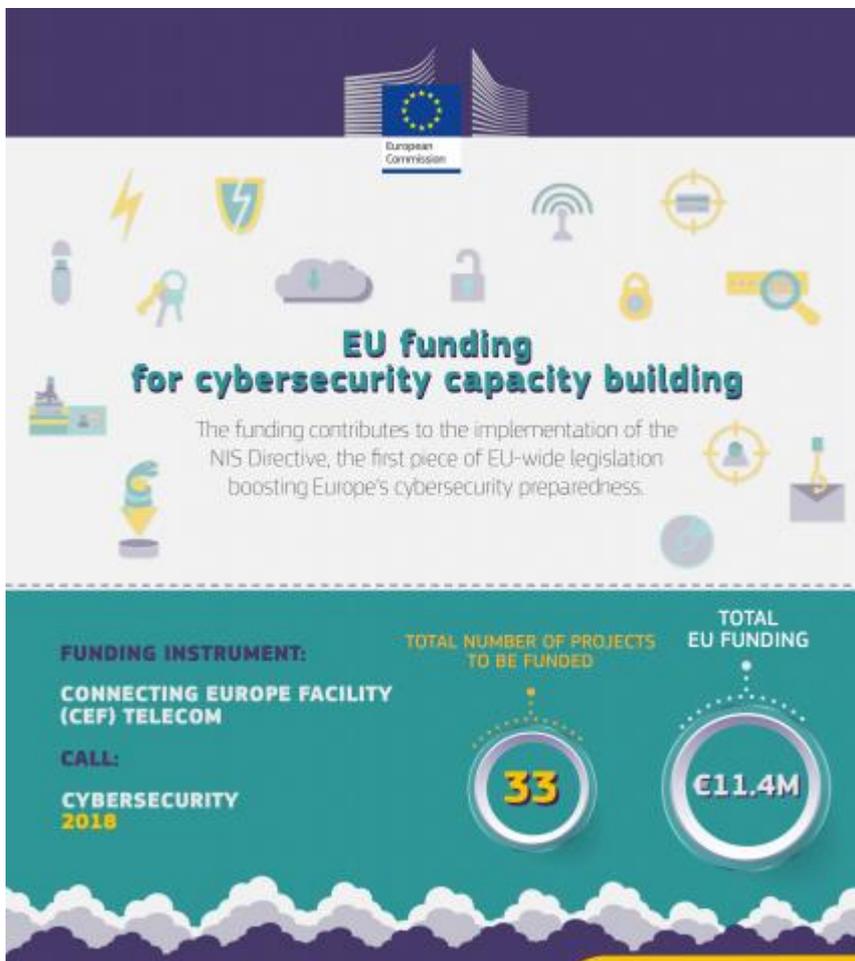


33 new EU funded projects to assist EU Member States in building up their cybersecurity capabilities

The European Union invests through the Connecting Europe Facility (CEF) programme €11.4 million (EU contribution) in projects which seek to strengthen the European Union's capacity and deal more efficiently with cyber-threats and incidents. It is the first time that EU is providing financial support under the CEF programme to broader categories of stakeholders which nevertheless are crucial for enhanced cybersecurity at national level.



European Commission

CEF Cybersecurity call

Operators of Essential Services (OES) such as electricity and gas companies, airports, water distribution providers and National Competent Authorities (NCAs) for cybersecurity are among the selected beneficiaries to receive funding by the Connecting Europe Facility cybersecurity call 2018. In addition, support has been provided for the build-up of cybersecurity capabilities in relation to Cooperative Connected and Automated Mobility (CCAM) .

In particular, EU has selected to grant:

- €7.5 million funding to Computer Security Incident Response Teams (CSIRTs)
- €3 million funding to Operators of Essential Services (OES)
- €0.2 million funding to National Competent Authorities (NCAs)

The beneficiaries have been selected to be funded by the EU in order to develop or acquire the necessary tools and skills to comply with the requirements set by the NIS Directive and to cooperate effectively at EU level. For example, some projects will set-up Security Operations Centres (SOCs), others are also developing the skills of their personnel, and some others are adapting tools for reporting cyber incidents at the European level. Projects in the area of CCAM, instead, are looking at integrating cybersecurity requirements in the deployment of related technologies and infrastructure in Europe.

The related grant agreements are foreseen to be signed by Q3 2019 and the new projects are expected to start before the end of the year.

Some other interesting facts about this call

- Most of the OES belong to the energy sector, reflecting the increasing digitalization of the sector and its attention to cybersecurity
- For the first time CSIRTs from Slovakia and Bulgaria are receiving funding through CEF
- One project setting-up a pan-European Information Sharing and Analysis Center (ISAC) in the digital infrastructure sector

You may find some additional interesting facts and numbers by checking the infographic presenting the outcome of this call.

Background information

Through the CEF Cybersecurity calls EU seeks to support the EU Member States in putting the NIS Directive's legal provisions into practice.

Since 2016, the EU has been providing support for improving the operations and capabilities of CSIRTs in EU Member States. Between 2016 and 2017 the European Commission has awarded €18 million funding - mainly to CSIRTs - to 19 EU Member States. CSIRTs are teams that provide support services to handle cybersecurity threats and incidents for their stakeholders, known as constituents in the public sector, operators of essential services, critical infrastructure entities and digital service providers.

In parallel, the European Commission has set up a platform that gives national CSIRTs concrete means to share information and to cooperate operationally EU wide to fight against cyber-attacks or mitigate cyber threats.

EU will continue investing in strengthening cybersecurity through CEF. In July 2019, a new CEF cybersecurity call of €10 million (CEF-TC-2019-2) will open.

Downloads

Infographic: 2018 CEF Telecom Cybersecurity call results
[Download](#)

Related topics

Connecting Europe Facility
Cybersecurity
Improving connectivity and access
Strengthening trust and security

Related content

€10 million EU funding available for projects stepping up EU's cybersecurity capabilities and cross border cooperation

Call for proposals | 04 July 2019

The latest Connecting Europe Facility (CEF) cybersecurity call offers funding opportunities to key

stakeholders identified by the NIS Directive such as European Computer Security Incident Response Teams (CSIRTs), operators of essential services (e.g. banks, hospitals, electricity and gas providers, railways, airlines, domain name providers, etc.) and various public authorities. For the first time European cybersecurity certifications authorities are also eligible to apply for this programme in order to allow them seize the EU Cybersecurity Act.

Source URL:

<https://digital-strategy.ec.europa.eu/news/33-new-eu-funded-projects-assist-eu-member-states-building-their-cybersecurity-capabilities>