Cybersecurity

The Cybersecurity DSI is established to enable Europe to make full use of its collective capabilities to improve cybersecurity through timely and effective collaboration between the Member States.

It contributes to the EU preparedness to deal with cyber threats by facilitating the implementation of the EU Cybersecurity strategy. The funding increases the cybersecurity capabilities and the cooperation of key European cybersecurity players, in particular, but not only, those addressed by the Directive on security of network and information systems ("NIS Directive", 2016/1148), the Cybersecurity Act (Regulation (EU) 2019/881) and the Commission Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises ("Cyber Blueprint" C(2017) 6100)

These are operators of essential services (OESs), national cybersecurity authorities, Computer Security Incident Response Teams (CSIRTs), as well as cybersecurity certification stakeholders.

As a result of the funding received, OESs are boosting their own internal cybersecurity capabilities and engage with relevant Information Sharing and Analysis Centres (ISAC) involving industry peers and public authorities. National bodies mainly focus on the take-up of the obligations deriving by European legislation. For example, they exchange best practices, train their staff and set-up incident reporting mechanisms. CSIRTs are expanding their capacities to run cybersecurity services and to co-operate across borders. Such cooperation is further facilitated by MeliCERTes, a platform set up by the European Commission with a common set of tools for information sharing and maturity development for CSIRTs. Projects funded also support trans-national cooperation and the roll-out of Cybersecurity certification schemes in the EU.

LEARN MORE

Highlights

Generic Services Projects

€43.2 million
98 projects in **27** countries (26 Member States + Norway)

More info on the Generic Services:

HaDEA

Deployment

26 Member States are involved with a given area of the EU Cybersecurity Strategy.

GSP funding has contributed to the increased cybersecurity capabilities of **35 operators of essential services (OES)** across sectors of energy, health, finance, transport and water supply.

CSIRTs have engaged in cooperation projects for the EUs joint cybersecurity preparedness and shared situational awareness

Indicators

As the CEF funding of the Core Service platform came to an end in Q4 2022, this is the cut off date for activities linked to this work strand. Activities linked to certification are still ongoing until 2024. The monitoring of the Generic Services projects presents the state of play by Q4 2022. 42 Generic Services projects are still under implementation and are foreseen to be completed by 2024.

