European Commission

STATE OF THE UNION 2017

CYBERSECURITY

EU AGENCY AND CERTIFICATION FRAMEWORK

In order to scale up the EU's response to cyber-attacks, improve cyber resilience and increase trust in the Digital Single Market, the European Commission has proposed:

- A **European Union Cybersecurity Agency**, building on the European Agency for Network and Information Security (ENISA), which will improve coordination and cooperation across Member States and EU institutions, agencies and bodies;
- The establishment of an **EU cybersecurity certification framework** that will ensure the trustworthiness of the billions of devices ("Internet of Things") which drive today's critical infrastructures, such as energy and transport networks, and also new consumer devices, such as connected cars.

An EU Cybersecurity Agency

The Commission's proposal will give the existing European Agency for Network and Information Security (ENISA) more tasks and resources in order to assist Member States in dealing with cyber-attacks. This will be done with:

- **A strong mandate**
- **A permanent status**
- **Adequate resources**

ENISA resources	Now	Future
Staff	84 people	125 people
Budget	€11 million	€23 million
	gradual increase: starting with +5 million 1st year and fully achieved 4 years after entry into force.	

ENISA will improve the EU's preparedness to react by organising annual pan-European cybersecurity exercises and by contributing to better information sharing between Member States through the network of Computer Security Incident Response Teams (CSIRTs). It will help Member States to implement the Directive on the Security of Network and Information Systems (NIS) which clarifies reporting obligations of national authorities in case of serious incidents.

Proposed tasks

Policy development and implementation: to strengthen support to the Commission and Member States in the development, implementation and review of general cybersecurity policy and in key strategic sectors identified by the NIS directive e.g. energy, transport and finance.

Operational cooperation: to contribute to cooperation in the network of Computer Security Incident Response Teams (CSIRTs) at EU level and provide assistance on request to Member States to handle incidents.

Knowledge and information: to provide analyses and advice and to raise awareness, to become the one-stop shop (InfoHub) for cybersecurity information from the EU Institutions and bodies.

Capacity building: to reinforce support to Member States in order to improve capabilities and expertise, for instance on the prevention of and response to incidents.

Market-related tasks within the **Cybersecurity Certification Framework** prepare candidate European cybersecurity certification schemes, with the expert assistance and close cooperation of national certification authorities. Schemes would be adopted by the Commission. ENISA will also support policy development in information communications technololgy (ICT) standardisation.

An EU framework for cybersecurity certification

What is it for?

Certification plays a critical role in increasing trust and security in products and services that are crucial for the Digital Single Market. At the moment, a number of different security certification schemes for ICT products exist in the EU. For example, smart meter producers currently need to undergo separate certification processes in France, the UK and Germany. Without a common framework for EU-wide valid cybersecurity certificate schemes, there is an increasing risk of fragmentation and barriers in the single market.

How will the certification process work?

The **Cybersecurity Agency, ENISA**, will put in place and implement this certification process. The proposed EU-wide certification framework creates a comprehensive set of rules, technical requirements, standards and procedures to agree each scheme. Each scheme will be based on agreement at EU level for the evaluation of the security properties of a specific ICT-based product or service e.g. smart cards. This certificate will attest that ICT products and services that have been certified in accordance with such a scheme comply with specified cybersecurity requirements. The resulting certificate will be recognised in all Member States, making it easier for businesses to trade across borders and for purchasers to understand the security features of the product or service.

Is the use of the certification framework compulsory?

No. The use of certification schemes will be voluntary unless future EU legislation prescribes an EU certificate as a mandatory requirement to satisfy a specific cybersecurity need. However, as the framework avoids multiple certification processes in different Member States, there will be an incentive to certify the quality and verify the security of the products and services in question.

Existing certification schemes in the EU

Currently, there is a patchwork of cybersecurity certification schemes and initiatives in Europe. On the one hand, national certification initiatives are already in place or are emerging without being mutually recognised. On the other hand, not all EU Member States are part of the main European mechanism based on mutual recognition (SOG-IS).

The **Commercial Product Assurance** (CPA) developed in the UK applies to commercial off-the-shelf products that are awarded certifications which prove good commercial security practice and certify that a product is suitable for lower threat environments. However, there is no mutual recognition agreement for CPA, which means that products tested in the UK will not normally be accepted as certified products in other markets.

Certification Sécuritaire de Premier Niveau (CSPN) is an IT security certification scheme established by the National Cybersecurity Agency of France (ANSSI). Similarly to the CPA, there is no mutual recognition for CSPN, which means that products tested in France will normally not be accepted in other markets.

The **Dutch Baseline Security Product Assessment** (BSPA) provides information on the suitability of IT security products for use in the "sensitive but unclassified" domain. The BSPA scheme has been in pilot phase since 2015 and is expected to be operational by the end of 2017.

Other emerging initiatives

SOG-IS MRA includes 12 Member States plus Norway and has developed a few protection profiles on digital products e.g. digital signature, digital tachograph and smart cards. Members can participate in a mutual recognition agreement as certificate consumers and producers.