JRC Technical Notes

Memorandum on the results of the sixth Workshop on the Implementation and Application of the Directive 2008/114/EC

Ispra 1-2 December 2011

Georgios Giannopoulos
Muriel Schimmer

EUR 25232 EN - 2012

JRC EUROPEAN COMMISSION

ipsc Institute for the Protection and Security of the Citizen

The mission of the JRC-IPSC is to provide research results and to support EU policy-makers in their effort towards global security and towards protection of European citizens from accidents, deliberate attacks, fraud and illegal actions against EU policies.

European Commission
Joint Research Centre
Institute for the Protection and Security of the Citizen

Contact information
Address: Via E. Fermi 2749, 21027 Ispra (VA), Italy
E-mail: georgios.giannopoulos@jrc.ec.europa.eu
Tel.: 00390322786211
Fax: 00390332789576

http://ipsc.jrc.ec.europa.eu/
http://www.jrc.ec.europa.eu/

JRC68759

EUR 25232 EN
ISBN 978-92-79-23171-1
ISSN 1831-9424
doi:10.2788/14841

Luxembourg: Publications Office of the European Union, 2012

Printed in ITALY

Contents

Memorandum on the results of the sixth workshop on the implementation and application of Directive 2008/114/EC

1 Background and purpose of the Workshop

This workshop was the sixth technical meeting of representatives of the MS, three years after the adoption and entry into force of the Directive. The workshop had six objectives:

- to exchange information and discuss problems - on a voluntary basis - on the application of the Council Directive 2008/114/EC of 8 December 2008
- to have preliminary results of the Study to support the Preparation of the Review of Directive 2008/114/EC by Booz
- to provide details of Operator Security Plans and more particularly a presentation of the Reference Security Management Plan for the energy sector
- to provide an overview of the European ICT sector including ICT related critical infrastructure and links to the Directive
- to provide an overview of the European Space sector including space related critical infrastructure and its links to the Directive
- to discuss the preparation of the review of the Directive including the inclusion of new target sectors in the reviewed Directive

2 Agenda

A copy of the original agenda can be found annexed to this memorandum. The agenda was fully respected.

3 Overview of the state-of-play regarding the transposition and implementation of the Council Directive 2008/114/EC of 8 December 2008

At the beginning of the round table discussion, Commission presented the status of the transposition and implementation of the Council Directive 2008/114/EC of 8 December 2008 (Directive).

DG HOME has closed nine out of thirteen infringement cases. Only two Member States (MS) did not fully transpose the Directive and have received a reasoned opinion letter. Two other Member States have only very recently notified their measures which are currently scrutinized.

For the Commission, EPCIP and the Directive remain a priority. However, the whole Critical Infrastructure policy should be reviewed and revised. In this context a reshaped EPCIP programme including a follow-up to the current Directive will be proposed in late 2012.

3.1 Views from the MS, round table discussion

The views were discussed following this template:

1. The status of the transposition of the Council Directive into national law in each Member State.
2. The application of the Directive, including identification and designation of ECI.
3. Experiences and particularly issues regarding the efficiency and efficacy of current procedures and provisions in place. This may include the scope and content of the Directive, the workflow, responsibilities of actors, legal issues and technical issues.

3.1.1 BELGIUM

Belgium has transposed the Directive into national law. Loi 01.07.2011 relative à la sécurité et la protection des infrastructures critiques. It includes all ECI sectors except air transport for which a separate royal decree has been adopted. It has engaged in constructive bilateral discussion with the Netherlands, Germany, France and Luxembourg to identify and designate potential European critical infrastructures.

However, according to Belgium, this bilateral approach is not appropriate to assess risks/vulnerabilities in European networks and systems and to measure the impact of a failure. Furthermore Belgium mentioned that the structure of the Directive does not empower multilateral issues and discussions and also that an impact analysis is missing.

3.1.2 BULGARIA

Bulgaria has transposed the Directive in national law by adopting the Decree of the Council of Ministers on 1.02.2011. There are amendments to the National Disaster Protection Law. Bilateral discussions have been engaged with Greece in November 2011 and bilateral discussions with Romania have been finalised in 2010 and a list of potential ECIs has been drafted. A national CIP policy is under development. The Bulgarian Academy of Science is in charge of a project that aims at developing diverse CIP tools with focus mostly against terrorism.

3.1.3 DENMARK

Denmark has transposed the Directive in national law by adopting four ministerial orders in the Energy and Transport sectors; one covering the three energy areas electricity, natural gas and oil and three different ministerial orders for the transports areas rail, harbors and roads. No ECI has been identified in Denmark nor in other MS.

3.1.4 FINLAND

Finland has completed the implementation process. It has been considered that the existing legislation fully covers the requirements of the directive and consequently, no new legislation has been adopted. Bilateral discussions have been conducted with Estonia, Sweden and Norway. No ECI has been identified. Finland recommends to discuss more in detail the EPCIP programme and to focus less on the Directive. It also suggests conducting a discussion on the usefulness and clearness of cross cutting criteria.

3.1.5 GERMANY

Germany has transposed the Directive via an amendment of the Energy law. It has implemented the Directive in two phases by using the procedure described in art 3.3. and in Annex III of the Directive. Germany considers that the bilateral approach is not suitable for networks as the electricity or ICT systems. The security plan however is a good instrument to improve the protection of CIs.

3.1.6 LITHUANIA

Lithuania has adopted a Government Resolution in 2011. It has concluded the bilateral discussions with Poland and could invite other neighbouring countries for the bilateral discussions regarding some potential ECI in their territory. Sectoral and Cross-Cutting criteria are difficult to apply, and the concept of alternatives is unclear; this will be even more difficult in case of ICT. Lithuania will have the Presidency of the EU in the second semester of 2013.

3.1.7 THE NETHERLANDS

The Netherlands have implemented the EPCIP directive on 24.12.2010. The conclusion of the Dutch identification process is that under the set criteria (as set out in the guidelines) there are no European critical infrastructures in The Netherlands. The Netherlands consider that a network approach is needed for systems as the electricity grid.

3.1.8 POLAND

Poland has fully transposed the Directive into national law. An Act of 29^{th} October 2010 amending the Act of 26th April 2007 on crisis management, transposing the Directive entered into force on 4^{th} of January 2011. In July 2011, Poland has adopted resolutions on the ECI designation. ECI have been identified in the energy sector. Poland recommends clarifying the ambiguities of the Directive as e.g. the identity of the Critical Infrastructure.

3.1.9 SLOVAKIA

Slovakia has transposed the Council Directive 2008/114/EC into national law by adopting Act No. 45/2011 Coll. on critical infrastructure. Slovakia has engaged in bilateral and multilateral discussions with Austria, the Czech Republic, Hungary and Poland. However, the designation process of the ECI with Hungary is still ongoing since no bilateral agreement on mutual protection of classified information that would enable the two MS to exchange classified information exists.

3.1.10 SWEDEN

Sweden has implemented the Directive. Bilateral discussions have been conducted with neighboring countries. They have found non-binding guidelines helpful, but due to high thresholds of criteria no ECIs are identified in Sweden.

3.1.11 UK

The UK has fully completed the transcription process of the Directive. The UK has conducted bilateral discussions with other MS, but no ECI has been identified. UK mentioned the positive impact and side-effects of the Directive at national, bilateral and multilateral level. Some systems, such as ICT, ATM or electricity would clearly touch on several countries. The Directive was only one tool in EPCIP which should be carefully reviewed.

3.1.12 SLOVENIA

Slovenia has transposed the Directive by adopting a governmental decree on 12 May 2011. The sectors have conducted the identification process by using the procedure in Annex III of the Directive. Discussions with Austria, Italy and Hungary are ongoing, but as of today, no ECI has been identified and no final conclusions can be drawn. Several issues need to be discussed during the review process as regards the energy sector.

3.1.13 ROMANIA

Romania has transposed the Directive by adopting a governmental ordinance in 2010. An Inter-Ministerial Working Group on CIP was established to implement the Directive. Consequently, a national strategy has been launched to protect critical infrastructures, potential ECIs identified, plans defined and SLOs trained. A number of potential ECIs exists in the energy sector.

3.1.14 NORWAY

Within the context of the EEA framework Norway has planned to amend a Civil Protection Act. An existing law protects national infrastructures and complies with the requirements of the Directive as regards OSP and SLOs. Norway has not identified any potential ECI on its territory.

3.1.15 MALTA

Malta has transposed the Directive in 2011. Under the Prime Ministers office. A CIIP strategy and CERT have been established.

3.1.16 LATVIA

Latvia has transposed the Directive by adopting an amendment to the National Security Law and by adopting Regulations of the Cabinet "Procedures for the Identification of Critical Infrastructures, Including European Critical Infrastructures and Planning and Implementation of Security Measures". Latvia has engaged bilateral discussions with neighboring MS, but no ECIs have been identified.

3.1.17 HUNGARY

Hungary has transposed the Directive in national law by amending the government resolution 2080/2008. Two governmental bodies were in charge of the implementation of the Directive. The Ministry of Interior has completed the implementation process. An Inter-Ministerial Working Group has proceeded to the identification of national infrastructures and has engaged in bilateral discussions with neighboring countries.

3.1.18 GREECE

Greece has implemented the EU Council Directive 2008/114/EC by adopting a presidential decree on 5.5.2011. Greece has had bilateral discussions with Bulgaria. Greece considers that a multilateral approach is needed to determine ECIs in the electricity sector. Directive is one of the tools to protect ECIs but other tools could be also foreseen.

3.1.19 FRANCE

France has transposed the Directive into French law by adopting a decree. The designation process is ongoing. France has engaged bilateral discussions with neighboring Spain, Belgium, Germany, UK, the Netherlands and Italy. Several ECIs have been identified in the energy and transport sectors. For now, a bilateral agreement has been reached for one of them. Generally speaking, air traffic control and the electric transmission grid need a common European approach, which should lead to start with a risk analysis at the European level. A multilateral forum would be an optimal idea. France proposed to organize a first meeting with European Network of Transmission System Operators for Electricity (ENTSO-E), Transmission Systems Operators (TSOs), DG HOME, DG ENER, the JRC and the MS.

3.1.20 CZECH REPUBLIC

The Czech Republic has transposed the Directive into national law by amendment of a law on crisis management which entered into force on January 1, 2011. The implementation process of the Directive is fully completed.

Based on art 4 of the Directive, the Czech Republic discussed the topic on the identification and designation of intended ECIs with the neighbouring MS, i.e. Austria, Slovakia, Germany and Poland on a bilateral and multilateral basis. The Czech Republic signed both the general and the technical protocols with these MS. ECIs that might affect those MS have only been identified in the energy sector.

3.1.21 AUSTRIA

Austria has employed existing, appropriate binding and non binding legal instruments to implement the Directive. Public-Private Partnerships have been established with owners or operators of critical infrastructures; these have largely been involved in the implementation process. Austria has based the identification of ECIs on sectoral criteria and economic effects. ECIs have been designated in the energy sub-sectors "Electricity". Discussions are still ongoing as regards the Gas sub-sector.

Austria has identified several problematic questions while transposing/implementing the Directive:

- Risks: The directive is based on an all hazards approach, but risks are not specified or mutually agreed. Establishing a broad risk catalogue would be a good initiative to reach a consensus as for threats and hazards to be taken into consideration.
- OSP, asset and systems approach: Austria considers that the OPS should not be limited to physical assets, but also take into consideration the organisation and systems, which need to be protected against all hazards.
- Identification process: a reciprocity principle should be applied. Also, the alternatives to a service or a CI should be located on the territory of the EU.
- The Cross-Cutting criteria are not appropriate for small countries and are not easy to apply. In addition thresholds are high.
- Alternatives for ECIs should be within the EU.

3.2 Conclusions on the transposition and implementation of the Directive

3.2.1 Cooperation with operators and other key stakeholders

Starting a stronger cooperation with operators, as for example with ENTSO-E in the electricity sector or Gas Infrastructure Europe (GIE) in the gas sector, is regarded as essential. ENTSO-E has a major role as regards the development of networks nodes and more generally systems within the 3^{rd} energy package . Also, ENTSO-E has established a Critical System Protection Working Group that is responsible for coordinating new critical system protection issues regarding electricity transmission. Another key stakeholder would be the new Agency for the cooperation of Energy regulators based in Ljubljana (Slovenia).

It has been decided that two meetings to cover separately the issues related to the electricity and gas sector. COM will invite ENTSO-E/GIE whereas MS will be in charge of inviting their national TSOs. An additional comment has been that high voltage networks should be regarded as a system and if so a single OSP should be drawn.

3.2.2 JRC Conclusions: Sectoral and Cross-Cutting Criteria: Lessons Learned and Further Steps: JRC Input for Consideration

The Directive is based on two fundamental elements.

- The designation process, which is deemed to define what is critical through an impact assessment (cross-cutting criteria) and to classify it as such;
- The assessment of the need to protect Critical infrastructures.

