Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

CHAPTER II

NATIONAL FRAMEWORKS ON THE SECURITY OF NETWORK AND INFORMATION SYSTEMS

Article 7

National strategy on the security of network and information systems

1 Each Member State shall adopt a national strategy on the security of network and information systems defining the strategic objectives and appropriate policy and regulatory measures with a view to achieving and maintaining a high level of security of network and information systems and covering at least the sectors referred to in Annex II and the services referred to in Annex III. The national strategy on the security of network and information systems shall address, in particular, the following issues:

a the objectives and priorities of the national strategy on the security of network and information systems;

b a governance framework to achieve the objectives and priorities of the national strategy on the security of network and information systems, including roles and responsibilities of the government bodies and the other relevant actors;

c the identification of measures relating to preparedness, response and recovery, including cooperation between the public and private sectors;

d an indication of the education, awareness-raising and training programmes relating to the national strategy on the security of network and information systems;

e an indication of the research and development plans relating to the national strategy on the security of network and information systems;

f a risk assessment plan to identify risks;

g a list of the various actors involved in the implementation of the national strategy on the security of network and information systems.

2 Member States may request the assistance of ENISA in developing national strategies on the security of network and information systems.

3 Member States shall communicate their national strategies on the security of network and information systems to the Commission within three months from their adoption. In so doing, Member States may exclude elements of the strategy which relate to national security.

Article 8

National competent authorities and single point of contact

1 Each Member State shall designate one or more national competent authorities on the security of network and information systems (‘competent authority’), covering at least the sectors referred to in Annex II and the services referred to in Annex III. Member States may assign this role to an existing authority or authorities.

2 The competent authorities shall monitor the application of this Directive at national level.

3 Each Member State shall designate a national single point of contact on the security of network and information systems ('single point of contact'). Member States may assign this role to an existing authority. Where a Member State designates only one competent authority, that competent authority shall also be the single point of contact.

4 The single point of contact shall exercise a liaison function to ensure cross-border cooperation of Member State authorities and with the relevant authorities in other Member States and with the Cooperation Group referred to in Article 11 and the CSIRTs network referred to in Article 12.

5 Member States shall ensure that the competent authorities and the single points of contact have adequate resources to carry out, in an effective and efficient manner, the tasks assigned to them and thereby to fulfil the objectives of this Directive. Member States shall ensure effective, efficient and secure cooperation of the designated representatives in the Cooperation Group.

6 The competent authorities and single point of contact shall, whenever appropriate and in accordance with national law, consult and cooperate with the relevant national law enforcement authorities and national data protection authorities.

7 Each Member State shall notify to the Commission without delay the designation of the competent authority and single point of contact, their tasks, and any subsequent change thereto. Each Member State shall make public its designation of the competent authority and single point of contact. The Commission shall publish the list of designated single points of contacts.

Article 9

Computer security incident response teams (CSIRTs)

1 Each Member State shall designate one or more CSIRTs which shall comply with the requirements set out in point (1) of Annex I, covering at least the sectors referred to in Annex II and the services referred to in Annex III, responsible for risk and incident handling in accordance with a well-defined process. A CSIRT may be established within a competent authority.

2 Member States shall ensure that the CSIRTs have adequate resources to effectively carry out their tasks as set out in point (2) of Annex I.

Member States shall ensure the effective, efficient and secure cooperation of their CSIRTs in the CSIRTs network referred to in Article 12.

3 Member States shall ensure that their CSIRTs have access to an appropriate, secure, and resilient communication and information infrastructure at national level.

4 Member States shall inform the Commission about the remit, as well as the main elements of the incident-handling process, of their CSIRTs.

5 Member States may request the assistance of ENISA in developing national CSIRTs.

Article 10

Cooperation at national level

1 Where they are separate, the competent authority, the single point of contact and the CSIRT of the same Member State shall cooperate with regard to the fulfilment of the obligations laid down in this Directive.

2 Member States shall ensure that either the competent authorities or the CSIRTs receive incident notifications submitted pursuant to this Directive. Where a Member State decides that CSIRTs shall not receive notifications, the CSIRTs shall, to the extent necessary to fulfil their tasks, be granted access to data on incidents notified by operators of essential services, pursuant to Article 14(3) and (5), or by digital service providers, pursuant to Article 16(3) and (6).

3 Member States shall ensure that the competent authorities or the CSIRTs inform the single points of contact about incident notifications submitted pursuant to this Directive.

By 9 August 2018, and every year thereafter, the single point of contact shall submit a summary report to the Cooperation Group on the notifications received, including the number of notifications and the nature of notified incidents, and the actions taken in accordance with Article 14(3) and (5) and Article 16(3) and (6).