The European Union Agency for Cybersecurity - A new chapter for ENISA

On Thursday 27 June 2019, the EU Cybersecurity Act (CSA) enters into force. ENISA will become the European Union Agency for Cybersecurity, with a new permanent mandate.

Published on June 26, 2019



Tagged with

* [cybersecurity](https://www.enisa.europa.eu/search?Subject%3Alist=cybersecurity)

The Cybersecurity Act gives ENISA a reinforced role in cybersecurity with new tasks. The Agency has also been given additional financial and human resources to address these tasks.

ENISA Executive Director, Udo Helmbrecht, stated:

“*I welcome the Cybersecurity Act and thank the Council, European Parliament and Commission for their support in the drafting and passing of this important piece of cybersecurity legislation. I also welcome the reinforced role of ENISA in the European cybersecurity ecosystem and the opportunity for ENISA to support the Digital Single Market. I believe the European Cybersecurity Certification Framework detailed in the Act will play a leading role for the advancement and harmonisation of cybersecurity certification in Europe and beyond. ENISA will have market related tasks, notably by preparing ‘European cybersecurity certification schemes’ that will serve as the basis for certification of ICT products, processes and services. ENISA is looking forward to working with Member States, the EU Institutions and industry to deliver the tasks set out in the Cybersecurity Act.”*

Commissioner Mariya Gabriel, EU Commissioner in charge of Digital Economy and Society, stated: "*The EU Cybersecurity Act has demonstrated the urgency to opt for an EU approach in this sensitive area. To respond to this political imperative, Europe has reinforced its Agency for Cybersecurity ENISA. It is crucial for citizens, businesses and Member States to feel more secure, including in cases of large-scale cross-border cyber-attacks. The Cybersecurity Act also enables EU-wide cybersecurity certification for the very first time, thus boosting the Single Market for cybersecurity. Through the Cybersecurity Act, the Directive on the security of networks and information systems and the proposed European Cybersecurity Competence Centre, we have put forward a strong EU pattern, based on values and open for strengthening cooperation with international partners.”*

**A new chapter**

One of the biggest changes brought about by this EU Regulation is that ENISA will have a permanent mandate and will be renamed as the European Union Agency for Cybersecurity. Additionally, the Agency is henceforth mandated to perform the following new tasks:

**Cybersecurity certification**

ENISA has a pivotal role in the new Cybersecurity Act in that the Agency will play a key role in the development of the EU Cybersecurity certification framework by preparing candidate certification schemes.

Cybersecurity certification is a new policy area at EU level. In delivering this task the Agency will provide high quality technical and policy support to stakeholders.

Upon request from the European Commission or the European Cybersecurity Certification Group (ECCG) composed of Member States, ENISA will coordinate the preparation of candidate cybersecurity certification schemes.

The candidate schemes prepared by ENISA and with the cooperation of national certification authorities and industry experts will be submitted to the European Commission for adoption.

It is expected that the development and delivery of cybersecurity certification schemes will make it easier for businesses to trade across borders and for buyers to better understand the security features of the product or service.

**Cyber resilience**

ENISA shall support capacity-building and preparedness across the Union by assisting the Union institutions, bodies, offices and agencies, as well as Member States and public and private stakeholders, to increase the protection of their network and information systems, to develop and improve cyber resilience and response capacities, and to develop skills and competencies in the field of cybersecurity.

At the EU level, ENISA will continue to support the coordination of responses to large-scale cyber-attacks and crises, in cases where two or more EU Member States are affected. This includes the possibility for the Agency to carry out post-incident analysis, when requested by the Member States.

This will improve the Union’s response to cyber-attacks, improve cyber resilience and increase trust in the EU Digital Single Market.

**Policy**

ENISA will actively support the European Commission and Member States in developing and implementing upcoming European cybersecurity policies.

The Act will provide an opportunity for the Agency to apply its knowledge and experience towards the future vision of EU cybersecurity.

**Vulnerability Disclosure**

Furthermore, ENISA will assist Member States and Union institutions, bodies, offices and agencies in establishing and implementing vulnerability disclosure policies on a voluntary basis.

**The way forward**

The Act provides for a number of statutory bodies, namely the Management Board, National Liaison Officers Group and the new Advisory Group (formerly known as the Permanent Stakeholder Group).

In terms of the certification framework, ENISA will shortly start developing candidate certification schemes. The Agency will closely work with the relevant expert groups set up by the CSA: the European Cybersecurity Certification Group (ECCG) comprised of representatives from Member States, which will have to appoint the representatives from their competent authorities, and the Stakeholder Cybersecurity Certification Group (SCCG), which will be responsible to advise ENISA and the Commission.

**ENISA in a nutshell**

ENISA was set up in 2004 to work on a wide range of topics on network and information security. The Agency has been supporting the EU Commission and the Member States by giving guidance on the technicalities of network and information security, thus contributing to the proper functioning of the internal market.

Aside from the new tasks, ENISA’s priorities include critical information infrastructure protection, the NIS Directive, capacity-building activities such as cybersecurity exercises, standardisation and certification, provision of consolidated threat information to its stakeholder community, identification and dissemination of best practices on how to mitigate threats associated with new technologies, and supporting EU legislation such as the General Data Protection Regulation (GDPR) and eIDAS - the Regulation on electronic identification and trust services for electronic transactions in the internal market.