An ECI can be designated on basis of quantitative or qualitative criteria (USA and Canada). In Europe, ECIs get designated based on impact assessment, both qualitative and quantitative criteria are applied. Sectoral criteria are based on a bottom-up approach. The sectoral approach focuses on the protection of assets from man-made threats and more particularly terrorist attacks. However this approach has limits: dependencies and interdependencies among systems and/or sectors are not considered, the focus is on man-made threats and the all hazards approach gets less attention, the nature of threat is disregarded as well as its probability. Threat scenarios can hardly be developed at European level. Cross-cutting criteria are based on a top-down approach; the use of quantitative threatholds is the key instrument to identify and designate ECIs. Dependencies and interdependencies however are considered only when measuring the economic impact of disruptions and failures. Terrorism has been the driving force behind the Directive; the asset-based approach was optimal to protect assets from terrorist attacks. The system approach however focuses more on systems. The role of JRC has been to provide technical support to the Commission services and also support to the Member States for the implementation of the Directive. With respect to the later it has released several relevant documents and organized several workshops where among others the following elements have been presented.

- Guidelines for the application of cross-cutting criteria to identify critical infrastructures
- Critical Energy Infrastructure Protection : EU activities
- Analysis of vulnerability in the European electricity and gas transmission systems
- Electricity : Cybersecurity of Power Systems
- Gas: European Security issues views of the GIE security group
- Reference security management plan for Energy infrastructure
- Air traffic control: presentations of ENAV and Eurocontrol

- Security certifications and EC Directive 114/08
- Dealing with network/system risks instead of threats to single assets in the context of the directive
- Resilience
- Domino: The Domino project: DOMINO effect modelling infrastructure collapse
- Dynamics of cascading events and in the assessment of associated consequences.
- Modelling and analysis of the impact of CI on the Fast Moving Consumer Goods Supply Chain
- CIPS conference: presentations of the results of CIPS

Several issues were raised subsequently to the presentation:

- The identification process has lead to the identification of many national CIs as well as to an awareness of threats and vulnerabilities.
- An absence of ECIs in the transport sector can also be seen as positive: there are many alternatives that can meet transport needs.
- Risk assessment is far more important than evaluating the relevance of criteria. What matters are threats, vulnerabilities and risk analysis.
- A multilateral understanding of systemic CI would be preferable to a bilateral understanding and consensus finding,
- An all hazards approach and risk assessments methodologies are missing. What are the plans to improve the identification methodologies of ECIs and the implementation deficits?
- Which criteria will be used for ICT, Space, Health and Finance?
- Only a limited number of ECIs have been designated. Poland asked whether sectoral criteria should be removed and the designation of ECIs based only on cross-cutting criteria.
- Cross-cutting criteria could be merged; more particularly casualties and public effects.
- The thresholds defined in the Cross-Cutting criteria are stand-alone. In principle, an analysis should precede the specification of thresholds; in this case, they were defined without clear argumentation.
- Common methodologies at European level should be defined for threats and risk assessment
- Risk assessments to identify the values of Cross-Cutting criteria and thresholds

3.2.3 A Reference Security Management Plan for Energy infrastructure assets

The Reference Security Management Plan for energy infrastructure assets, based on the Prism methodology developed by the Harnser group, is a guidebook that provides a practical methodology and guidelines on how to set up a security plan. It is comprised of four stages: strategy and planning, assessment, design, implementation and review. Although this plan is for the moment applicable to the energy sector, it can be adapted in order to serve other sectors as well. Several issues were raised subsequently to the presentations:

- What is the practical application for operators?
- Is this plan valuable for a single sector or can it be used for all sectors? Who is defining the level of acceptable risk as e.g. the acceptable number of hours of disruption? Are cross-border issues addressed? Member States make their own risk assessment and these are not necessarily consistent.
- At the end of the presentation it was announced that DG ENER will shortly launch a study on economics of security in the energy sector.

4 Preparation of the review of the directive

Booz has presented the status of the study and has scheduled a first validation meeting for the month of February 2012. Several questions came up during the interviews, such as the applicability of the thresholds of the Cross-Cutting criteria, the location of alternatives in candidate MS, and the difficulty to assess the transboundary impact. Also, some MS consider that it is essential to first evaluate the benefit of the Directive in the Energy and Transport sector before adding new sectors to the scope of the Directive. It is difficult to have a final idea as for the improvement of the protection of critical infrastructures.

Finland believes that an update of the 2006 Communication and of the EPCIP programme should first be considered.

5 State of play - ICT related critical infrastructure and links to the directive

On 30 March 2009, the Commission adopted a first Communication on Critical Information Infrastructure Protection Protecting Europe from large scale cyber-attacks and cyberdisruptions: enhancing preparedness, security and resilience setting out a plan (the CIIP action plan) to strengthen the security and resilience of vital Information and Communication Technology (ICT) infrastructures. The aim was to stimulate and support the development of a high level of preparedness, security and resilience capabilities both at national and European level. The CIIP action plan is built on five pillars: preparedness

and prevention, detection and response, mitigation and recovery, international cooperation and criteria for European Critical Infrastructures in the field of ICT.

On 30 March 2011, the Commission adopted the new Communication on Critical Information Infrastructure Protection Achievements and next steps: towards global cyber-security COM(2011) 163 final, that takes stock of the results achieved since the adoption of the CIIP action plan in 2009. It describes the next steps planned for each action at both European and international level. It also focuses on the global dimension of the challenges and the importance of boosting cooperation among MS and the private sector at national, European and international level, in order to address global interdependencies.

The impact assessment accompanying the CIIP action plan and a broad array of analyses and reports by private and public stakeholders highlight not only Europe's social, political and economic dependencies on ICT, but also the steady growth in the number, scope, sophistication and potential impact of threats be they natural or man-made.

Areas of achievements since 2009:

- European Forum for Member States (EFMS) to discuss CIIP between national competent authorities
- European Public-private Partnership for Resilience (EP3R)
- Baseline of capabilities and services for pan-European cooperation of national/governmental CERTs
- European Information Sharing and Alert System (EISAS)
- National contingency planning and exercises
- Pan-European exercise on large-scale network security incidents
- Internet resilience and stability

The technical discussion in EFMS led to a first draft of the ICT sector-specific criteria for identifying European Critical Infrastructures, with a focus on fixed and mobile communications and the Internet. The technical discussion will continue and benefit from the consultations on the draft criteria, at national and European (via EP3R) level, with the private sector. The Commission will also discuss with MS the ICT sector specific elements to be considered for the review of the Directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection in 2012.

Several issues were raised subsequently to the presentations:

- A regulatory framework for European security is necessary
- CIIP security is necessary. ICT has a crucial cross-sectoral role; disruptions can seriously affect other sectors.

BUT:

- The objectives of these criteria are not clear and the difficult issues are not self evident in the paper.
- These criteria are not applicable to a system. Defining the assets that are necessary for the system should be the first step, followed by an impact analysis on multilateral basis.
- The added value of the Directive should first be assessed before adding new sectors as ICT to the Scope of the Directive.
- Consolidation of an in depth system approach before expanding the directive.
- The challenges for the ICT sector should first be assessed before adding the sector to the Directive.
- How do we cope with the competences and plans of DG INFSO?
- Would the Directive bring added value to the ICT sector?

6 State of play - space related critical infrastructure and links to the directive

DG ENTR presentation on the space sector (Annex) detailed the various factors that make the space sector vital for Europes economy and the well-being of its citizens. ICT, road transport, aviation, maritime transport, precision agriculture and environment protection, civil protection and surveillance benefit from satellite functionalities. Part of the space infrastructure located in the space segment is at risk of damage or destruction by natural phenomena, such as solar radiation and asteroids, and by other spacecraft and space debris. It is also under threat from electromagnetic interference, be it intentional or otherwise. Ground segments can be damaged by man-made, technological or natural hazards. Some Member States have the resources to respond in part to these risks. However, these resources are inadequate because of their technical shortcomings and the absence of sufficient coordination mechanisms. Also, on the 4^{th} April 2011 the European Commission released the Communication "Towards a space strategy for the European Union that benefits its citizens", which reflects the crucial role of space for the economy and society. The Communication sets out the main priorities for the EU, which include ensuring the success of the EU's two flagship space programmes Galileo and GMES, the protection of space infrastructures, and space exploration. The Communication also calls for the development of an industrial space policy in close cooperation with EU Member States and the European Space Agency.

On the 30th November 2011, The Commission released a proposal for a Regulation of the European parliament and of the Council on the implementation and exploitation of European satellite navigation systems (COM(2011) 814 final). It recommends that the Member States shall take all necessary measures so that the systems' earth stations are designed as European critical infrastructures within the meaning of Council Directive 2008/114/EC.

Several Member States host private satellite operators. The Galileo satellite systems are owned by the Union at least until 2020. In November 2011, the Commission has proposed to earmark 7.0 billions to guarantee the completion of the EU satellite navigation infrastructure and to ensure the exploitation of the systems until 2020, such as the operations of the space and terrestrial infrastructures, the necessary replenishment/replacement activities, certification procedures, and notably the provision of services. According to the new framework proposal for the financing and governance of the two European satellite navigation programmes Galileo and EGNOS (GPS signal augmentation) for the period 2014-2020, the management of the programmes' exploitation should be delegated to the European GNSS Agency while management of the programmes' deployment should be delegated to the European Space Agency.

Several issues were raised subsequently to the presentations:

- Does this proposal for a new regulation also apply to private satellite operators? Who owns Galileo?
- ESA is an international organisation. How can the EU impose regulations to an international organisation? How an OSP can be imposed to them?
- Satellite applications must be secured apart from physical space installations.
- It needs to be defined what the Directive should provide as an added value and what we want to achieve with the inclusion of space in the scope of the Directive.
- Gallileo is purely European. In that sense who is responsible for its protection?
- Austria underlined that a future framework needed to encompass EU owned infrastructure (the current Directive does not handle this issue).

7 Discussion of potentially new target sectors - Tour de table. Views from MS

Further discussions and evaluations of the Directive are needed to clarify the opportunity to include new sectors in the scope of the Directive. Below MS individual proposals:

7.1 AUSTRIA

- Pharmaceutical industry is a vital sector with a limited number of alternatives.

7.2 CZECH REPUBLIC

- ICT and Space are regarded as important.

- The cooperation with other stakeholders as international organizations or operator associations should be improved. Interdependencies and sector boundaries related issues should be addressed in collaboration with other DGs.
- Support to multilateral cooperation.
- Proposition to invite relevant financial authorities in case the finance sector is further discussed for inclusion in the scope of the Directive

7.3 FRANCE

- Finance

7.4 HUNGARY

- A proposal will be made in January 2012.

7.5 LATVIA

- Finance and agreement with the proposal for multilateral cooperation.

7.6 MALTA

- ICT.
- The coordination with other DGs or EU agencies needs to be improved.

7.7 NORWAY

- Finance
- A review of the Directive is necessary as well as an assessment of the added value of including sectors to the scope of the Directive.
- Clear conclusions on the existing sectors before including new ones.

7.8 ROMANIA

- ICT and Finance
- Romania considers that it is too early to propose new sectors as the designation process is still ongoing and the directive might be modified.

7.9 SLOVENIA

- ICT, Food and Health.
- Slovenia considers that the designation process should be finished first before making any further decision.

7.10 UK

- Finance
- The problems in the sector need to be assessed in the first place as well as the policy activities

7.11 SWEEDEN

- Sweden has no suggestions for further sectors.
- A discussion should take place on the geographical imbalance of ECIs.
- ECIs are located mostly in the centre of Europe, none has been identified on the peripheries and those affecting on a reciprocal basis non EU Member States have not been included.

7.12 SLOVAKIA

- ICT and Space.
- Gallileo should be included as ECI

7.13 POLAND

- Finance and ICT
- Sectoral and cross-cutting criteria should be eliminated and the ambiguities of wording used in the Directive clarified or removed (e.g. Identity)

7.14 LITHUANIA

- Support for ICT sector in the scope of the Directive based on the evidence of added value of the Directive and other additional benefits.
- Still not clear impact on Energy and Transport sector
- Detailed impact analysis would be helpful for discussions about ICT sector.
- Step by step approach for including in the Directive scope additional sectors: ICT and maybe other sectors later, based on evidence of added value of the Directive

7.15 THE NETHERLANDS

- ICT and Space
- The JRC presentation highlighted the weakness of the asset approach as regards the protection of national or EU-wide systems. That discussion should be continued, also on interdependencies.

7.16 ITALY

- ICT, Space, Finance,
- Issues in the energy sector needs to be discussed

7.17 GERMANY

- The Directive needs to be reviewed. General minimal guidelines should be developed that cover systems as a whole.
- First step is to consider EPCIP and then the Directive.
- EPCIP and its instruments need to be reviewed.

7.18 FINLAND

- A substantial comprehensive discussion should be conducted on the need to have the Directive. Other instruments as recommendations are available.
- The earlier directive was launched based on art 308 of the Rome treaty. What are the legal implications after the adoption of the Treaty of Lisbon?
- Who declares that an event is critical- such as the volcano eruption on Iceland?

