Meeting minutes of NLO annual meeting of 8 June 2016

1.1 NIS Directive and its implications for ENISA

The Head of ENISA's Core Operations Department, Steve Purser, presented the NIS Directive and its implications for ENISA.

The scope of the NIS Directive is to achieve a high common level of security of NIS within the Union. It is the first EU regulatory act at this level.

***Status*:** The Netherlands presidency together with the ENISA, has already started preparing the implementation of the directive. A first informal meeting of the network of Computer security incident response teams (CSIRT) set up under the directive took place in The Hague on 5 April, followed by a second meeting in Riga on 10 May.

The Council position at first reading adopted on 17 May 2016, confirmed the agreement reached with the European Parliament in December 2015. To conclude the procedure, the legal act must still be approved by the European Parliament at second reading. The directive is expected to enter into force in August 2016.

Key Provisions of the Directive are the following:

•Obligations for all Member States to adopt a National NIS strategy and designate National Authorities.

• Obligations for all Member States to designate national competent authorities and CSIRTS.

•Creates first EU cooperation group on NIS from all Member States.

•Creates an EU national CSIRTs network.

•Establishes security and notification requirements for operators of Essential Services (ESP) and Digital Service Providers (DSP).

The NLO network is one of the principle mechanisms ENISA uses to exchange information with the Member States.

A lot of the NIS Directive is concerned with communication, therefore the challenge is to bridge this communication with the communication carried out in the NLO network. Alignment with upcoming cPPP is also necessary in terms of ENISA/NLO network activities.

1.2 Update of the activities of the network

Katerina Christaki, the NLO network coordinator on behalf of ENISA, welcomes the new members of the network (7) and gave an overview of activities that took place since the last annual meeting.

The network currently counts 32 Members from EU Member States, European Economic Area countries and 1 representative by the European Commission and the European Council.

NLO's input in ECSM, National Cybersecurity strategies project and workshop and ENISA Report on stocktaking on MS regulatory approaches for cyber security, was instrumental in 2015, while there was significant input in 5 other projects.

The NLOs terms of reference were briefly presented as well in order to give new members of the network what the role of the NLO is.

During 2015 and Q1 2016 ENISA sent ongoing time-critical announcements and information to the members of the NLO network such as the Info Notes series, request for experts to join working groups, messages to act as multipliers, upcoming ENISA project related tenders, vacancy notices, events organized by ENISA, or where the Agency contributes to e.g. HLE, Secure Cloud, security certification of ICT products, CSIRT workshop in Latvia etc., invitations for participation to surveys and confidential briefings.

ENISA appreciates the steady rise in the networks' participation to ENISA's requests and would like to maintain the momentum.

1.3 cPPP – contractual Public Private Partnership

European Commission's representative for the NLO network, Ms. Gemma Carolillo, gave a brief overview of the upcoming public-private partnership on cyber security.

The EU will invest up to €450 million in this partnership, under its research and innovation programme Horizon 2020, recognising that cyber security is an economic opportunity for the EU. This partnership on cybersecurity is expected to trigger €1.8 billion of investment by 2020.
See also: the European Commission and the European Cyber Security Organisation (ECSO) signed the cPPP on 5 July 2016, in order to achieve the goals of the Digital Single Market strategy.

1.4 CIIP in FRANCE

The French NLO gave a presentation on the French critical information infrastructures protection (CIIP) approach.

Acknowledging the increasing number and sophistication of cyberattacks against French interests, France has recognized since 2008 CIIP as a strategic priority, calling for a dedicated approach to the cybersecurity of critical operators. Over the past few years, France therefore engaged in a major and ambitious CIIP regulation effort, co-elaborated by the private and public sectors, offering real incentives and solutions for the operators.

In the context of the finalization of the European NIS Directive, the goal of this talk was to share some key elements and lessons learnt with ENISA and the members of the NLO network (from the EU and EEA).

1.5 NIS developments in the Dutch Presidency

Stephanie de Ridder from the Dutch NCSC highlighted actions during the Dutch Presidency in Q1 and Q2 of 2016.

The former Minister of Security and Justice has selected cyber security to be one of the Ministries' priorities during the Dutch Presidency. Cyber security was a subject on the agenda of the Informal Justice and Home Affairs Council in January 2016.

Furthermore, during the past months the Netherlands has drafted a paper, a first attempt in which the principles and goal and rules of procedure s of the future CSIRT Network are examined. This has been discussed during the first Informal Meeting in The Hague in April and a follow-up meeting in Riga in May. All Member States were invited to send their written input on the food for thought paper (deadline 17 June). At the end of the Presidency the work will be handed over to the Slovakian Presidency.

In May 2016, the Netherlands organized a High Level Meeting on Cyber Security. The results of the conference have been combined in a report and an infographic which are available online.
Follow: https://english.eu2016.nl/documents/publications/2016/05/13/infographic-high-level-meeting-cyber-security for the infographic.

1.6 Hungarian Input: new National Cyber-Security Centre, electronic identification card and future plans in NIS

The Hungarian NLO, Ms. Anita Tikos spoke on recent developments in NIS that took place in Hungary.

The Act L of 2013 on the Electronic Information Security of Central and Local Government Agencies has been modified in Hungary in July, 2015. As a result of this modification, the National Cyber-Security Centre was established in October 2015, by uniting the GovCERT-Hungary, the National Electronic Information Security Authority and the Cyber Defence Management Authority (CDMA).

