

13/12/2011

EPR20/2011

www.enisa.europa.eu

Clarifying cyber security incident reporting: guidelines on how to implement the new telecom legislation on security & integrity “Art 13a”.

ENISA, the EU’s ‘cyber security’ agency, has today issued two technical guidelines. The first describes how to implement the mandatory cyber security incident reporting scheme for telecom operators, parameters, thresholds, and how to report; the second describes specific security measures telecom operators should take.

The new telecommunications legislation (EU directive 2009/140/EC) [among other things](#) offers protection for consumers against security breaches. Article 13a of the new legislation requires telecoms operators to report security incidents and to take security measures to enable secure and uninterrupted delivery of communication services over European telecommunication networks.

In 2010, ENISA, the European Commission (EC), Member States’ Ministries and Telecommunication national telecom regulatory authorities (NRAs), as the “Art13 Working Group” started work to bring clarity to the actual reporting, and to achieve a consistent implementation of Article 13a. This group of actors reached consensus on two guidelines: [Technical guideline on cyber security incident reporting](#), and [Technical guideline for minimum security measures](#).

“A clarification of how to report cyber incidents and how to implement article 13a in a consistent way provides a level playing field for the European telecom sector. This will remove the barriers for European telecommunications providers operating across borders.” say Dimitra Liveri and Marnix Dekker, editors of the two documents.

“Incident reporting and minimal security measures are important tools to provide consumers, businesses and governments confidence in the security of telecommunication services. After the recent [Diginotar](#) case there is also growing support for broadening the scope of this kind of legislation beyond the telecom sector”, says Professor Udo Helmbrecht, Executive Director of ENISA.

The guideline on [incident reporting guides NRAs](#) about two types of incident reporting mentioned in Article 13a: the annual summary reporting of significant incidents to ENISA and the EC, and ad hoc notification of incidents to other NRAs, in case of cross-border incidents. This guideline defines the scope of incident reporting, the incident parameters and thresholds. It also contains a reporting template for submitting incident reports to ENISA and the EC, and explains how reports will be processed by ENISA. The guideline for [Minimum Security Measures](#) advises NRAs on the minimum security measures that telecom operators should take to ensure security of these networks.

For full reports: <https://resilience.enisa.europa.eu/article-13>

For interviews: Ulf Bergstrom, Spokesman, ENISA, press@enisa.europa.eu, Mobile: + 30 6948 460 143, or Dr, Marnix Dekker, Expert, Marnix.Dekker@enisa.europa.eu