7.19 DENMARK

- The added value for the sectors needs to be assessed. Has the Directive contributed to improve the protection of CIs?
- Is there a real need for better protection? What are the threats and the vulnerabilities of CIs?
- A bilateral approach is not sufficient. A European perspective should be adopted.

7.20 BULGARIA

- ICT, Space and Finance

7.21 BELGIUM

- Finance
- Assessing the results of the implementation of the Directive should be the first step before adding other sectors. Also, a discussion on networks should take place for the Energy and Gas sectors. The contributions of other agencies need to be assessed.
- The identification process is inadequate as the criteria do not indicate which parts of the system are concerned.

8 Conclusions

- EPCIP goes beyond the Directive
- EPCIP vs other policies (sectoral/horizontal)
- Directive. Challenges to:

  Assets approach (vs Networks/Systems)

  Sectoral approach (criteria, boundaries)

  Criteria and thresholds

  Identification and designation procedure (complexity, multilateral issues, EU owned infrastructure)

  No clear view how to handle other sectors (e.g. ICT)
- Areas for further workshops

  Finance, ICT, Space, Pharmaceutical, Transport, Energy

  Horizontal issues, instruments, programme scope,

9 Dates for next Workshops

- Booz validation + Electricity Workshop 15/02/12
- CIP POC + Final Booz Workshop; 14-16/03/12
- 7th Workshop + CIPS week of 23/04/12
- EU-US 22-23/05/12
- CIP POC + EPCIP Impact assessment presentation week of 25/06/12

10 Annexes

- Agenda of the VI EPCIP Workshop on the Implementation and Application of the 2008/114/EC Directive
- Explanatory Note of the VI EPCIP Workshop on the Implementation and Application of the 2008/114/EC Directive
- Study to Support the Preparation of the Review of Directive 2008/114/EC
- Sectoral and Cross-Cutting Criteria: Lessons learned and further steps JRC Input for consideration
- A Reference Security Management Plan [RSMP] for Energy Infrastructure Assets
- State of play on Critical Information Infrastructure Protection CIIP Achievements and next steps: towards global cyber-security
- Space and CIP

JRC
EUROPEAN COMMISSION

ipsc
Institute for the Protection and Security of the Citizen

Agenda of the VI EPCIP Workshop on the Implementation and Application of the 2008/114/EC Directive

ipsc
Institute for the Protection and Security of the Citizen
European Commission
Joint Research Centre (JRC)
Institute for the Protection and Security of the Citizen

Via E. Fermi, 2749
I-21027 Ispra (VA) - Italy

Tel.: +39 0332 78 6038
Fax: +39 0332 78 5469

Web: http://ipsc.jrc.ec.europa.eu/
E-mail: JRC-STA-SECRETARIAT@ec.europa.eu

VI EPCIP Workshop on the Implementation and application of the 2008/114/EC Directive

Casa Don Guanella, Ispra, Italy

1-2 December 2011

Final Agenda

JRC
EUROPEAN COMMISSION

Robust science for policy making

OUR MISSION

The mission of the Joint Research Centre is to provide customer-driven scientific and technical support for the conception, development, implementation and monitoring of European Union policies. As a service of the European Commission, the Joint Research Centre functions as a reference centre of science and technology for the Union. Close to the policy-making process, it serves the common interest of the Member States, while being independent of special interests, whether private or national.

JRC
EUROPEAN COMMISSION

VI EPCIP Workshop on the Implementation and Application of the 2008/114/EC Directive

	1 December
09:00-09:30	**Welcome and Introduction – Overview of the State-of-Play (DG HOME, JRC)**
09:30-10:15	**Implementation issues – Tour de table. Views from the MS.**
10:15-10:30	**Coffee Break**
10:30-11:15	**Implementation issues – Tour de table. Views from the MS.**
11:15-11:45	**Lessons learned by JRC (sectoral and cross cutting criteria, preparation for risk assessment)**
11:45-12:30	**General discussion**
12:30-14:00	**Lunch**
14:00-15:00	**Operator Security Plans (including presentation of Reference Management Security Plan for the energy sector)**
15:00-15:15	**Preparation of the review of the Directive (DG HOME, JRC, MS)**
15:15-15:45	**Preliminary results of the study by Booz**
15:45-16:00	**Coffee Break**
16:00-17:00	**State of play - ICT related critical infrastructure and links to the Directive (DG INFSO, JRC)**
17:00-17:30	**General discussion**
19:00	**Dinner**

	2 December
09:00-10:30	**State of play - space related critical infrastructure and links to the Directive (DG ENTR, JRC)**
10:30-11:00	**Coffee Break**
11:00-12:00	**Discussion of potentially new target sectors - Tour de table. Views from MS**
12:00-12:30	**Overall discussion, way forward, discussion of topics and date for next workshop**
12:30-14:00	**Lunch**
14:00	**End of the Workshop**

Please note that the working language will be English.

Practical details

Registration
Registration to the meeting can be made through the following link by **20 November** at the latest: https://jrc-meeting-registration.jrc.ec.europa.eu (Create an account is required, then go to Ispra site on top and check for the events in December)

Venue:
Casa Don Guanella, Ispra Italy

Milan Airports:
Milano Malpensa, Milano Linate

Local transports
Transport from and to the airport will be organized by JRC.

Hotel
Rooms have been pre-booked at Casa Don Guanella.

Workshop content information:

Mr. Christian Krassnig (DG HOME)
+32 (02) 29 86 445.
Christian.KRASSNIG@ec.europa.eu

Mr. Georgios Giannopoulos (DG JRC)
+390332786211
Georgios.GIANNOPOULOS@jrc.ec.europa.eu

For **organizational issues (Hotel, transport, etc.)** please contact:
Mrs. Maria Giovanna Giuliani :
+39 0332 786038
Maria-Giovanna.GIULIANI@ec.europa.eu

JRC
EUROPEAN COMMISSION

ipsc
Institute for the Protection and Security of the Citizen

Explanatory Note of the VI EPCIP Workshop on the Implementation and Application of the 2008/114/EC Directive

EUROPEAN COMMISSION
DIRECTORATE GENERAL JRC
JOINT RESEARCH CENTRE
Institute for the Protection and Security of the Citizen
STA Unit

Subject: Explanatory note for the 6th workshop on the Implementation and Application of the 2008/114/EC Directive

Ispra, 22.11.11

Introduction

The 6th EPCIP workshop on the Implementation and Application of the Directive is organized to communicate the current status of the implementation and application across the MS and the Commission services. Apart from the *business as usual* of the workshop - discuss current implementation issues and best practices among the participating MS for the application and implementation of the Directive – this workshop has a more important role, that is to set the cornerstone for the review of the Directive that is due to kick off in January 2012.

Items on the Agenda

The Agenda will be flexible, and may be adapted to the needs of discussions that emerge during the workshop.

Round Table Discussion

In order to render the procedure more efficient the items for the round table discussion can be organized in the following lines:

1. Any updates on the legal/administrative implementation of the Directive in your Member State

2. Any updates on the application of the Directive, including identification and designation of ECI (e.g. new ECI's designated)

3. Experiences and particularly issues regarding the efficiency and efficacy of current procedures and provisions in place. This may include positive experiences or problems faced regarding the scope and content of the Directive, the workflow, the criteria, responsibilities of actors, legal issues and technical issues (such as OSP).

4. Any other points

Any ideas or items to be added in this informal questionnaire are welcome so please do not hesitate to contact me on this.

Lessons learned by JRC (sectoral and cross cutting criteria)

The main topic of this talk will be a review on the procedure to establish the sectoral and cross cutting criteria and how these have served the designation of ECIs. The scope of this review is to identify strong and weak points of this procedure and investigate its applicability within the scope of the review of the Directive.

Joint Research Centre · Via E. Fermi, 2749I-21027 Ispra (VA), Italy · TP 723
Telephone: direct line (+39-0332) 785339- , exchange 789111 · Telefax: 78 5469
E-mail: jrc-sta-secretariat@ec.europa.eu
http://sta.jrc.it/

Operator security plans

The Operator Security Plan is an important element of the Directive since it describes the actions that operators have to take in order to protect designated ECI. Several MS have expressed their need to have more info on operator security plans. Thus we take the opportunity in this workshop to present the work related to the energy sector. This work can be used as an example for establishing similar documents for other sectors.

Preparation of the review of the Directive

The preparation of the review of the Directive is an important element of this workshop. After a small introduction on general elements of the review and the scope for reviewing the Directive, Booz will present the preliminary steps of their study. The study is structured around 4 pillars: The set up of the Directive implementation, the ECI designation process, results and feedback and finally future directions. All the data collected during this study will serve the identification of gaps and points that need improvement in order to be taken on board for the review process. In this workshop only preliminary results are expected from Booz based on the time constraints and the fact that their study has only recently started.

ICT related critical Infrastructure

ICT has been debated for its importance for inclusion in a review process of the Directive. The consideration of the ICT sector is important based on its particular characteristics and also the fact that it cuts horizontally several other sectors that rely on the services of the ICT sector in order to operate (e.g. smart grids). For this reason we have foreseen a presentation on this topic in order to give to the MS the opportunity to see the difficulties related to the ICT infrastructure as an ECI. Feedback from such activities by other Commission services will be provided for further consideration by the MS.

Space Related Infrastructure

Space related infrastructure is particularly important for the functioning of several other infrastructures such as ICT, banking, transport etc. The nature of this infrastructure and its importance require special consideration by the MS and thus we have foreseen a presentation from DG ENTR for this topic. It is an opportunity for the MS to debate the importance of this infrastructure and consider its further consideration for the review of the Directive.

A general issue that MS should take into account is that both ICT and space related infrastructure can be used as driving elements for the review of the Directive not just as an extension of its scope (in other words just adding sectors).

Conclusion of the Workshop

The final part of the workshop will be used to draw conclusions, decide on the actions to carry on and also decide on the content and the items to be included for the next workshop.

For information on the contents of the workshop you can best contact:
Christian Krassnig: +32 (02) 29 86 445
Christian.KRASSNIG@ec.europa.eu

Georgios Giannopoulos: +390332786211
Georgios.GIANNOPOULOS@jrc.ec.europa.eu

For issues regarding the logistics of the workshop please contact:
Mrs. Maria Giovana Giuliani: +390332786038
Maria-Giovanna.GIULIANI@ec.europa.eu

JRC
EUROPEAN COMMISSION

ipsc
Institute for the Protection and Security of the Citizen

Sectoral and Cross-Cutting Criteria: Lessons learned and further steps-JRC input for consideration

Georgios Giannopoulos
EC, DG JRC
Unit G.6 Security Technology Assessment
email: georgios.giannopoulos@jrc.ec.europa.eu

JRC EUROPEAN COMMISSION
ipsc Institute for the Protection and Security of the Citizen

Sectoral and Cross-Cutting Criteria: Lessons learned and further steps JRC Input for consideration

Georgios Giannopoulos

IPSC - Institute for the Protection and Security of the Citizen

Ispra - Italy

http://ipsc.jrc.ec.europa.eu/

http://www.jrc.ec.europa.eu/

JRC EUROPEAN COMMISSION

Presentation outline

ipsc Institute for the Protection and Security of the Citizen

JRC 1-2 December 2011 – VI EPCIP Workshop on the Application and Implementation of the 2008/114 EC Directive

- **Rationale of cross-cutting and sectoral criteria**
- **Procedure to identify these criteria**
- **Tasks performed by JRC**
- **Experiences implementing cross-cutting and sectoral criteria**

General Framework of the Directive

- **Scope of the Directive: Designation and Assessment of the need to increase their protection**
- **Designation: Means that we have to find what is European critical and classify it as such.**
- **Assessment of the need: Related to Impact assessment to identify what are the consequences of infrastructure disruption and if existing measures are adequate**
- **Article 2(b): "…effects resulting from cross-sector dependencies on other types of infrastructures"**

Designation of ECIs

- **In order to protect ECIs you have to know what is an ECI**
  - An approach that is usually applied is **expert knowledge** (e.g. US) with **qualitative** criteria
  - Canada as well has introduced an approach that is based on **criteria**, but mostly **qualitative** (scoring)
- **The approach selected at the European level was the one of cross-cutting and sectoral criteria for the identification of ECIs (quantitative approach)**

Criteria methodology

- **Establishment of criteria: Based on impact assessments and not risk assessments**
  - **Type** of threat is not considered
  - **Probability** of threat is not considered
  - **System approach** is not obvious - implicitly in the **economic effects** (indirect losses through cascading effects)
  - No higher order **dependencies**
- **Two categories of criteria: Cross-Cutting and Sectoral**