Uptake

26
Member States in a given area of the EU Cybersecurity Strategy and that are financed as GSP*

Service Availability

100%
Average uptime of the central node of the Cybersecurity MeliCERTes facility

Financial Monitoring

€ 11,847,845
CEF Core Service Platform funding

€ 43,212,848
CEF funding through Generic Services Projects

CEF Building Blocks reused by Cybersecurity

Cybersecurity is not reusing any Building Blocks

** Generic Services Projects*

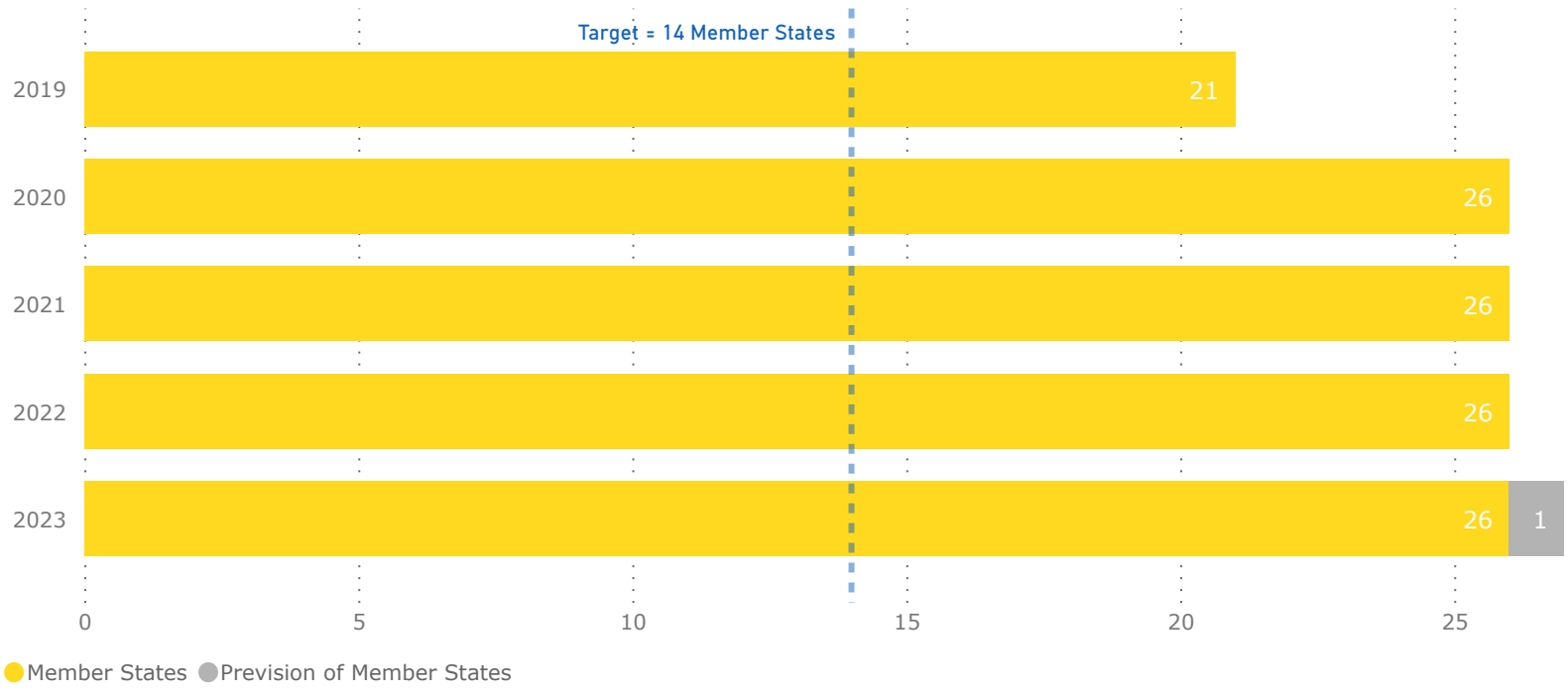
Indicators

Cybersecurity > Uptake > Member States in a given area of the EU Cybersecurity Strategy and that are financed as Generic Services Projects

This indicator measures the **number of Member States** in a given area of the EU Cybersecurity Strategy and that are financed as Generic Services Projects at the time of yearly data collection.

Target

14 Member States in a given area of the EU Cybersecurity Strategy and that are financed as Generic Services Projects.

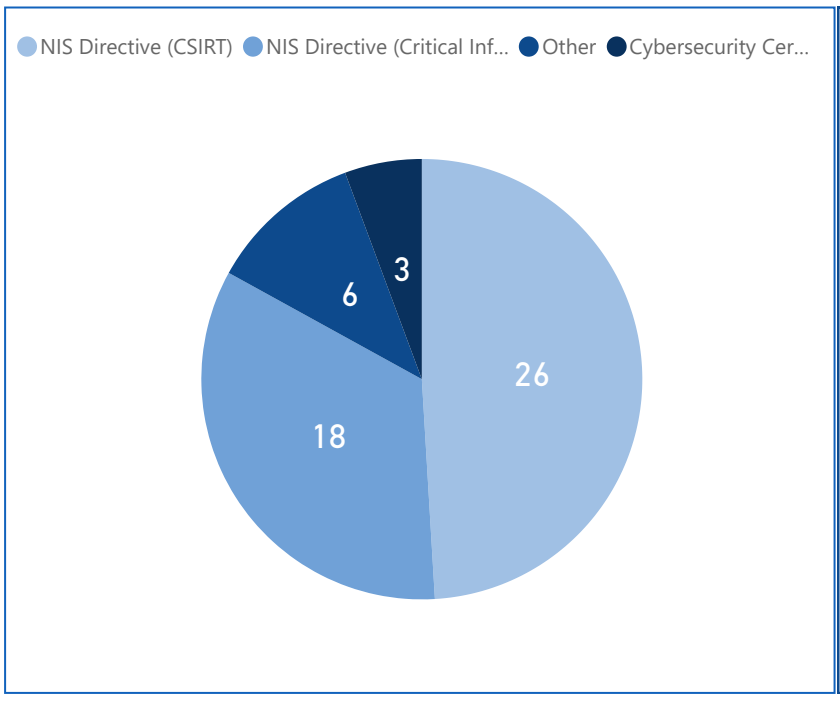


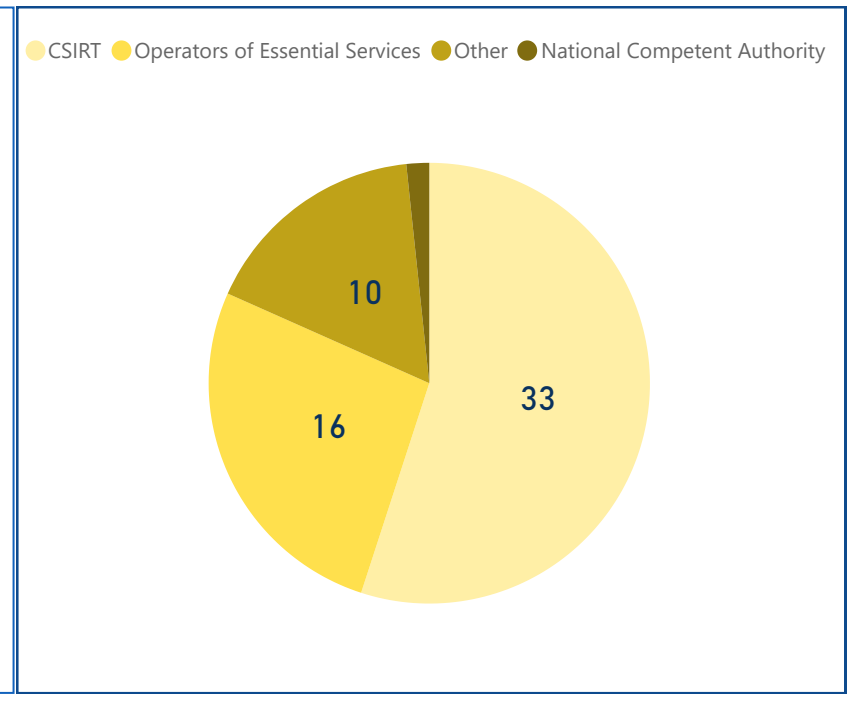
1 additional Member State is expected to be be in a given area of the EU Cybersecurity Strategy and that are financed as Generic Services Projects by 2024.

