ENISA's contribution to the Digital Single Market

1 ENISA's mission is:

'Securing Europe's Information Society'

The ENISA mandate is very broad in scope. The Agency therefore seeks to contribute to those areas where it adds the most value and shifts its focus to other areas when these areas reach maturity.

2 By 2020, ENISA's vision is:

- To be '**the hub'** for exchange of information on cybersecurity between the EU public sector and Member States.
- To have developed its operational model, based on recommendations, policy support and 'hands on' work so as to provide seamless support to its stakeholders in all areas covered by the mandate.
- To have an established presence in all key industry sectors and be a recognised name among security professionals.
- To be able to demonstrate a positive contribution to EU economic growth through its initiatives.

3 ENISA's Strategic Objetives

ENISA can influence the growth of the cyber security market in Europe. In cooperation and in support to the Member States and the Union institutions, ENISA will in priority seek to achieve:

- #Expertise **Anticipate and support Europe in facing emerging network and information security challenges**, by collating, analyzing and making available information and expertise on key NIS issues potentially impacting the EU, taking into account the evolutions of the digital environment.
- #Policy **Make network and information security an EU policy priority**, by assisting the Member States and the Union institutions in developing and implementing EU policies and regulations related to NIS.
- #Capacity **Support Europe in setting up state-of-the-art network and information security capacities**, by assisting the Member States and Union institutions in reinforcing their NIS capacities.
- #Community **Make the European network and information security community a reality**, by enhancing cooperation at EU level among Member States, Union institutions and related NIS stakeholders, including private sector.
- #Enabling **Reinforce ENISA's impact**

4 Key Messages

- Maximize the contribution of NIS to the EU economy
- Facilitate dialogue on cyber-security in the EU
- Support operational cyber-security communities to work together
- Support technologies that make on-line privacy meaningful
- Provide strategic foresight on cyber threats
- Harden cyber responses in critical industries
- We create a strong Information Security Community – 'Together Secure'
- We facilitate dialogue on cyber-security in the EU
- We train the trainers in cybersecurity

- ENISA should be the authoritative reference for NIS in the EU
- We secure Europe's Infrastructures and Services
- Together with the operational communities we enhance the EU proactive and reactive cyber-capabilities through 'training' and 'Exercises'
- We help establish trust online and protect fundamental EU rights by IT security technologies

5 ENISA's priorities for 2016

ENISA will broaden its scope in:

- smart cars, smart airports and smart hospitals
- new studies in mHealth
- security of IoT

ENISA will continue its work on established priorities such as:

- the pan-European cyber security exercises
- improving critical information infrastructure protection (CIIP) across the EU
- support for implementation of Security & Data Breach notification obligations
- the ENISA threat landscape
- the EU Cybersecurity Month
- capacity building
- CSIRTs development and training, supporting the CSIRT community
- Continue to encourage and support Article 14[1] requests
- continue its collaborations through MoUs both with public and private entities

6 ENISA's support to the EU Digital Single Market

ENISA's founding regulation states "… contributing to the establishment and proper functioning of the internal market. ENISA can influence the growth of the cyber security market in Europe and thus support the IT-security level in EUROPE.

- The European market for IT security is €20bn growing at 6% CAGR[2]
  - There are 900,000 IT security professionals in Europe, forecast to grow at 6% p.a.
  - 7 of the top 37 global IT security companies are domiciled in Europe, generating global IT security revenues of €6bn

  There is the opportunity to grow the cyber security market in Europe by up to €7bn, and enable value creation in the EU economy of up to €640bn to 2020
- Cyber-attacks are increasing in complexity and severity, with reported incidents growing at 41% p.a.
  - Aligning with global benchmarks could grow the EU IT security market by up to €7bn

[1] Article 14 of ENISA Regulation (EU) No 526/2013
[2] Cyber-security market size in Europe – Gartner 2014

- Matching North American spend on cyber security as a proportion of GDP would grow the EU cyber security industry by €7bn
- Growing at the global average for IT security spend would increase the European market by €1.0bn to 2018
- Achieving the same growth in cyber spend as a share of GDP as North America would increase the European cyber market by €0.4bn
- Reducing shortage of talent within organisations could grow the workforce by up to 0.3m jobs in 2018
- Revenues of companies domiciled in Europe could be increased by €1bn

- It is estimated that up to €640bn of potential EU economic is at risk[3] depending on future scenarios: **EU currently lags behind North America for technology adoption**

ENISA can add value here:

- ENISA has developed a strong network of stakeholders in both the public and private sector and can call upon these at any time to support policy initiatives. The ENISA approach to working with its stakeholders greatly increases the scalability of its operations and results in a feeling of 'ownership' and a high level of buy-in.
- ENISA is well positioned to support the Commission in implementing the NIS Directive and the cybersecurity component of the Digital Single Market (DSM) approach. The Agency could also sensibly support the implementation of the upcoming General Data Protection Regulation.
- ENISA is well integrated in the EU approach to Cybersecurity, but could take a more proactive role in ensuring effective and efficient information exchange between other EU agencies and bodies. The Agency could also act as coordinator for all activities in other agencies related to cybersecurity preparation.
- In conclusion, we believe that ENISA can play a role supporting the economic benefits of cyber in Europe (through helping companies better protect/create value based on effective security, as well as supporting European vendors to access and grow in the market), ENISA's contribution could come in the form of additional information, support and community building, on the threat and the solutions.

7 ENISA's recommendations for responding to evolving threats

The following compact messages correspond to conclusions from the analysis of this year's cyber threats, in particular:

Message 1: **context** is more relevant than the volume of information

> **"In cyber-security, it is important to create as much as possible long-living contextual information and knowledge on threats from the vast amount of short-living incident data. The acquired knowledge and context should be of high quality and be transferrable to all relevant players in the cyber space"**

[3] Risk and Responsibility in a HyperconnectedWorld –World Economic Forum

Message 2: **sharing** is promising but does not yet work properly

> ***"sharing of cyber-threat intelligence will be more efficient if the context of shared information is known and if there is a balance of knowledge among the participating parties. There is a lot of work to be done to achieve this"***

Message 3: cyber threat **statistics** will need to be elaborated

> ***"The statistic and metrics models used in cyber-threat intelligence require elaboration. Otherwise the quality and comparability of the achieved results will remain questionable. This is an obstacle in the creation of usable, contextual cyber threat intelligence"***

Message 4: cyber **attack methods** become more pervasive

> ***"Most of the attacks are based on low-end, low to medium-tech attack methods. Keep calm, maintain long memory and implement baseline protection. If you are someone who might be targeted by cyber-espionage, you are at high risk"***

Message 5: **threat agents** need to be looked at more closely

> ***"Efforts to increase attribution rates of cyber threat agents are necessary. This will lead primarily to sentence already performed criminal activities, but it will also achieve precedent and increase the knowledge about who is the enemy"***

Message 6: **internet of things** is here to stay, so is the cyber threat exposure that it represents

> ***"The internet of things is at the edge of the cyber-space. As such, cyber-security must be embedded and ready-to-use without any technical knowledge. In order to achieve this, a bigger cooperation between producers and operators of technical systems, but also society and service providers will be necessary"***

Message 7: lessons from **data breaches** in 2015

> ***"Lessons learned from data breaches are one of the most valuable resources for cyber intelligence. Lessons learned need to be made available for all relevant stakeholders at the highest speed possible. The form of this information need to be such, that it can be immediately translated to corrective actions"***