Sectoral and Cross-Cutting Criteria

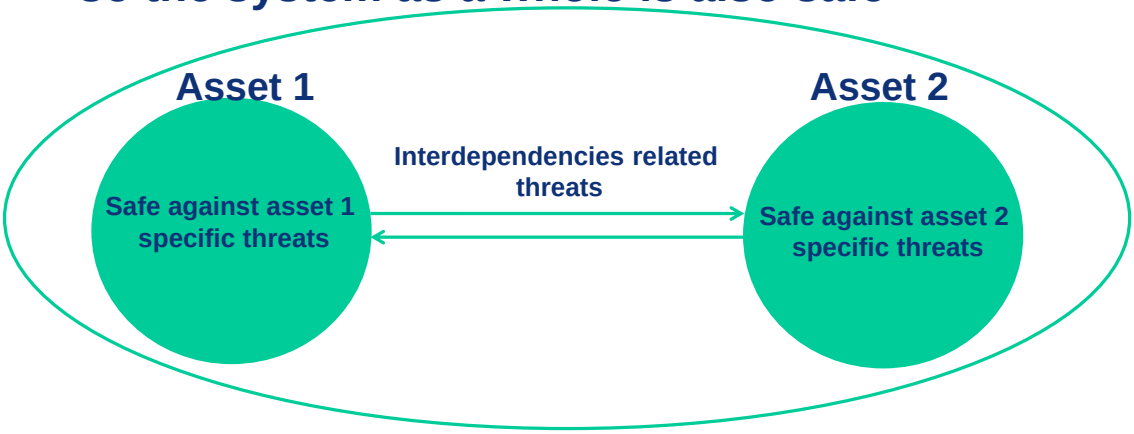
- **A mix of a bottom-up and top-down approach**
- **Bottom-Up: Sectoral criteria**
  - Criteria for each **sector**: Identifying critical infrastructures based on **assets**
  - **Interdependencies** issues were less considered
  - More focus on **sector specific threats**
  - **High sectoral criteria thresholds** may become an issue for infrastructure criticality designation
- **Top-Down: Cross-Cutting criteria**
  - **High level impacts** are considered (economic, public, casualties)
  - Certain **impact thresholds** required at European level

Sectoral and Cross Cutting Criteria (cont'd)

- **Sectoral criteria**
  - The focus is on the **assets**
  - A **European perspective** is less obvious
  - **Threat scenarios** at European level are less considered
- **Added value of sectoral approach**
  - Lots of work on different sectors
  - Detailed insight of the **infrastructure**
  - **Extensive experience** by **MS authorities**, **operators** and relevant associations
  - Consolidated knowledge that can be used for further development of a **system approach**
  - Can be considered for **resilience** measures

System vs Sectoral approach

- **General perception is that assets maybe safe so the system as a whole is also safe**



- **Although not necessarily true it is a solid base on which a system approach can be built**

Assessment of the need to be protected

- A driving force for EPCIP has been the response to terrorism
- Necessity to protect society and infrastructures from terrorist attacks
- Protection of assets is priority for terrorism
- Sectoral approach served this necessity

JRC Contribution

JRC contributed along the following lines:

- Definition of Criteria to designate ECIs
- Guidelines for the technical application of the Directive
- Preparation of a flowchart of the activities in support of the Directive
- Facilitating communication of Member States with the Commission services through regular workshops

JRC Modeling work

The modeling work by JRC has extensively contributed to the designation of critical infrastructures through:

- **Enabling establishment of criteria (both sectoral and cross-cutting)**
  - Not the concept but the relevant values
- **Development of scenarios for impact assessments**
- **Performing studies to identify vulnerabilities of sectors and selected networks**

JRC Modeling work (cont'd)

- **JRC work on modeling of networks has been mainly sectorial.**
  - Impact assessments
  - Vulnerability assessments
  - Detailed modeling of networks
- **Threats and vulnerabilities are considered at sectoral level but the consequences are expressed in terms of ccc**
  - Benchmarking with respect to economic loses
  - The identification of the criticality of certain elements of sectors has been served by these studies

Implementation workshops

Implementation workshops have served as a forum for exchanging information and best practices

- 6 workshops from June 2009 to December 2011
- Voluntary basis, participation of 90% of the Member States
- Point of contacts and sector representatives
- It is foreseen to continue with this activity

Presentations and relevant material from JRC, MS and Associations

JRC 1-2 December 2011 – VI EPCIP Workshop on the Application and Implementation of the 2008/114 EC Directive

- Analysis of vulnerability in the European electricity and gas transmission systems
- Electricity : Cybersecurity of Power Systems
- Gas: European Security issues - views of the GIE security group
- Modelling and analysis of the impact of CI on the Fast Moving Consumer Goods Supply Chain
- Air traffic control: presentations of ENAV and Eurocontrol and DG MOVE
- Resilience presentation

Observations based on the criteria approach

- **Designation of a limited number of ECIs in few MS**
  - Energy Sector
  - No ECIs from transport sector
- **Risk analysis and all hazards approach seem to be less obvious**
- **Increased awareness in MS and stakeholders for threats and vulnerabilities of CIs**
- **Positive side effects at national level and CIP programs**
- **A better view of the impact of disruption of CIs at European level**

JRC EUROPEAN COMMISSION
ipsc Institute for the Protection and Security of the Citizen
JRC 1-2 December 2011 – VI EPCIP Workshop on the Application and Implementation of the 2008/114 EC Directive

Thank you for your attention!!!

JRC
EUROPEAN COMMISSION

ipsc
Institute for the Protection and Security of the Citizen

A Reference Security Management Plan [RSMP] for Energy Infrastructure Assets

Jose Antonio Hoyos Perez
EC, DG ENER
Unit B.1 Energy Policy, Security of Supply and Networks
email. joseantonio.hoyosperez@ec.europa.eu

A Reference Security Management Plan [RSMP] for Energy Infrastructure Assets

6th EPCIP-Directive 2008/114 Workshop
Ispra 1-2 Dec 2011

José A. Hoyos Pérez, DG Energy

Directorate-General for Energy
EUROPEAN COMMISSION

Context for the RSMP

- The reliability of energy infrastructure is essential to the supply of energy across the European Union and beyond
- Security aims to take *prevention, mitigation* and *responsive measures* to ensure:

Asset Integrity → **Reliability of Supply** → **Impacts:CCC** →

- So energy is a priority sector for the **European Programme for Critical Infrastructure Protection [EPCIP]**
- One requirement is an '**Operator's Security Plan**' for all 'European Critical' infrastructure
- DG Energy commissioned a **guidebook** to aid the preparation of security startegies for **all operators**, regardless of whether the asset was designated as ECI or not
- The RSMP is the name of this guidebook and was prepared by an external contractor following a competitive tendering process

Directorate-General for Energy
EUROPEAN COMMISSION

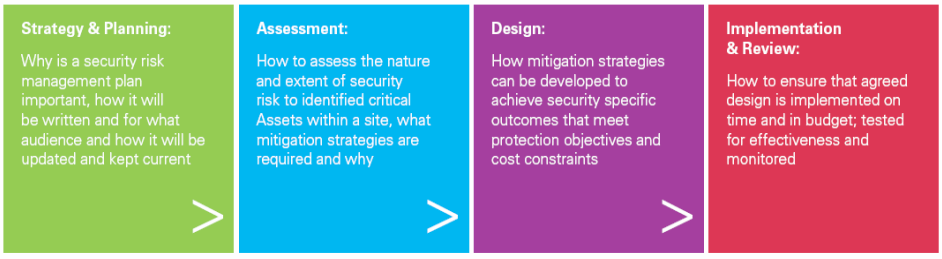
Principles behind the RSMP

- The RSMP is designed to:
  - **Look at all the elements** that create and shape the threat environment around a facility with good risk identification, measurement, evaluation, mitigation and monitoring.
  - **Be applied anywhere in the world to any asset,** so there is assurance that security threats to a facility/site/company are being managed on a consistent basis.
  - **Define a benchmark for good risk assessment and design** which can include existing material used in a company or unify what can be a fragmented process.
  - Create an **audit trail of decision making** that meets internal control requirements.
  - Ensure risk mitigation is **performance-led and delivers value for money** so risks are reduced at a cost a company feels is right or a government is happy to fund.
  - Include a **complete reporting and monitoring model** to encompass both implementation and change thereafter.

In sum, all the key elements of any good risk management framework

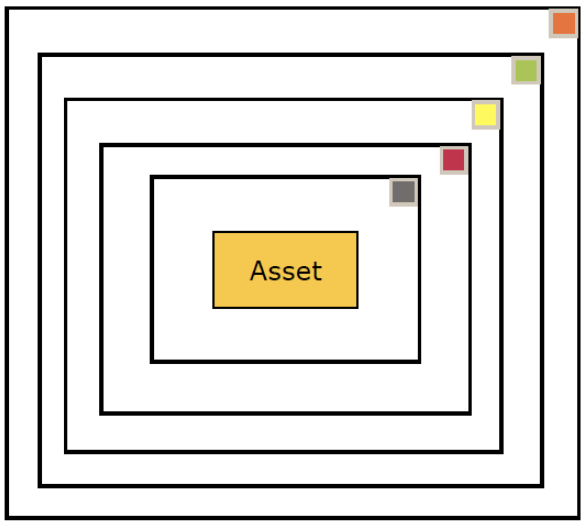
Structure of the RSMP

- The RSMP is based on a process called **PRISM®** [*Performance & Risk-based Integrated Security Methodology*] which has four phases:



- Each phase is distinct but generates the outcome for the next phase – so it has to be **completed in full**
- It can be **tailored to an existing security risk management approach** joining elements together into a visible and aligned process
- PRISM won an award in 2011 from the **Institute of Risk Management** as the comprehensive security risk methodology developed to date

Stakeholder interests are a challenge



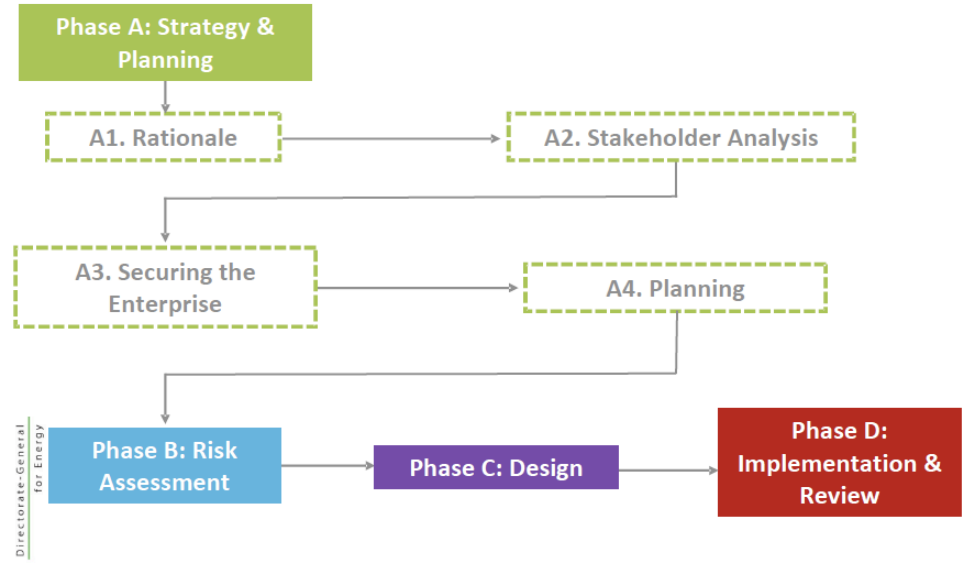
- Asset Owner
- Police & Emergency Services
- Government agencies
- Ministries/National Governments
- International organisations: NATO, EU, ISOs etc
- Stakeholders

Directorate-General for Energy

…the **Asset Owner** remains responsible for the risk and its consequences…..

