**European Network and Information Security Agency**
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 710 01 Heraklion, Greece, P.O.BOX 1309
www.enisa.europa.eu, Tel: +30 2810 391280 Fax: +30 2810 391410

15 April 2009

# ENISA's Role in Supporting the Commission's Strategy on CIIP

## Introduction

The European Network and Information Security Agency (ENISA) recognises the importance of Critical Information Infrastructures as an essential factor in economic and social development. Computing and networking are now becoming ubiquitous utilities in the same way as electricity or water supply. The security of communication networks and information systems, in particular their availability, is therefore of increasing concern to society.

ENISA welcomes the recently announced EU Commission's Communication on Critical Information Infrastructure Protection (CIIP). This Communication, which provides a clear framework to enable Europe to act in case of major disruptions, defines the main pillars of a pan European strategy on CIIP.

## ENISA's Expertise

ENISA, through its annual Work Programme activities, has already developed knowledge and expertise relevant to CIIP within the scope of its mandate. This includes, among others, activities in the areas of security and resilience of public eCommunications networks, co-operation of national/governmental Computer Emergency Response Teams (CERTs) and risk assessment and risk management.

- ✓ ENISA's Program on Security and Resilience of public communications networks, took stock of national policy and regulatory environments, providers' measures, and technologies and standards. The Agency currently develops good practice guides on information sharing, incident reporting, exercises, and providers' measures.

- ✓ On a more technical level, ENISA has conducted a study on technologies that could potentially be used to increase the resilience of European network infrastructure. It is clear from this study that widespread deployment of DNSSec would bring about a significant improvement. Consequently, the Agency is in the process of conducting a study on the cost of DNSSEC deployment identifying the new operations and changes arising from DNSSEC deployment and their impact in terms of cost.
- ✓ In the field of establishment and operation of Computer Emergency Response Teams (CERTs) ENISA has positioned itself as an independent, knowledgeable and trustworthy partner for Member States, the Commission and the CERT communities. By producing and piloting valuable good practice material the Agency aims at closing the gap of incident management capabilities among the Member States and on European level.
- ✓ The work of ENISA in the area of Risk Management covers a wide spectrum of activities, including the promotion of good practices, the performance of assessments, gap analyses and provision of recommendations for protecting information and systems. This work looks at many different types of risk, notably information security risks, continuity risks, IT contingency and emerging technological risks.

ENISA is in constant dialogue with relevant stakeholders, such as the Agency's Permanent Stakeholders' Group (PSG), National Liaison Officers (NLO) network, ad-hoc Working Groups and other expert groups. These groups are often called upon to support ENISA's activities, such as thematic workshops on relevant topics, or direct discussions with providers, regulators or other policy makers. Access to these networks has enabled the Agency to develop unique insights on important issues of CIIP.

Since the start of its operational activities in 2005, the Agency supports and actively participates in the Meridian conference/process, an international platform for informal information exchange and cooperation on CIIP. In parallel, ENISA contributes actively to relevant international fora, such as the OECD, ITU and FIRST where technical contribution must be strengthen.

## ENISA's Contribution

### Preparedness and Prevention

- ✓ *Baseline Capabilities of National CERTs*

  ENISA fully recognises the importance of baseline capabilities of national/governmental CERTs. This would enable the day-to-day, in-depth information sharing and cooperation among Member States' CERTs.

  As a first step, the Agency will assemble a first version of an inventory of minimal (baseline) services and capabilities for National/Governmental CERTs in close cooperation with the relevant stakeholders.

  This inventory will then be refined and updated on a periodic basis, to support the goals of the Commission and this strategy.

- ✓ *Strategic pan European Public Private Partnership for Resilience (EP3R)*

  ENISA is uniquely positioned to support the Commission in establishing a pan European Public Private Partnership (PPP) for Resilience. Such a partnership could significantly reduce differences among Member States and pave the way towards a more harmonised policy and regulatory environment in Europe.

  In 2009, ENISA through technical interaction with EU Commission and Stakeholders will clarify the mission, objectives, desired services/products, funding, profiles of participants, operational modalities, and other issues relating to the PPP. Based on this analysis the Agency will work with the Commission to define a roadmap for setting up the proposed PPP.

- ✓ *European Forum for information sharing between Member States*

  ENISA proposes to support this Forum by bringing in its expertise on policy and operational aspects of security and resilience, its good practice guides in certain areas, and its network of organisations and experts that are interested in deploying such good practices.

  ENISA is actively involved in the development of such good practice guides, namely on information sharing, exercises, and incident reporting schemes. In addition, the Agency has established good practice collections in various fields of establishment and operation of CERTs. In 2009, ENISA will finalise the good practice guides referred to above and provide them to the Forum as a starting point. It will also assist the Commission in identifying possible participants of such a Forum and promote the establishment of the Forum in its workshops and events.