Professor Zoltán Rajnai (PHD), Minister of Interior, was nominated as the new Hungarian Cyber coordinator in February 2016.

In March 2016, the military's National Security Service- Cyber Defence Centre was created.

Ms. Tikos also presented the new electronic identification card used in Hungary, and highlighted the main future plans (implementation of NIS directive, EWS project etc).

1.7 European Cybersecurity Month 2016 (ECSM)

Vangelis Stavropoulos, ENISA's project manager for ECSM, gave an overview of the ECSM project and its current status including the launch of the kick-off event on 30 September, in Brussels, at the premises of the European Banking Federation.

Requested feedback from NLO members for the ECSM project:

NLOs are kindly requested to confirm their participation to the kick-off event. An email will be sent to the network in this regard. (**Email sent on 28.07.2016**)

NLOs of Belgium, Croatia, Cyprus, Greece, Denmark, Ireland, Italy, Latvia, Lithuania, Malta, Portugal, Slovakia, and Slovenia are kindly requested to inform us on who the ECSM coordinator of their country is.

https://cybersecuritymonth.eu/

1.8 Round table discussion

Industry remains an important challenge for ENISA. Engaging new industry sectors is very difficult. This is a point where NLOs could help build relevant Industry communities in their countries.

New ENISA Info Notes series are very much appreciated. Specific mentions and very positive comments given by NLOs in this respect and in particular by ITALY and ROMANIA who appreciates the unbiased opinion expressed in Info Notes which is hard to find.

The example of Austria that launched in 2015 a consultation on EU Cyber Security structures was applauded. The consultation gave very positive results and constitutes good practice to be repeated in the future in the case of projects that require European input.

SP spoke on the recent re-organisation at ENISA whose main objective was to give a life-cycle approach to ENISA's activities. There is a need for ENISA to have a complete set of advice, ideas and blueprints that collaborators from relevant national administrations, cyber-security centres and stakeholders in general, could consult.

Specific mention was given to the certification of standards as there is a lot of interest and effort put currently in this domain. SP noted that currently there are contradictions in the Industry. For instance, the use of cryptography to secure data and communications in IoT devices may well be too expensive given the low cost of several of these devices.

Extra caution needs to be put on several upcoming NIS technologies, for instance in the case of IoT. All relevant actors need to remain alert on developments before important aspects are not being taken into account.

International certification is another example where things are complicated since it is difficult to reach interoperability.

James Caffrey, Irish NLO, stressed the NIS directive challenges in terms of use of personal data.

SP noted that we should take the opportunity that NIS directive is in the beginning and remain alert on developments and pitfalls.

Finally, Ratislav Machel, Slovakian NLO, has asked for promotional material for the upcoming presidency. (**OPEN call)**

NLOs' participation to ENISA's requests for input has increased and interaction through the network has become livelier. ENISA is pleased with this development and encourages new NLOs to use the network and those relatively inactive to get more involved.

1.9 Request sent by ENISA to the network in 2016

1. **eHealth and IoT – request (CLOSED)**

Project manager: Dimitra.Liveri(AT)enisa.europa.eu

Request to identify one contact point to use for all the studies that ENISA does, eHealth security, eHealth and IoT and eHealth and Cloud. In this request ENISA asked for contact points from the healthcare sector having responsibility like CISOs, CIOs etc. to whom we would address the above mentioned topics.

2. **Request on nominating a national representative for common baseline security requirements of security ICT products group.(CLOSED)**

Project manager: Prokopios.Drogaris@enisa.europa.eu

ENISA is conducting a study on common baseline security requirements for the procurement of secure ICT products. The Agency will create a dedicated expert group to support this activity and we would like to offer all Member States the possibility to nominate a national representative to join this group.

3. Updating contact points and email address of the dedicated CSIRTs of MS that would like to be part of the **CSIRT network (CLOSED)**

Project manager: Andrea. Dufkova@enisa.europa.eu

In order to prepare the setup of this CSIRT Network, ENISA organised also a Workshop in May 10 in Riga, Latvia.

4. **Security Requirements for DSPs - ENISA study - (OPEN)**

Project manager: Anna.Sarri(AT)enisa.europa.eu; Konstantinos. Moulinos (AT) enisa.europa.eu

ENISA is conducting a study with the objective to define baseline security requirements for Digital Service Providers, as defined in the recently agreed NIS Directive.
See relevant email communication of 17 June, 2016.

5. **Letter to be distributed for DSPs Incident Reporting NIS directive – (OPEN) deadline 31 July**

Project manager: Dan.Tofan (AT)enisa.europa.eu

Letter and survey that should be sent to digital service providers (DSPs) in MS countries targeting mostly local providers.

6. Request to UK, SI, CY NLOs of Austria, Cyprus, Slovenia and UK, for the purpose of **updating the guidebook on NCSS** with detailed objectives, steps and actions on how to develop and implement a NCSS. (CLOSED)

Project manager: Anna.Sarri(AT)enisa.europa.eu; Dimitra.Liveri(AT)enisa.europa.eu

7. Requests to nominate ECSM contact points in MS - (CLOSED**) & Invitation for the European Cyber Security Month kick-off event to the NLO network - (OPEN- deadline for registration: 9 September)**

Project manager: Vangelis.Stavropoulos(AT) enisa.europa.eu