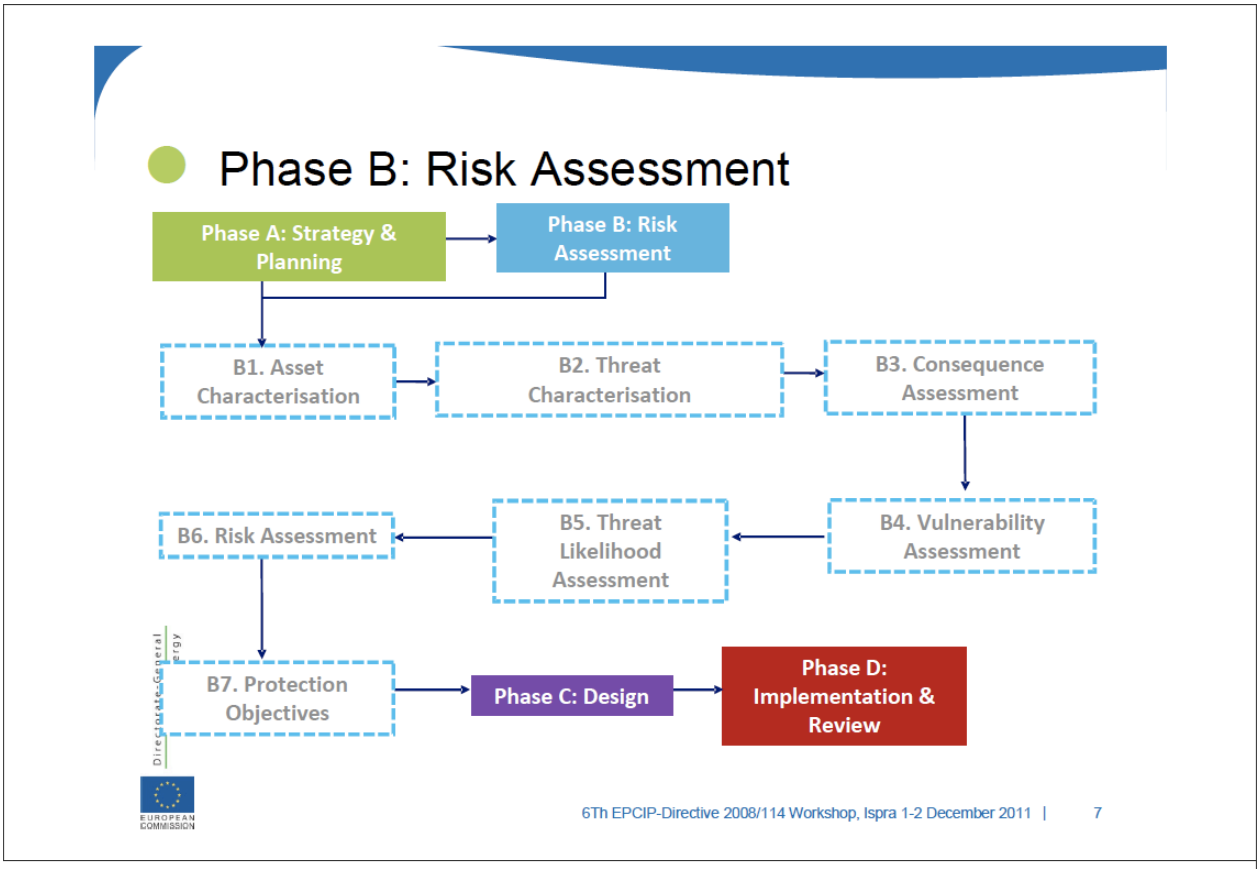
EUROPEAN COMMISSION

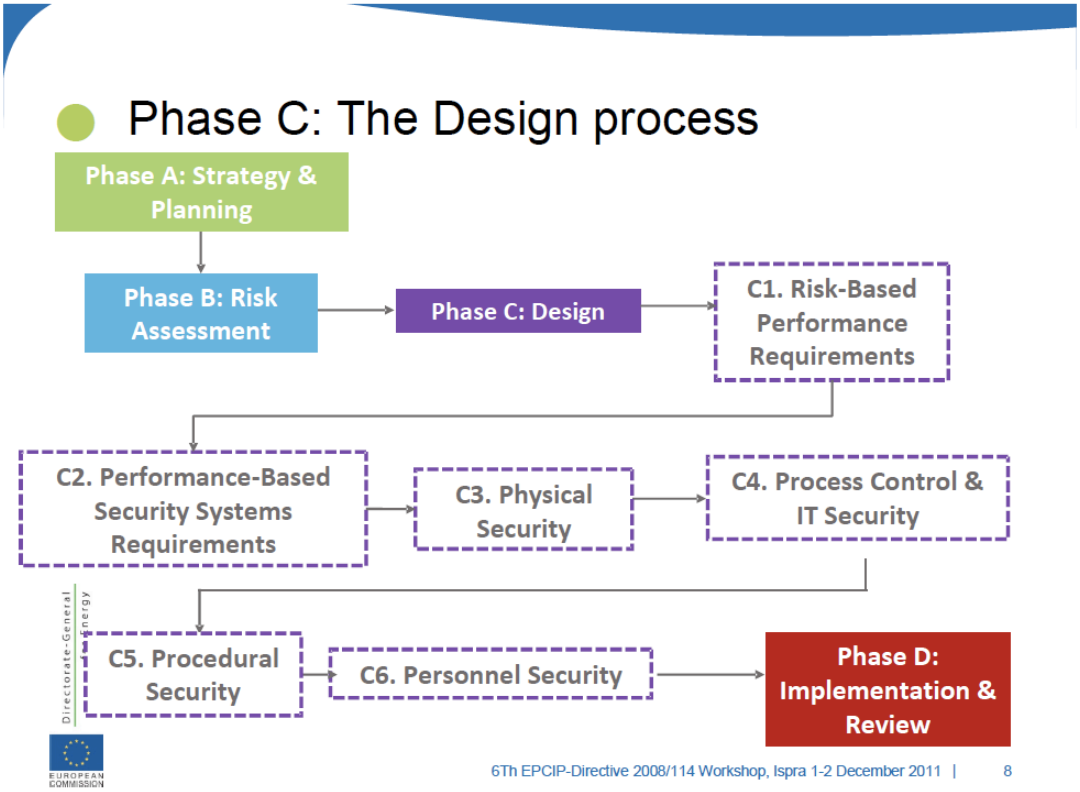
Phase A: Strategy & Planning



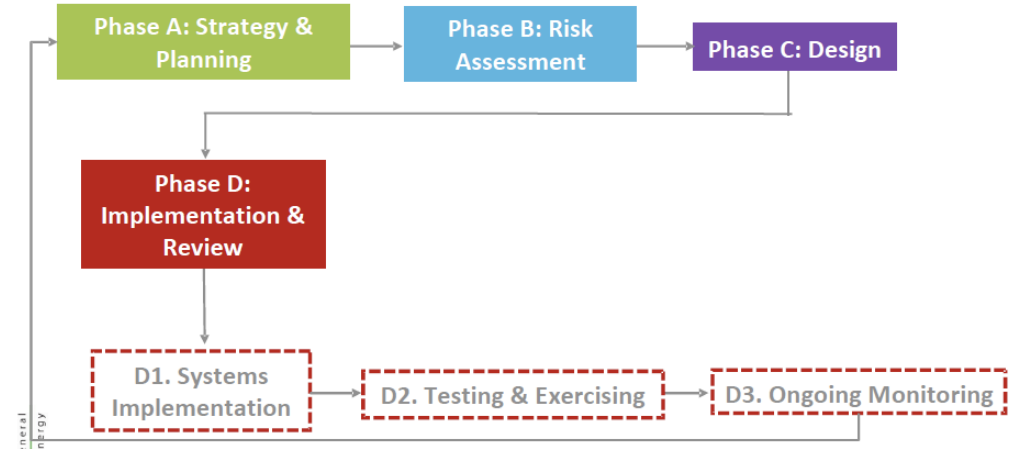
Directorate-General for Energy

EUROPEAN COMMISSION


Phase B: Risk Assessment
Phase A: Strategy & Planning
Phase B: Risk Assessment
B1. Asset Characterisation
B2. Threat Characterisation
B3. Consequence Assessment
B4. Vulnerability Assessment
B5. Threat Likelihood Assessment
B6. Risk Assessment
B7. Protection Objectives
Phase C: Design
Phase D: Implementation & Review
Directorate-General Energy
EUROPEAN COMMISSION
6Th EPCIP-Directive 2008/114 Workshop, Ispra 1-2 December 2011 | 7


Phase C: The Design process
Phase A: Strategy & Planning
Phase B: Risk Assessment
Phase C: Design
C1. Risk-Based Performance Requirements
C2. Performance-Based Security Systems Requirements
C3. Physical Security
C4. Process Control & IT Security
C5. Procedural Security
C6. Personnel Security
Phase D: Implementation & Review
Directorate-General Energy
EUROPEAN COMMISSION
6Th EPCIP-Directive 2008/114 Workshop, Ispra 1-2 December 2011 | 8

Phase D: Implementation & Review



Directorate-General for Energy

Value of the RSMP

- This can be summed by looking at Risk and Performance:

RISK

1. An understanding of the **specific risks** facing each facility
2. Scenario-based to identify **specific incidents or methods** that need to be mitigated
3. Risks considered at the **component** as well at **site level** to focus on specific critical components and processes which must be protected
4. Scoring that enable specific **Protection Objectives** to be derived

PERFORMANCE

1. The **level and type** of performance required to mitigate specific risks from the measures identified as meeting Protection Objectives
2. Allows users to understand and identify **their own performance requirements** in the areas vital to effective security the core functions of which are:

