

The EU Cybersecurity Act

The Cybersecurity Act strengthens the EU Agency for cybersecurity (ENISA) and establishes a cybersecurity certification framework for products and services.



© iStock by Getty Images -1037348986 Urupong

A new mandate for ENISA

ENISA, the EU Agency for cybersecurity, is now stronger. The EU Cybersecurity Act grants a permanent mandate to the agency, and gives it more resources and new tasks.

ENISA will have a key role in setting up and maintaining the European cybersecurity certification framework by preparing the technical ground for specific certification schemes. It will be in charge of informing the public on the certification schemes and the issued certificates through a dedicated website.

ENISA is mandated to increase operational cooperation at EU level, helping EU Member States who wish to request it to handle their cybersecurity incidents, and supporting the coordination of the EU in case of large-scale cross-border cyberattacks and crises.

This task builds on ENISA's role as secretariat of the national Computer Security Incidents Response Teams (CSIRTs) Network, established by the Directive on security of network and information systems (NIS Directive).

A European cybersecurity certification framework

The EU Cybersecurity Act introduces an EU-wide cybersecurity certification framework for ICT products, services and processes. Companies doing business in the EU will benefit from having to certify their ICT products, processes and services only once and see their certificates recognised across the European Union.

[More on the certification framework](#)

[Cybersecurity Act](#)

[Background information](#)

Q&A: Cybersecurity Act

Follow the latest progress and learn more about getting involved.

Follow the Commission's work on cybersecurity @CyberSec_EU

Latest

PRESS RELEASE | 30 September 2021

Trade and Technology Council: Inaugural meeting agrees on important deliverables and outlines areas for future EU-US cooperation

At the first meeting of the Trade and Technology Council (TTC) in Pittsburgh, the EU and the US agreed on concrete deliverables and outlined the

future scope of work. Notably, the EU and the US committed to cooperating closely on shared priorities such as export controls, foreign investment screening, critical and emerging technology standards including Artificial Intelligence, and secure supply chains including on semiconductors. They also agreed to work together on important global trade issues, such as the challenges posed by non-market economies and trade-related climate and environment

PRESS RELEASE | 30 September 2021

The European Cybersecurity Month is kicking off: 'Think Before U Click'

The ninth edition of the European Cybersecurity Month has kicked off and will run for the entire month of October under the motto 'Think Before U Click'. This is an annual awareness campaign organised by the Commission, the European Union Agency for Cybersecurity (ENISA) and over 300 partners in the Member States, including local authorities, governments, universities, think tanks, NGOs and professional associations.

PRESS RELEASE | 28 June 2021

The European Cybersecurity Competence Centre and Network is now ready to take off

The regulation establishing a new Cybersecurity Competence Centre and a Network of National Coordination Centres has entered into force this week. The Cybersecurity Competence Centre, which will be located in Bucharest, will contribute to strengthening European cybersecurity capacities and to boosting research excellence and the competitiveness of the Union's industry in the cybersecurity field.

PRESS RELEASE | 23 June 2021

EU Cybersecurity: Commission proposes a Joint Cyber Unit to step up response to large-scale security incidents

The Commission has laid out a vision to build a new Joint Cyber Unit to tackle the rising number of serious cyber incidents impacting public services, as well as the life of businesses and citizens across the European Union. Advanced and coordinated responses in the field of cybersecurity have become increasingly necessary, as cyberattacks grow in number, scale and consequences, impacting heavily our security. All relevant actors in the EU need to be prepared to respond collectively and exchange relevant information on a 'need to share', rather than only 'need to know', basis.

[Browse Cybersecurity](#)

Related Content

Big Picture

Cybersecurity Policies

The European Union works on various fronts to promote cyber resilience, safeguarding our communication and data and keeping online society and economy secure.

See Also

European Cybersecurity Competence Network and Centre

The European Cybersecurity Network and Cybersecurity Competence Centre help the EU retain and develop cybersecurity technological and industrial capacities.

Stakeholder Cybersecurity Certification Group

The Stakeholder Cybersecurity Certification Group was established to provide advice on strategic issues regarding cybersecurity certification.

The EU cybersecurity certification framework

The EU cybersecurity certification framework for ICT products enables the creation of tailored and risk-based EU certification schemes.

NIS Directive

The NIS Directive is the first piece of EU-wide legislation on cybersecurity. It provides legal measures to boost the overall level of cybersecurity in the EU.

Source URL: <https://digital-strategy.ec.europa.eu/policies/cybersecurity-act>