

Cybersecurity

Supporting the CIIP Action Plan

Dr. Steve Purser

Head of Technical Competence Department,
European Network & Information Security Agency (ENISA)

10 November 2011

Agenda



- ★ Introduction to ENISA
- ★ Supporting the CIIP Action Plan
- ★ Cybersecurity Exercises

- ★ The European Network & Information Security Agency (ENISA) was formed in 2004.
- ★ The Agency is a *Centre of Expertise* that supports the Commission and the EU Member States in the area of information security.
- ★ We facilitate the exchange of information between EU institutions, the public sector and the private sector.



Agenda



- ★ Introduction to ENISA
- ★ Supporting the CIIP Action Plan
- ★ Cybersecurity Exercises

The Commission CIIP Communication

- ★ “Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience” – published 30 March.
- ★ Strengthens the role of ENISA.
- ★ Activities within the scope of the European Program for Critical Infrastructure protection (EPCIP).
- ★ Proposes five areas, or ‘pillars’, of action.
- ★ ENISA is explicitly called upon to contribute to three of these areas.



The Role of ENISA

- ★ ENISA's role is to proactively support Member States in achieving the objectives of the CIIP action plan.
- ★ Member States must take the lead in addressing the issues.
- ★ ENISA is currently supporting the CIIP action plan in a number of ways:
 - ★ Assisting Member States in the planning process.
 - ★ Setting up mechanisms to facilitate the establishment and day-to-day running of key instruments (European Forum for IS, EP3R, ...).
 - ★ Providing input in the form of studies and best practices.



EFMS

- ★ The **European Forum for Member States** builds on national approaches to CIIP.
- ★ It will be used to foster common understanding of the issues and strategies for dealing with them.
- ★ ENISA is supporting this initiative in the following way:
 - ★ Assisting the Commission and Member States in defining a roadmap for the EFMS.
 - ★ Ensuring exchange of expertise on policy and operational aspects.
 - ★ Provision of good practice guides as a starting point.
 - ★ Identifying significant risks and proposing suitable mitigation strategies.



EP3R

- ★ The **European PPP for Resilience** will provide a framework for supporting collaboration between public and private sectors on NIS policy issues.
- ★ There are many challenges in establishing such a PPP, but we can learn a lot from national initiatives.
- ★ ENISA is supporting this initiative in the following way:
 - ★ Summarising lessons learned from national PPPs.
 - ★ Identifying challenges and obstacles.
 - ★ Working together with Member States to identify a common approach.
 - ★ Supporting the creation and day-to-day running of EP3R



Agenda



- ★ Introduction to ENISA
- ★ Supporting the CIIP Action Plan
- ★ **Cybersecurity Exercises**

First Pan European Exercise

- ★ Table top exercise
- ★ Incidents affecting all Member States
- ★ Tested only communication aspects
- ★ Involvement of public authorities/bodies only
- ★ Concentrated on members of the CIIP community
– no political escalation
- ★ Test Carried out on 4 November 2010



Objectives

- ★ Increase understanding of how cyber incidents are handled by Member States
- ★ Test communication points and procedures between participating Member States
- ★ Build trust among participants - help to establish mutual support procedures
- ★ Create a CIIP community with a focus on exercises
- ★ Highlight interdependencies between MS across Europe



Objectives - Measures

- ★ Measures to test:
 - ★ The contact points in the MS.
 - ★ The communications channels and the type of data exchanged over these channels.
 - ★ The understanding that MS have of the role and mandate of their counterparts in other MS.



The Scenario

- ★ The scenario was not the focus of the test **but was used to support the test.**
- ★ Based on a Cyber Incident.
 - ★ The impact is on IP networks - large operators – cross country interconnections.
 - ★ We assume that voice (PSTN/Mobile) communications are not affected.
 - ★ Similarly, supporting facilities, such as power supply are not affected.
- ★ Implemented as 320 injects.



Participation

- ★ All EU Member States and 3 EFTA countries (Switzerland, Norway, Iceland) participated
- ★ Profile of Participants:
 - ★ Ministries, National Regulatory Agencies, CIIP and Information Security related organisations, CSIRTs and other related stakeholders
 - ★ 70 organisations and 150 experts
- ★ The role of ENISA was to help Member States to prepare - facilitation and project management.
- ★ The role of the JRC was to provide scientific and technical support for the exercise itself.



Findings

- ★ Findings have been published and are available on the ENISA web site.
- ★ These findings have been grouped:
 - ★ Planning & Structure.
 - ★ Building Trust.
 - ★ Understanding.
 - ★ Points of contact.
- ★ A set of recommendations can also be found in the final report.



1st Joint EU-US Exercise - key facts

- ★ Announced in April during the Hungary Ministerial Conference
- ★ Table top, centralised, discussion based
- ★ Exploratory nature, how do we engage each other?
- ★ Planning team with experts from 15 countries
- ★ Exercise completed on 03.11.11