  Once the Forum has been established, ENISA will continue to support its activities in a number of ways. The Agency will align its Resilience good practices strategy with that of the Forum. ENISA proposes to be the technical body that supports the day to day operations of the Forum, i.e. the body that will develop on behalf of the Forum good practices on any matters proposed by its members. The Agency could also undertake actions on disseminating good practices and create awareness at national level.

## Detection and Response

- ✓ *European Information Sharing and Alert System (EISAS)*

  ENISA welcomes the actions proposed in this area, which are in line with the conclusions of its own study conducted in 2006/2007 on “a Europe wide Information Sharing and Alerting System for citizens and SMEs”.

  One of the main conclusions of the feasibility study is that the most feasible scenario does not imply any “system” but rather a framework of good-practice collection and sharing with the goal to enhance all Member States capabilities in reaching out to their citizens and SMEs with NIS information. Within this framework the Commission and

ENISA have an important role to play as collector and custodian of good information sharing practices, expertise and contacts to stakeholders.

ENISA will follow the two pilot projects of EISAS mentioned in the Communication. The Agency will furthermore prepare itself to take stock of the results and other national initiatives.

## Mitigation and Recovery

✓ *National Contingency Plans and Exercises*

ENISA fully recognises the importance of national contingency plans on CIIP. Exercises are an indispensable tool for assessing the national emergency and crisis preparedness measures.

ENISA already developed exercises for National CERTs. The Agency is in the process of piloting them. The current ENISA Resilience Program is developing good practice guides on defining and running national exercises. Both these efforts include scenarios that aim at enhancing the preparedness of Member States on CIIP.

ENISA will continue its efforts in collecting, analysing and sharing good practices on contingency plans, preparedness measures and national and pan European exercises. The Agency will be in dialogue with Member States (e.g. national CERTs, national CIIP organisations) to address their needs. Through workshops organised by ENISA, Member States will be able to enhance their knowledge on preparedness measures and contingency plans.

✓ *Pan-European exercises on large-scale network security incidents*

ENISA welcomes this action as it goes beyond national boundaries and enables pilot exercises at the level of the European Union.

Using lessons learned through the stock taking exercises, ENISA will advice Member States on the different options of exercises to deploy through its good practice guides. In addition, ENISA will contribute with knowledge on the management of continuity risks to support such exercises and reflect achieved results back to the continuity/contingency plans.

Where CERTs are concerned, ENISA will encourage the sharing of good practices with regards to cross-border exercises in Europe and on international level (like Cyberstorm or ASEAN drill exercises), where European CERTs were involved.

✓ *Reinforced cooperation between National / Governmental CERTs*

A few national/governmental CERTs are already involved in everyday in-depth sharing of information in a group called "European Government CERT" group (EGC). ENISA aims at learning more about the incentives but also the barriers for this kind of close cooperation in order to facilitate participation by of all Member States. The previously mentioned inventory of baseline capabilities for national/governmental CERTs will be accompanied by an updated report on "CERT cooperation and its further facilitation" with an emphasis on analysing the standards and obstacles to cooperate and to share information.

### International cooperation

- ✓ *Internet resilience and stability – European priorities on long term Internet resilience and stability and Principles and guidelines for Internet resilience and stability (European level)*

  Based on the results of the stocktaking exercises and the work carried out in the area of secure Internet protocols, the Agency is well-positioned to support the Commission and Member States in defining EU priorities on critical Internet components and issues, as well as in establishing a roadmap towards principles and guidelines for Internet resilience and stability.

  In particular, the areas of technologies and standardisation present a great potential for International Co-operation. In this light, the identification of technologies with a potential to improve resilience of communication networks and associated areas for R&D investment and co-ordination of this work at International level is a priority. Standardisation by definition encompasses the need of early consensus building at an International level. In this respect, identifying the gaps in terms of standards and setting the priorities of International Standardisation bodies plays an important role.

- ✓ *Internet resilience and stability – Principles and guidelines for Internet resilience and stability (Global level)*

  The Agency will support the Commission in its dialogue with Third Countries and international fora, including the Internet Governance Forum. Such support could build on the cooperation between the Commission and ENISA in the representation of the European Communities in the OECD Working Party on Information Security and Privacy.

  In particular, as part of the 2010 Work Programme, the Agency will explore international cooperation opportunities with the aim to improve the capabilities of all Member States and increase the overall coherence and interoperability levels. The Agency invites the Commission to discuss the scope of this activity with a view to support the EU policy making process in order to assess if and how the Agency could fulfil such mission.

## Conclusions

ENISA views the publication of the communication on CIIP as a significant step towards securing Critical Information Infrastructure against large scale disruptions. Where ENISA is mentioned, the recommendations are largely aligned with the Agency's current approach and constitute a logical extension of its current activities.

This document has demonstrated that ENISA has the experience and the willingness to respond to the Commission's requests and has outlined how this might be achieved in practice by aligning accordingly its resources.