Detection – Delay – Response-Emergency planning

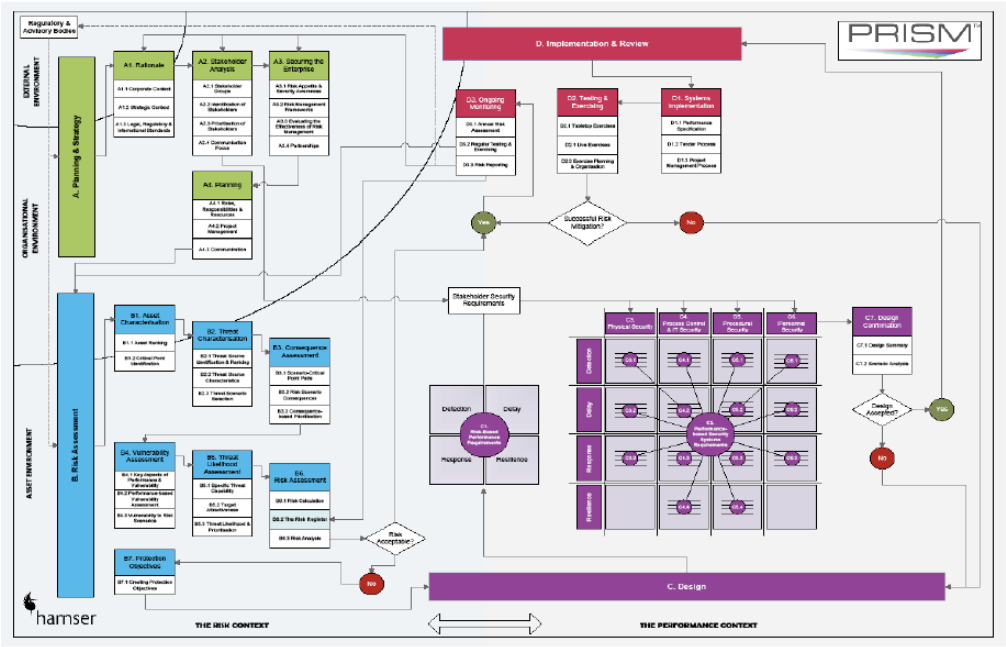
Directorate-General for Energy

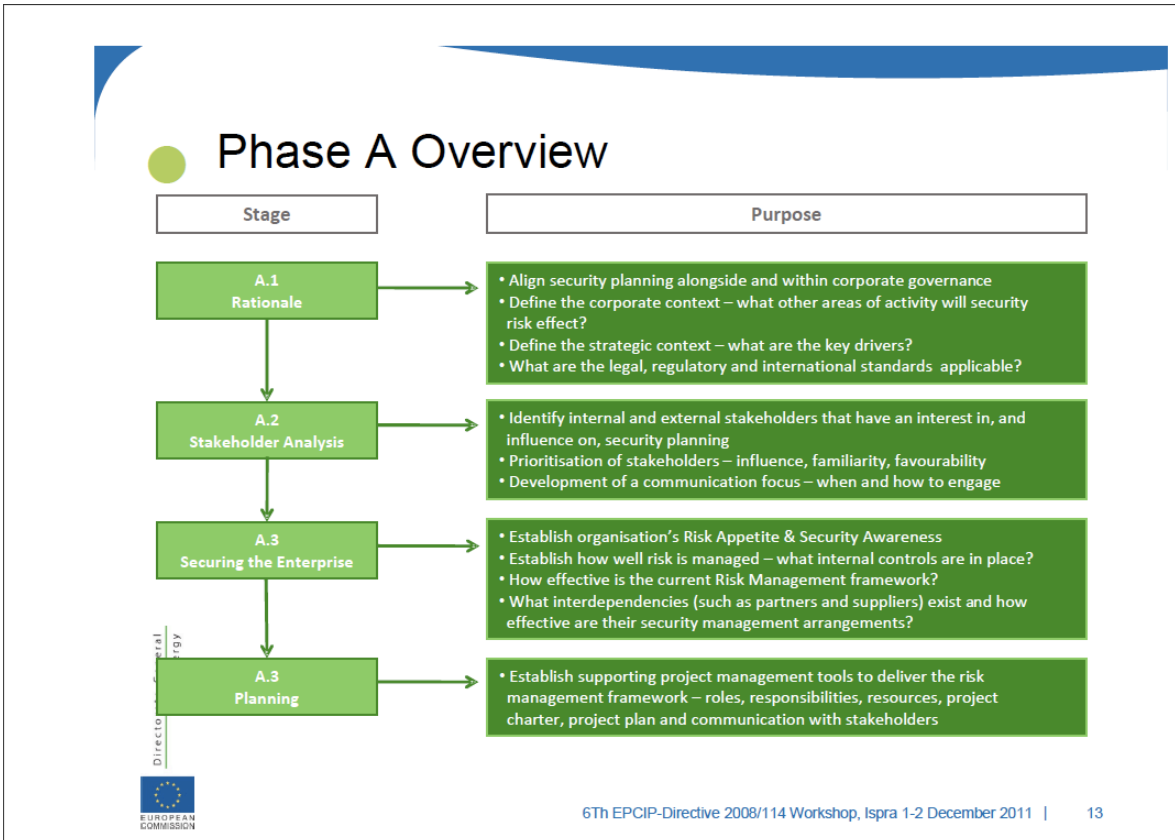
In Conclusion

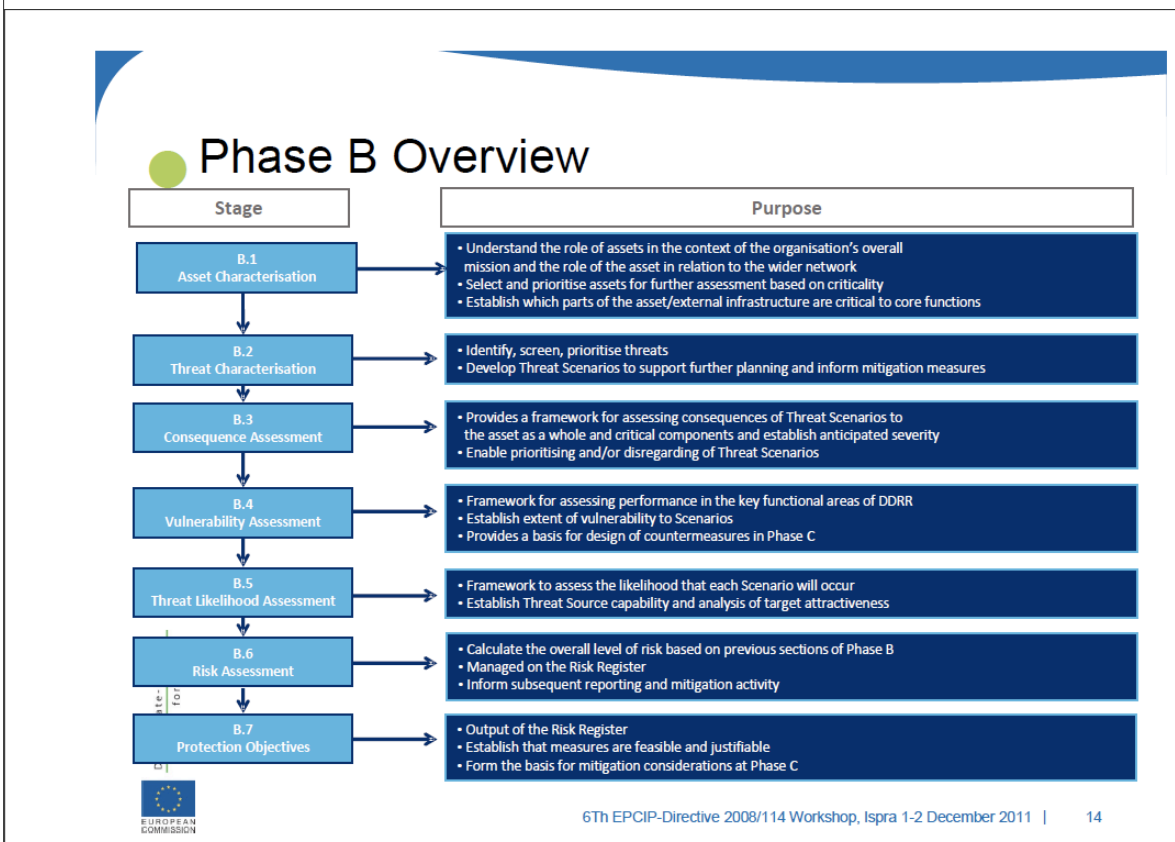
- The **reliability of energy infrastructure to the supply of energy** is critical
- It is a sector given Commission **priority** under the EPCIP
- The RSMP has been prepared **to aid** owners/operators apply a comprehensive security risk management process to all energy infrastructure assets
- Security risks do impact upon the supply chain and all parties need to have robust and effective Security Plans that deal with risks **in a consistent manner**
- So I would commend use of the RSMP as **a guidebook** against which your existing Security Plans, and the environment they have to function in, to be checked
- Electronic copies of the RSMP as available on our website free of charge or at www.prismworld.org where you can also obtain a hard copy at cost price

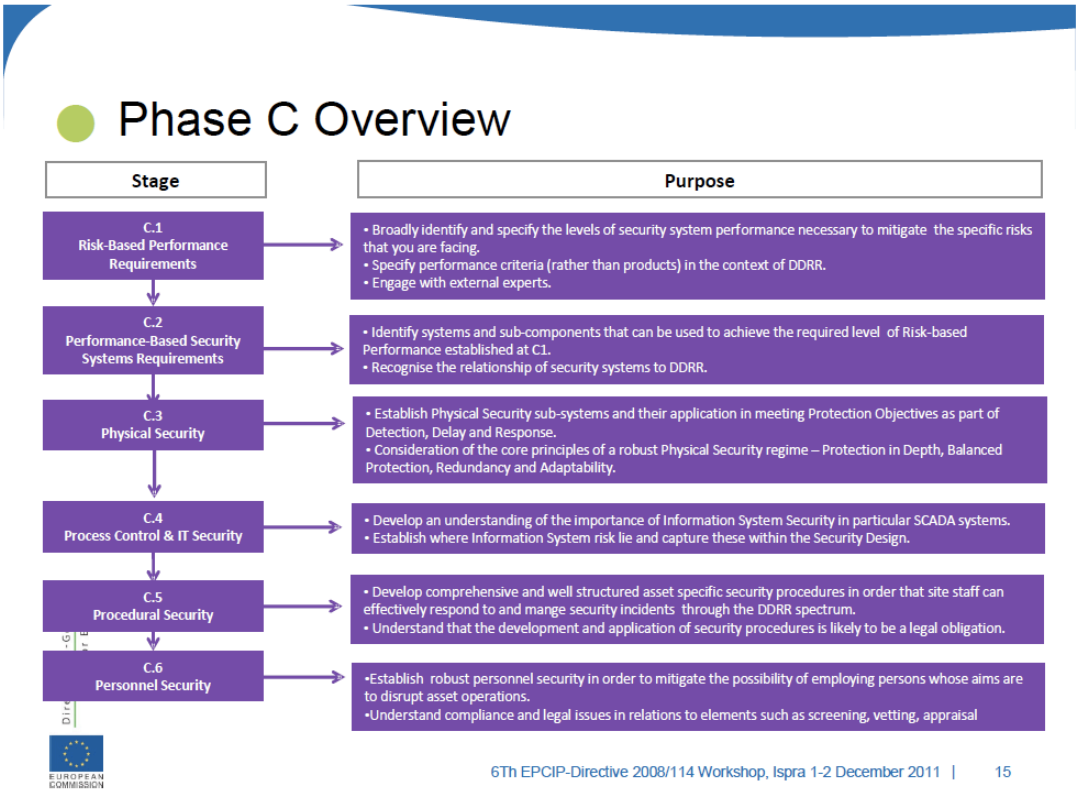
Directorate-General for Energy
EUROPEAN COMMISSION

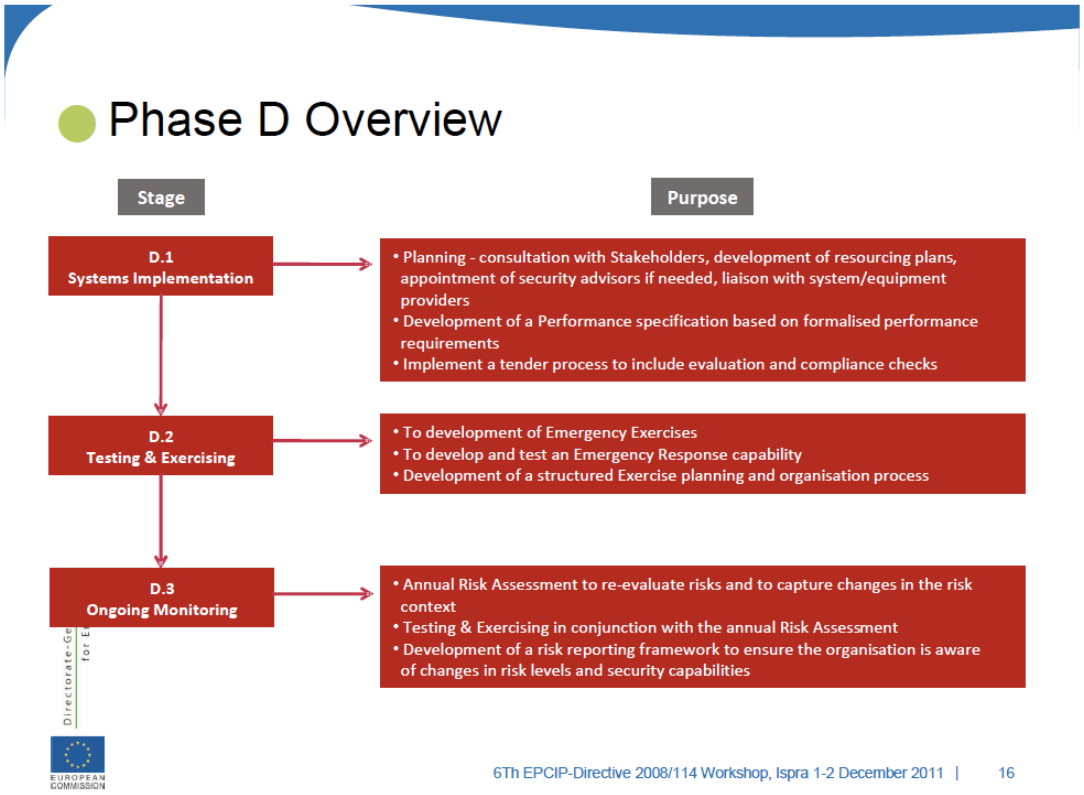
PRISM Process Overview




Phase A Overview
Stage
Purpose
A.1
Rationale
• Align security planning alongside and within corporate governance
• Define the corporate context – what other areas of activity will security risk effect?
• Define the strategic context – what are the key drivers?
• What are the legal, regulatory and international standards applicable?
A.2
Stakeholder Analysis
• Identify internal and external stakeholders that have an interest in, and influence on, security planning
• Prioritisation of stakeholders – influence, familiarity, favourability
• Development of a communication focus – when and how to engage
A.3
Securing the Enterprise
• Establish organisation's Risk Appetite & Security Awareness
• Establish how well risk is managed – what internal controls are in place?
• How effective is the current Risk Management framework?
• What interdependencies (such as partners and suppliers) exist and how effective are their security management arrangements?
A.3
Planning
• Establish supporting project management tools to deliver the risk management framework – roles, responsibilities, resources, project charter, project plan and communication with stakeholders
EUROPEAN COMMISSION
6Th EPCIP-Directive 2008/114 Workshop, Ispra 1-2 December 2011 | 13


Phase B Overview
Stage
Purpose
B.1
Asset Characterisation
• Understand the role of assets in the context of the organisation's overall mission and the role of the asset in relation to the wider network
• Select and prioritise assets for further assessment based on criticality
• Establish which parts of the asset/external infrastructure are critical to core functions
B.2
Threat Characterisation
• Identify, screen, prioritise threats
• Develop Threat Scenarios to support further planning and inform mitigation measures
B.3
Consequence Assessment
• Provides a framework for assessing consequences of Threat Scenarios to the asset as a whole and critical components and establish anticipated severity
• Enable prioritising and/or disregarding of Threat Scenarios
B.4
Vulnerability Assessment
• Framework for assessing performance in the key functional areas of DDRR
• Establish extent of vulnerability to Scenarios
• Provides a basis for design of countermeasures in Phase C
B.5
Threat Likelihood Assessment
• Framework to assess the likelihood that each Scenario will occur
• Establish Threat Source capability and analysis of target attractiveness
B.6
Risk Assessment
• Calculate the overall level of risk based on previous sections of Phase B
• Managed on the Risk Register
• Inform subsequent reporting and mitigation activity
B.7
Protection Objectives
• Output of the Risk Register
• Establish that measures are feasible and justifiable
• Form the basis for mitigation considerations at Phase C
EUROPEAN COMMISSION
6Th EPCIP-Directive 2008/114 Workshop, Ispra 1-2 December 2011 | 14


Phase C Overview
Stage
Purpose
C.1
Risk-Based Performance Requirements
• Broadly identify and specify the levels of security system performance necessary to mitigate the specific risks that you are facing.
• Specify performance criteria (rather than products) in the context of DDRR.
• Engage with external experts.
C.2
Performance-Based Security Systems Requirements
• Identify systems and sub-components that can be used to achieve the required level of Risk-based Performance established at C1.
• Recognise the relationship of security systems to DDRR.
C.3
Physical Security
• Establish Physical Security sub-systems and their application in meeting Protection Objectives as part of Detection, Delay and Response.
• Consideration of the core principles of a robust Physical Security regime – Protection in Depth, Balanced Protection, Redundancy and Adaptability.
C.4
Process Control & IT Security
• Develop an understanding of the importance of Information System Security in particular SCADA systems.
• Establish where Information System risk lie and capture these within the Security Design.
C.5
Procedural Security
• Develop comprehensive and well structured asset specific security procedures in order that site staff can effectively respond to and mange security incidents through the DDRR spectrum.
• Understand that the development and application of security procedures is likely to be a legal obligation.
C.6
Personnel Security
•Establish robust personnel security in order to mitigate the possibility of employing persons whose aims are to disrupt asset operations.
•Understand compliance and legal issues in relations to elements such as screening, vetting, appraisal
EUROPEAN COMMISSION
6Th EPCIP-Directive 2008/114 Workshop, Ispra 1-2 December 2011 | 15


Phase D Overview
Stage
Purpose
D.1
Systems Implementation
• Planning - consultation with Stakeholders, development of resourcing plans, appointment of security advisors if needed, liaison with system/equipment providers
• Development of a Performance specification based on formalised performance requirements
• Implement a tender process to include evaluation and compliance checks
D.2
Testing & Exercising
• To development of Emergency Exercises
• To develop and test an Emergency Response capability
• Development of a structured Exercise planning and organisation process
D.3
Ongoing Monitoring
• Annual Risk Assessment to re-evaluate risks and to capture changes in the risk context
• Testing & Exercising in conjunction with the annual Risk Assessment
• Development of a risk reporting framework to ensure the organisation is aware of changes in risk levels and security capabilities
EUROPEAN COMMISSION
6Th EPCIP-Directive 2008/114 Workshop, Ispra 1-2 December 2011 | 16

Phase D Overview

Stage	Purpose
D.1 Systems Implementation	• Planning - consultation with Stakeholders, development of resourcing plans, appointment of security advisors if needed, liaison with system/equipment providers • Development of a Performance specification based on formalised performance requirements • Implement a tender process to include evaluation and compliance checks
D.2 Testing & Exercising	• To development of Emergency Exercises • To develop and test an Emergency Response capability • Development of a structured Exercise planning and organisation process
D.3 Ongoing Monitoring	• Annual Risk Assessment to re-evaluate risks and to capture changes in the risk context • Testing & Exercising in conjunction with the annual Risk Assessment • Development of a risk reporting framework to ensure the organisation is aware of changes in risk levels and security capabilities

Directorate-General for Energy
EUROPEAN COMMISSION

Download RSMP

http://ec.europa.eu/energy/infrastructure/studies/doc/2010_rsmp.pdf

http://ec.europa.eu/energy/infrastructure/critical_en.htm

Directorate-General for Energy
EUROPEAN COMMISSION

THANK YOU!

José Antonio Hoyos Pérez
Policy Officer, Critical Energy Infrastructure Protection
Directorate-General for Energy

joseantonio.hoyosperez@ec.europa.eu

Directorate-General for Energy
EUROPEAN COMMISSION

JRC
EUROPEAN COMMISSION

ipsc
Institute for the Protection and Security of the Citizen

Study to Support the Preparation of the Review of Directive 2008/114/EC

Das-Purkayastha Arindam
Booz&Co

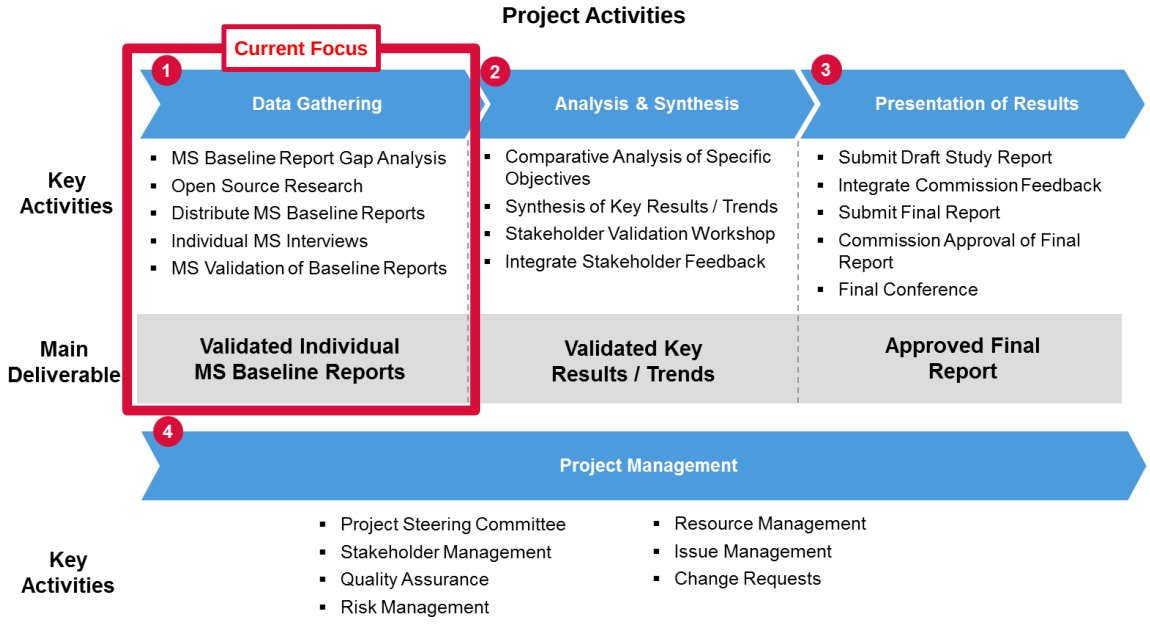
Booz & Company Ispra, 1 December 2011 Discussion Document

booz&co.

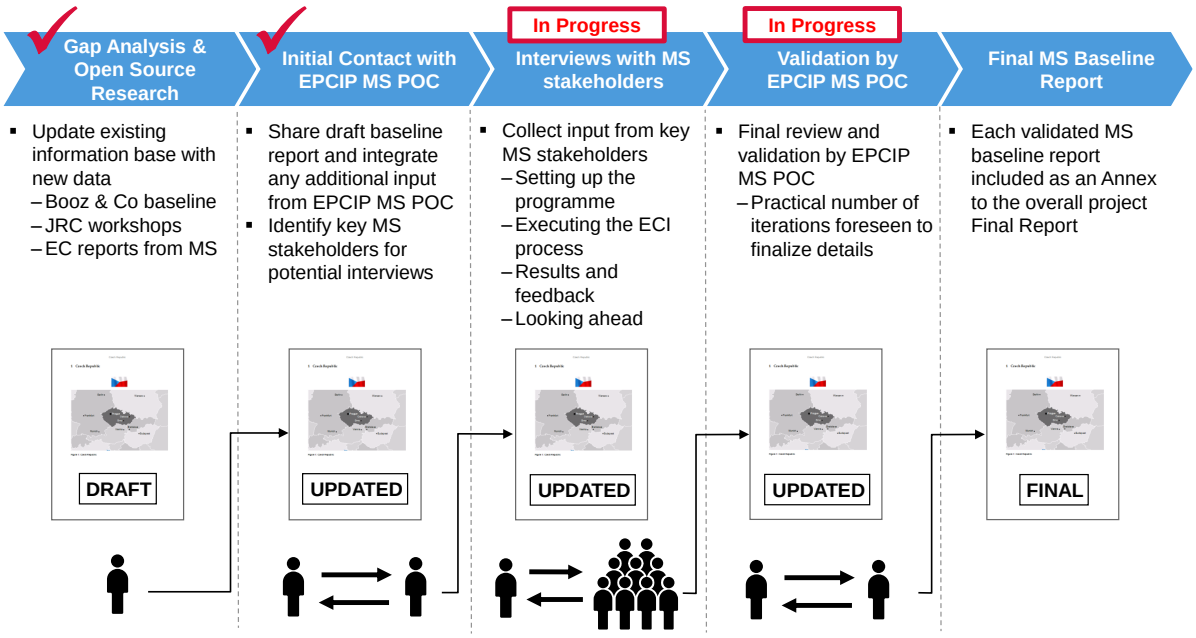
Study to Support the Preparation of the Review of Directive 2008/114/EC

Project Status

The project is currently on schedule in the data gathering phase



Data gathered through open source research and stakeholder interviews is being validated by EPCIP MS Contact Points



We will continue the interview process through mid-January – no major delays encountered so far

Status of Data Gathering Interviews

- **16 Face-to-Face Interviews**
  - 6 completed
  - 5 scheduled for December/Early January
  - 4 currently being scheduled
  - 1 raised concern about the process
- **12 Telephone Interviews**
  - 1 completed
  - 6 scheduled for December/January
  - 5 not responded

Member State Participation			
● European Commission	● Estonia	● Italy	● Portugal
● Austria	● Finland	● Latvia	● Romania
● Belgium	● France	● Lithuania	● Slovakia
● Bulgaria	● Germany	● Luxemburg	● Slovenia
● Cyprus	● Greece	● Malta	● Spain
● Czech Republic	● Hungary	● Netherland	● Sweden
● Denmark	● Ireland	● Poland	● UK

●: Engaged ●: Not Responded

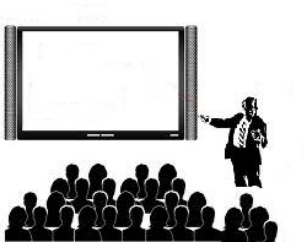
Next key steps requiring stakeholders participation are validation workshop and final conference to disseminate the results

Validation Workshop

- Date: tbd Location: tbd
- **Interactive workgroup setting** intended to foster discussion on key points
- Primary **focus on EPCIP MS POC's** and select additional stakeholders
- Input **integrated into final study report**

Final Conference

- Date: tbd Location: tbd
- **Dissemination setting** intended to "broadcast" results (sanitized if needed)
- Open to **wider group of MS stakeholders**
- Presentation of final results – **no further updates / modification** of study results



Early trend indicates common approach to implementation along with shared concern about adding ICT in the Directive scope

General Trend based on completed interviews

Setting Up the Program	Executing the ECI Process	Results and Feedback	Looking Ahead
▪ Majority of MS implemented provisions of the Directive through legislative changes, except 2 MS ▪ Directive, in few cases helped establish and strengthen national CIP activities ▪ In all the MS the same actors were involved in national CIP and ECI activities	▪ Smaller MS expressed concern on absolute value of criteria thresholds ▪ Issue of external dimension of alternatives will benefit from clarity i.e. can non-EU alternatives be considered? ▪ Transboundary impact could not be confidently evaluated without engaging with the affected MS	▪ Potential ECIs were far fewer in the Transport sector, when compared to Energy sector ▪ Directive has helped add CIP focus in the cooperation between MS ▪ Most MS cite better cooperation as contributing to improved security, while others say such conclusion is anecdotal and should be evidence based	▪ Some MS suggest to assess threats at the EU level based on inputs from MS ▪ Some MS support inclusion of ICT in scope, while others want evidence of tangible benefit in Ener & Tran sector prior to inclusion. All agree sector boundary is hard to specify. ▪ Opinion on addition of other sectors in scope of Directive is largely undecided

JRC
EUROPEAN COMMISSION

ipsc
Institute for the Protection and Security of the Citizen

State of play on Critical Information Infrastructure Protection - CIIP

Prepared by Andrea Servida
EC, DG INFSO
Unit A.3 Internet; Network and Information Security

Presented by Christian Krassnig
EC, DG HOME
Unit A.1 Crisis Management and Fight Against Terrorism
email. christian.krassnig@ec.europa.eu

State of play on Critical Information Infrastructure Protection - CIIP
"Achievements and next steps: towards global cyber-security"

Andrea SERVIDA
European Commission
Directorate General
Information Society and Media - DG INFSO
Unit A3 – Internet Governance; Network and Information Security
andrea.servida@ec.europa.eu

CIIP COM(2011)163
"Achievements and next steps: towards global cyber-security"

New communication on CIIP adopted on 31 March 2011 – CIIP COM(2011)163:

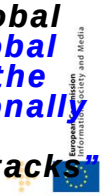
- **Takes stock** of results achieved since the 2009 Communication setting-up the "CIIP action plan"
- **Builds** on existing policy initiatives, in particular **Digital Agenda**, **Stockholm Action Plan** and **Internal Security Strategy**
- **Describes** next steps at **European** and **International** level

CIIP COM(2011)163
"Achievements and next steps: towards global cyber-security"

- **The threats scenario is evolving and sees the emergence of new motivations:**
  - **exploitation purposes** (e.g. GhostNet, European Trade System, recent attacks against government systems and EU Institutions)
  - **disruption purposes** (e.g. Conficker, StuxNet, submarine cable breaks)
  - **destruction purposes** (fortunately not yet materialised)

CIIP COM(2011)163
"Achievements and next steps: towards global cyber-security"

- **EU and the global context**
  - **A purely European approach is not sufficient and needs to be embedded into a global coordination strategy**
  - **The Digital Agenda for Europe calls for the "*cooperation of relevant actors […] to be organised at global level to be effectively able to fight and mitigate security threats*" and sets out the goal to "*work with global stakeholders notably to strengthen global risk management in the digital and in the physical sphere and conduct internationally coordinated targeted actions* against *computer-based crime and security attacks*"**



CIIP COM(2011)163

"Achievements and next steps: towards global cyber-security"

Areas of achievements

- **European Forum for Member States (EFMS) to discuss CIIP between national competent authorities**
- **European Public-private Partnership for Resilience (EP3R)**
- **Baseline of capabilities and services for pan-European cooperation of national/governmental CERTs**
- **European Information Sharing and Alert System (EISAS)**
- **National contingency planning and exercises**
- **Pan-European exercise on large-scale network security incidents**
- **Internet resilience and stability**
- **Sector specific criteria for identifying European Critical Infrastructures in the ICT sector**

