MS CSIRTs*** • CERT-EU • Competent authorities of DEP-associated third countries

*** The CSoA is very explicit in terms of the Cybersecurity Reserve governance and the current composition of the PoC network does not necessarily involve the appropriate MS representatives**

Question: How should we approach the restructuring of the PoC group? Should MS appoint representatives from the SPOC designated under NIS2?

CYSIG: WHAT?

An informal stakeholders' group that gathers trusted managed security services providers (MSSPs) in the EU that will support ENISA in delivering cybersecurity services to the EU Member States.

Core tasks of the group:

- Supporting ENISA in providing cybersecurity services to the EU Member States under the umbrella of the Support Action;
- Contribution to the Support Action Assessment Framework;
- Contribution in turning to operational the EU Cybersecurity Reserve by ENISA;
- Input to market analysis of cybersecurity services within the EU, including the mapping of services needed by the EU Cybersecurity Reserve.

CYSIG: WHO?

Companies were selected based on their participation in the call for tenders 'Supporting ENISA for the provision of cybersecurity services to European Union Member States'. In fact, 2024 call for tenders' winners (in cascading system) were invited. 41 external participants on-site!

List of companies that were represented:

- CSA
- CENTRO REGIONAL DE SERVICIOS AVANZADOS, S.A.
- ITSec Area Kft.
- Balasys IT Zrt
- Ukatemi Technologies Plc.
- GMV
- Andrews IT Engineering Ltd.
- Alverad Technology Focus Ltd.
- NRD Cyber Security
- IstroSec s.r.o.
- NVISO
- Infigo IS
- Airbus Protect
- CybrOps
- UniSystems Luxembourg Sàrl
- Tet
- S2 Grupo Cybersecurity
- certSIGN S.A.
- UNI SYSTEMS S.M.S.A
- Span d.d.
- Uni Systems Luxembourg Sarl
- Bit Sentinel
- Adacom
- CybExer

PAN-EU TESTING

CYBER EUROPE

Alignment with Cyber Europe 2026's mission

Three levels of engagement, offering increasing MS involvement

1. **No SPoC involvement/ENISA simulation**: ENISA will just stress-test the local support (contractor's skills/capabilities/reaction times).
   - All interactions with MS (e.g. SPoC request, beneficiary/victim) are simulated
   - Threshold for activation is assumed crossed (Art 15.2)
2. **SPoC involvement**: In addition to the above we also test the communication with the SPoC (request, follow-up interactions)
   - TODO agree on objectives per MS (e.g. reaction time KPIs)
   - MS will test procedure and criteria of activation (Art 15.2)
3. **Full involvement**: We allow your players to initiate the whole chain of actions
   - Highest gains but also most likely option to fail

WORK TO BE DONE (IN PROGRESS) IN 2025!

- CSoA – Cybersecurity Reserve introduce **substantial changes**
- 2025 should be viewed as a **transition year**
- Cybersecurity Reserve introduces changes in **scope of services** as well as **stakeholders** involved
- NIS CG, CSIRTs Network and EU-CyCLONe have roles in the Cybersecurity Reserve
- (At least) biennial **mapping of required services** and **assessment of availability** of services in the EU (on- going; Sept-Dec)
  - Collaboration with industry (CyCIG)
- Detailed Services catalogue and descriptions (delivered – living doc)
- IR Retainer conversion SOP to ex ante services (proposal developed – agreed)
- Participation in Cyber Europe 2026 (ongoing)
- New tenders for EUIBAs (CERT EU), Moldova and Ukraine, DEP associated 3rd countries (Q3 2025), EEA/EFTA (2026)

THANK YOU FOR YOUR ATTENTION

European Union Agency for Cybersecurity
Vasilissis Sofias Str 1, Maroussi 151 24
Attiki, Greece

- +30 28 14 40 9711
- info@enisa.europa.eu
- www.enisa.europa.eu