About the ENISA / NIS directive

*Guest editorial for CECUA ([www.cecua.eu](http://www.cecua.eu))*

In a constantly evolving digital environment, threats to the network and information systems in Europe are growing rapidly. While all economic and societal activities today rely upon information systems and communication networks, the development of European digital society can only be sustainably achieved with the establishment of proper network and information security (NIS) practices, policies, organizations and capacities.

ENISA is the European Union Agency for Network and Information Security, established in 2004. As set out in the current mandate, ENISA has been set up “for the purpose of contributing to a high level of Network and Information Security within the Union [...] thus contributing to the establishment and proper functioning of the internal market”, contributing to growth and employment in Europe.

NIS has been set high in the EU political agenda notably in the European Cybersecurity Strategy (2013), the European Cyberdefence Policy Framework (2014) and the European Digital Single Market (2015). ENISA will in the future, more than ever, need to accompany the efforts of Member States and Union institutions in reinforcing NIS across Europe. Above all, the recent adoption of the European NIS Directive of the European Parliament and the Council, further calls for enhanced commitment of ENISA in supporting a coherent approach towards NIS across Europe.


The main objective of the Directive is to achieve a *high common level of security of network and information systems within the EU*, by means of improved cybersecurity capabilities at national level, increased EU-level cooperation and risk management and incident reporting obligations for operators of essential services and digital service providers. As the entry into force date will probably be in August 2016, the member states (MS) have 21 months (up to May 2018) to adopt it into their national legislation.

Different types of stakeholders are mentioned in the provisions of the upcoming Directive. Member states governments’, private companies and bodies of the EU Commission will all have to work together for assuring a safer European cyber-space. The main obligations are the following:

- Obligations for all MS to adopt a national NIS strategy and designate national NIS authorities.
- Establishment of an EU level Cooperation Group on NIS, which consists of representatives from all MS designated authorities, EU Commission and ENISA.
- Establishment of an EU-wide CSIRTs network which consists of representatives from all EU Member States’ national CSIRTs and CERT-EU.
- Security and notification requirements for operators of essential services (ESP) and digital service providers (DSP).

ENISA, as the EU’s Cyber Security Agency which allocates a full unit to the NIS, will play a significant role in the implementation process of the new Directive, mostly by acting as a central hub for...
knowledge exchange and by providing support to all types of stakeholders involved in the process. The agency is mentioned several times in the Directive having the following responsibilities:

- Assistance for MS and the EU Commission by providing its expertise and advice and by facilitating exchange of best practices.
- Assistance for MS in developing national NIS strategies, a task already started several years ago.
- Participation within the Cooperation Group.
- Support EU Commission in developing security and notification requirements for ESPs and DSPs.
- Assistance for MS in developing national CSIRTs, a process that has been successfully going on for some years now.
- Coordination/Secretariat/Active Support of the CSIRT network.
- Advice and guidelines regarding standardization in NIS security, together with MS.

For a better understanding of the NIS Directive check the following figure which constitutes a graphical representation of the overall activities and stakeholders.

![The NIS Directive](image)

ENISA’s projects and activities in this area started several months before the NIS directive was adopted by providing support to different types of stakeholders and especially the European Commission. Currently, there are several ongoing projects in areas like: security measures and incident notification for digital service providers, identification of essential service providers, etc. This effort will be substantially increased in the following months, after the entry into force of the Directive. ENISA has already started the preparatory work by reorganising the internal activities/processes to favour the ones directly related to the Directive. Nevertheless, new resources are required, in order to cover all activities that derive from the implementation process.

References and additional sources: