



National Cyber Security Centre
Ministry of Justice and Security

ENISA-EU Newsletter

In this newsletter, we inform you of relevant developments in the area of cybersecurity related to the European Agency for Cybersecurity (ENISA) and the European Union.

The National Cyber Security Centre (NCSC) represents the Netherlands in ENISA's Management Board and serves as the first point of contact in the Netherlands for ENISA. You can reach us at international@ncsc.nl.

New permanent mandate for ENISA: more resources and new certification tasks

With the entry into force of the EU Cybersecurity Act on 27 June 2019, ENISA has been granted a permanent mandate¹. Its budget has doubled² and it has been assigned the official title of 'EU Agency for Cybersecurity' [1]. The doubling of the budget will strengthen ENISA's implementation capabilities with respect to its current tasks (assisting Member States in improving their digital resilience) and provide support for the performance of its new certification tasks and responsibilities.

Increased support to Member States for strengthening digital resilience

ENISA will further enhance the EU's cybersecurity preparedness and resilience by contributing to a better exchange of information between EU Member States. It will do this by acting as the secretariat for the *EU National CSIRTs Network* and organising pan-European cybersecurity exercises and trainings. ENISA will also continue to assist Member States in the implementation of the Directive on security of network and information systems (NIS Directive).

Developing and supporting the implementation of the EU cybersecurity certification framework

Under this framework, certification schemes are developed for various categories of IT products, processes and services. ENISA develops these certification schemes in cooperation with stakeholders and keeps the public informed about this [2] [3]. ENISA also plays a role in setting up the necessary governance structures for EU certification: the European Cybersecurity Certification Group, which consists of representatives from the appointed National Cybersecurity Certification Authorities in the Member States, and a Stakeholder Cybersecurity Certification Group, which is responsible for advising ENISA and the Commission [4].

Apply for membership in the Stakeholder Cybersecurity Certification Group and other EU working groups

The European Commission has launched a call for applications to select the members of the EU Stakeholder Cybersecurity Certification Group (SCCG) [5]. This group is primarily responsible for advising the Commission and ENISA on strategic issues related to cybersecurity certification.

The call is open until **17 September 2019** for academic institutions, consumer organisations, conformity assessment bodies, standards development organisations, companies and sector organisations.

Other informal or ad-hoc ENISA expert working groups are also looking for cybersecurity experts. For example, you can express your interest in participating in the Informal Expert Groups on:

1 Earlier, ENISA's mandate had to be renewed every seven years.
2 To allow it to fulfil the new mandate and additional tasks, ENISA's annual budget has been increased from €11 million to €23 million for the next five years.

the Transposition of the SOGIS-MRA³ Certification Framework [⁶], the Network and Information Security Directive [⁷], ENISA Technical Trainings [⁸] and EU Member States Incident Response Development [⁹].

EU funding to the tune of €10 million available for projects for the development of cybersecurity capabilities within the EU

The Connecting Europe Facility (CEF) cybersecurity call for 2019 [¹⁰] offers funding opportunities for the key stakeholders identified in the NIS Directive, such as CSIRTs, Operators of Essential Services (OES)⁴ and various government bodies⁵. For the first time, funds will also be available for European certification authorities in the context of the implementation of the EU Cybersecurity Act. These funds are intended to promote projects for strengthening the cybersecurity capabilities of Member States and boosting cross-border cooperation and information exchange.

The deadline for the submission of proposals is **14 November 2019**.

Juhan Lepassaar chosen as new Executive Director of ENISA

On 16 July 2019, Juhan Lepassaar from Estonia was chosen by ENISA's Management Board as the new Executive Director of ENISA for a five-year term. Lepassaar has previously worked as Head of Cabinet for the European Commission Vice-President Ansip on issues relating to the digital internal market and EU affairs for the Government of Estonia.

Publications

In recent months, ENISA has published several reports on best practices followed in different Member States. Some of these are listed below:

Reports

- [ENISA's Opinion Paper on EU ICT Industrial Policy](#) over o.a. digitale soevereiniteit en de cybersecurity keten in de EU [¹¹];
- [Industry 4.0 Cybersecurity Challenges and Recommendations](#) concerning the biggest challenges for the adoption of security measures for Industry 4.0 and Industrial IoT [¹²];
- [7 Steps to shore up the Border Gateway Protocol \(BGP\)](#) dealing with BGP vulnerabilities and why it is important to address these [¹³];
- [ENISA's Opinion Paper on ISAC Cooperation](#) on how ISACs can contribute to further strengthening digital resilience in the EU [¹⁴];

- [Update of ENISA's CSIRT Maturity Assessment Model](#) from 2017 [¹⁵];
- [Study on CSIRT Landscape and Incident Response Capabilities in Europe 2025](#) concerning the future of CSIRTs and IR capabilities and possible blind spots [¹⁶];
- [Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity](#) concerning the human aspects of cybersecurity [¹⁷];
- [IoT Security Standards Gap Analysis](#) on the shortcomings of and advice on the development and repositioning of IoT standards [¹⁸].

Conferences and events

- [Trust Services Forum](#) 25 September 2019, Berlin [¹⁹];
- [National Cyber Strategies Workshop: Research and Innovation](#) 26 September 2019, Warsaw [²⁰];
- [3rd ENISA-Europol IoT Security Conference](#) 24-25 October 2019, Athens [²¹];
- [5th eHealth Security Conference](#) 30 October 2019, Barcelona [²²];
- [Maritime Cybersecurity Workshop](#) 26 November 2019, Lisbon [²³].

Other developments

Cyber attacks: European Council now able to impose sanctions [²⁴]; European Commission advocates a common EU approach to ensuring the security of 5G networks [²⁵]; EU launches four pilot projects in preparation for the EU Cybersecurity Competence Network [²⁶]; EU introduces bug bounty programme open source software [²⁷]; Overview of the progress of the EU 5G Action Plan [²⁸]; European Commission initiates public consultation on the new Digital Europe programme [²⁹].

³ ENISA seeks to assist the European Commission in the preparation of a candidate cybersecurity certification scheme to serve as a successor to the existing Senior Officials Group Information Systems Security (SOG-IS) Mutual Recognition Agreement (MRA).

⁴ Responsible for developing internal cybersecurity capabilities and setting up an Information Sharing and Analysis Centre.

⁵ Cybersecurity certification authorities, national cybersecurity competent authorities and single points of contact as referred to in the NIS Directive and the Cybersecurity Act.

Publication

National Cyber Security Centre (NCSC)
PO Box 117, 2501 CC The Hague,
The Netherlands
Turfmarkt 147, 2511 DP The Hague,
The Netherlands
070 751 5555

More information

www.ncsc.nl
info@ncsc.nl
[@ncsc_nl](https://twitter.com/ncsc_nl)

30 July 2019