This subindicator measures the **distribution of projects according to the (i) Type of beneficiary and (ii) Area of Cybersecurity Strategy** at the time of yearly data collection.

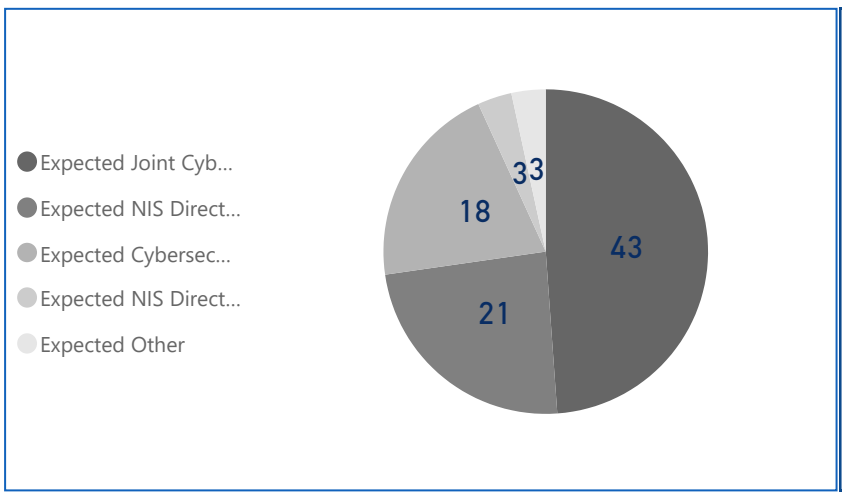
The areas of the cybersecurity strategy (see figure on the left) considered are: NIS Directive (CSIRTs); NIS Directive (Critical Infrastructures); Cybersecurity Certification; Joint Cybersecurity Capabilities; Other

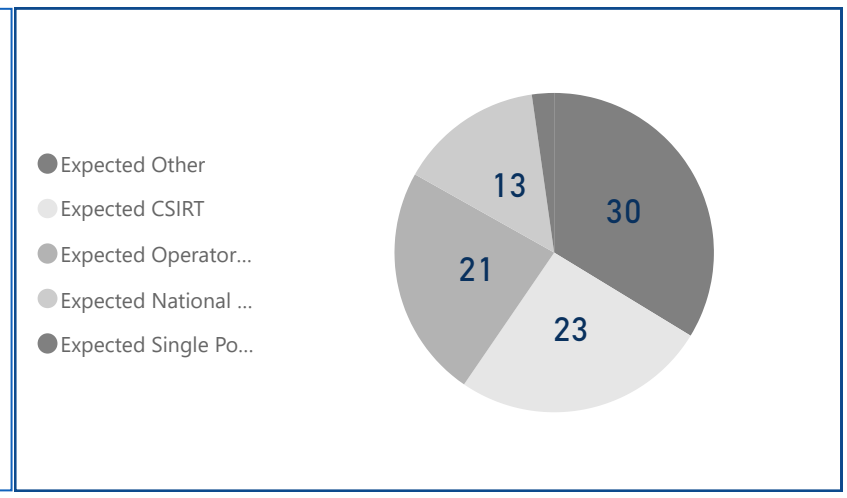
The types of beneficiary (see figure on the right) considered are: CSIRTs; National Competent Authority; Operators of Essential Services; Single Point of Contact; Other





The 42 ongoing CEF Generic Services Projects are expected to produce the following additional type of beneficiary and area of Cybersecurity Strategy by 2024.





Cybersecurity Milestones

All the **Cybersecurity** milestones defined within the CEF Monitoring framework were successfully achieved.
A detailed overview of the milestones can be found in the table below.

Milestone title	Start date	End date	% complete	Status
1.Implementation of CSP common services general requirements*	07 November 2016	31 December 2022	100	Completed
2.CSP deployment, operation and support*	20 January 2017	31 December 2022	100	Completed
3.Trust building for the use of CSP*	10 January 2017	31 December 2022	100	Completed
4.Successful development of the CSP and its general requirements, including documentation*	02 May 2017	31 December 2022	100	Completed

**The Cybersecurity DSI is composed of three strands: MeliCERTes, ISACs FM and Certification. The work reported here is mainly on MeliCERTes and ISACs, completed and operational. Regarding Certification, it is expected to be completed in 2024.*