CIIP COM(2011) 163

"Achievements and next steps: towards global cyber-security"

The way forward (1/2)

- **Very positive results** achieved so far in CIIP within the EU
- **Further efforts are needed** and the EC calls upon MS to **commit** to:
  - Enhance EU preparedness by establishing a **network of well-functioning National/Governmental CERTs by 2012;**
  - A **European cyber-incident contingency plan** and **regular National and pan-European cyber exercises** by 2012**;**
  - **European coordinated efforts in international fora** and discussions on enhancing **Internet security and resilience.**

CIIP COM(2011) 163

"Achievements and next steps: towards global cyber-security"
The way forward (2/2)

- **Global coordination is important and necessary**
- The Commission will:
  - Promote **principles for Internet resilience and stability*** developed within the EFMS;
  - Build **strategic international partnerships** (e.g. EU-US Working Group on Cyber-security and Cyber-crime) and pursue coordination in International *fora*
  - Develop **trust in the cloud**

**http://ec.europa.eu/information_society/policy/nis/docs/principles_ciip/guidelines_internet_fin.pdf*

Follow-up to the 2011 CIIP Communication

- **CIIP Ministerial Conference** in Balatonfüred 04/2011
  - Political commitment to **enhance EU cooperation** and to **reinforce coordination and cooperation at the International level**
- **Council Conclusions on CIIP of May 2011 invite stakeholders to:**
  - Participate in PPP for the development of resilient and secure networks and reinforce multi-stakeholder dialogue and understanding
  - Support the Member States in their efforts to develop national cyber-incident contingency plans and to organise cyber exercises
  - Participate in the establishment and take up of minimum requirements and generally internationally recognized standards on network and information security

Definition of sectoral criteria to identify ECIs in the ICT sector

Policy context & Scope

- **Policy context**
  - **EU Council Directive 2008/114/EC on the identification and designation of European Critical Infrastructures (ECI)**
    - Scope in 2008: Energy and Transport Sectors
    - Use of sectoral criteria to identify ECI (defined by EC and MS)
  - **5th pillar of the 2009 CIIP Action Plan = Develop proposal for ICT criteria**
- **Scope of the proposal**
  - **For the time being the sub-sectors under focus are Internet, fixed and mobile telecommunications**

Definition of sectoral criteria to identify ECIs in the ICT sector

Objectives of the process

1. **Contribute to a better collective understanding of what is meant by Critical Information Infrastructures as a basis for enhanced EU collaboration and coordination in the CIIP area**
2. **Be prepared with a technical proposal of ICT criteria in case of extension of the ECI Directive to the ICT sector.**

Definition of sectoral criteria to identify ECIs in the ICT sector

General remark / clarification

- The process / discussion with Member States under the European Forum for Member States (EFMS) and with private sector under the European Public-Private Partnership for resilience (EP3R) is not on the review of the ECI Directive.
  → Discussion and decision in the Council
- In case the Council decides to extend the Directive, we would have a technical proposal on ICT criteria. This proposal will be without prejudice to the Council decision.
- The readiness of a technical proposal on ICT criteria should not be the basis for the decision to extend the ECI Directive to the ICT sector.

Development of a non-paper on ICT criteria to identify ECIs in the ICT sector

Milestones – Consultation with MS and private sector

Jun 2009 – Jun 2010	Study to support the process to define ICT criteria focusing on Internet, fixed and mobile coms
23 Jun 2010	Initial non-paper on the process to define sectoral criteria to identify ECIs in the ICT sector presented and discussed at 4th EFMS meeting
12 Oct 2010	Non-paper on sectoral criteria to identify ECI in the ICT sector - Version 1.0 presented and discussed at the 5th EFMS meeting
21 Jan 2010	Presentation of synthesis of feedbacks on the non-paper on ICT criteria at the 6th EFMS meeting
22 Feb 2011	Non-paper on sectoral criteria to identify ECI in the ICT sector - Version 2.0 – Approved by MS for discussion with private sector under EP3R
16-17 Mar 2011	Presented and discussed at EP3R meeting (WG1)
05-06 July 2011	Discussion with ISPs and within EP3R – Written feedbacks requested by 15 Aug 2011

Development of a non-paper on ICT criteria to identify ECIs in the ICT sector

State of play of received feedbacks and next steps

- **Written feedbacks on the last version of the non-paper received from**
  - **Member States: DE, FI, NO, RO, UK**
  - **Private sector: CENTR, eco, EURid, netnod, RIPE NCC, Symantec, Telefonica, Joint response from 6 European ISPs,**
    Results of discussion with DK ISPs summarised by DK National IT and Telecom Agency,
    Results of discussion with SE ISPs summarised by PTS
  - **Private research institute: Formit**
- **Analysis of input and revision of the non-paper is on-going.**
- **Alignment of revised non-paper will follow later this autumn 2011 and finalisation is expected by end of 2011 / early 2012.**

Non-paper on ICT criteria – Feedbacks on the proposed approach (1/4)

- **Asset-based approach of the ECI Directive is challenged**
  - **Limitations have been discussed**
    - **Asset approach could be a start, but further study should be conducted on alternatives. There were also concerns that the asset approach is not appropriate at all.**
  - **Alternative approaches (like risk management) should (also) be considered**
  - **Simplicity approach is agreeable**
  - **Feedback from energy and transport sector would be helpful**

Non-paper on ICT criteria – Feedbacks on the proposed approach (2/4)

- **Criticality**
  - People, procedures and systems to be considered
  - Analysis of criticality is an ongoing process
  - Resilience vs. criticality:
    - *"Would it be possible to buy free from being labelled >critical< by putting resilience measures in place?"*

Non-paper on ICT criteria – Feedbacks on the proposed approach (3/4)

- **Scope**
  - Kind of networks to be considered should be defined
    - Public and/or private networks
    - Possibly following the definition in the Framework Directive on electronic communications
  - Global dimension so far not addressed
  - Interdependencies between and within the CI sectors

Non-paper on ICT criteria – Feedbacks on the proposed approach(4/4)

- **Beyond the ECI Directive**
  - There are challenges which cannot be captured by the Directive.
    - *"The simultaneous failure of infrastructures cannot be addressed following the logic of the ECI directive."*
  - Proposal to complement the approach of the Directive
    - In practice: Insert further chapter to the non-paper collecting what goes beyond the Directive

State of play on CIIP

"Achievements and next steps: towards global cyber-security"

Thanks!

Web Sites

- EU policy on Critical Information Infrastructure Protection – CIIP
  http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm
- A Digital Agenda for Europe
  http://ec.europa.eu/information_society/digital-agenda/index_en.htm
- EU policy on promoting a secure Information Society
  http://ec.europa.eu/information_society/policy/nis/index_en.htm
- European principles and guidelines for Internet resilience and stability
  http://ec.europa.eu/information_society/policy/nis/docs/principles_ciip/guidelines_internet_fin.pdf

Links to policy documents

- Council conclusions on Critical Information Infrastructure Protection
  http://register.consilium.europa.eu/pdf/en/11/st10/st10299.en11.pdf
- Commission Communication on Critical Information Infrastructure Protection – "Achievements and next steps: towards global cyber-security" - COM(2011) 163
  http://ec.europa.eu/information_society/policy/nis/docs/comm_2011/comm_163_en.pdf
- Digital Agenda for Europe - COM(2010)245 of 19 May 2010
  http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF
- The EU Internal Security Strategy in Action: Five steps towards a more secure Europe COM(2010)673
  http://ec.europa.eu/commission_2010-2014/malmstrom/archive/internal_security_strategy_in_action_en.pdf
- Commission Communication on Critical Information Infrastructure Protection – "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" - COM(2009) 149
  http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF

Space and CIP

Antoine Kopp
EC, DG ENTR
Unit H.1 Space Policy and Coordination
email: antoine.kopp@ec.europa.eu

JRC EUROPEAN COMMISSION

ipsc Institute for the Protection and Security of the Citizen

6th EPCIP workshop

Ispra, 1-2 December 2011

Space and CIP

Antoine Kopp
Unit H1 – Space Policy and Coordination

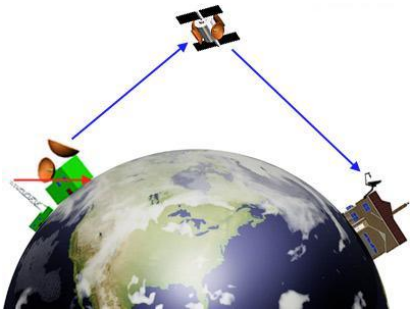
European Commission
Enterprise and Industry

The space sector (1)

- System enabling the
  - transmission
  - gathering

  of data via relay stations and infrastructures orbiting around the planet

- Situation in space enables much broader coverage than land-based systems



The space sector (2)

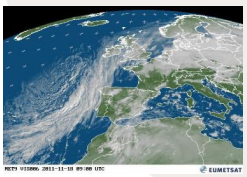
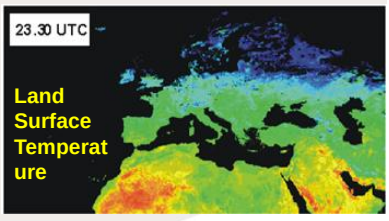
- Three main physical segments
  - Space segment - satellites
  - Launchers and space port
  - Ground segments – receivers, antennas, transmitters/transponders, control stations




- Data flow from ground station to satellite and back

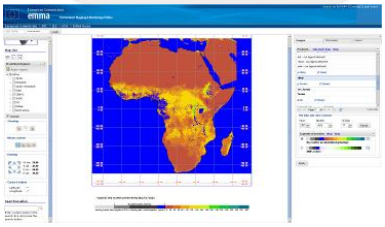
The space sector (3)

- Three main areas of activity
  - Navigation and positioning: GPS, Galileo
  - Earth observation: GMES, EUMETSAT
  - Communications: data transfer, phone, TV, internet


The space sector (4)

- Space applications have become truly ubiquitous
- Essential for economy and every day life
  - Transport – optimization via satellite navigation
  - Meteorology
  - Agriculture – “precision farming” by mapping of crop land for irrigation and harvest forecast
  - Fisheries – surveillance of stocks
  - Communication networks, particularly in remote areas
  - Crisis and emergency response
  - Environmental observation
  - Synchronisation of networks
  - Border protection
  - Remote medical support
  - …



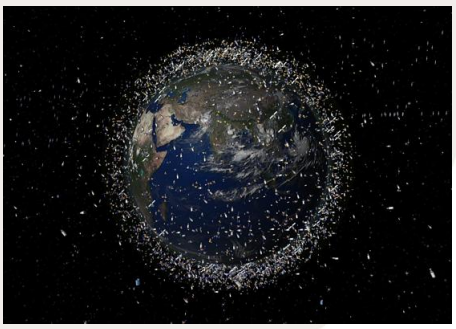
Vulnerable points

- Basically every segment of the system is critical as they are fully interdependent
  - Satellites
  - Ground stations and equipment
  - Space port and launchers
  - Spectrum and frequencies for dataflow

- Satellites cannot be repaired or replaced rapidly and at low cost

Threats

- To satellites
  - (intentional or in-) Collision with objects, e.g. debris
  - Space weather
- To ground infrastructure and launchers
  - Natural disaster
  - Man-made accidents
  - Terrorism
  - Control over segments situated in 3rd countries
  - Social acceptance
- IT systems (on the ground and in satellites)
  - Hacker and cyber attacks
- Data flow
  - Interference (intentional or in-)
  - Spectrum availability



Criticality of space applications

- Synchronisation of networks via Global Navigation Satellite Systems (banks, stock exchange, electricity grids, …)
- Emergency situations when ground infrastructure is unusable or not existing
- Maritime and air transport
- Military/defence
- Border protection

Ongoing activities

- Galileo
  - Has a transport legal basis (i.e. within scope of current CIP Directive)
  - Criticality has been acknowledged
  - Ground segments declared as NCI; Commission proposal for a new regulation (art 27.2) calls upon the Member States to designate them as ECI
  - Other segments not covered because outside of scope; some voluntary specific arrangements with some MS
- Space situational awareness ("SSA")
  - Preparation of a EU programme to protect satellites against space debris and space weather
- Workshop with US on SSA and space-related CIP aspects

Conclusion

- Use of space applications is ubiquitous
- Some are critical
- Has been acknowledged for Galileo
- Current CIP Directive cannot accommodate this

➔ Scope of CIP Directive should be broadened to space


Thank you for your attention!
European Commission
Enterprise and Industry
6th EPCIP Workshop •11

European Commission

EUR 25232 EN - Joint Research Centre – Institute for the Protection and Security of the Citizen
Title: **Memorandum on the results of the sixth workshop on the implementation and applications of the Directive 2008/114/EC**
Author(s): Georgios Giannopoulos, Muriel Schimmer
Luxembourg: Publications Office of the European Union
2012 – 70 pp. – 210 x 297 cm
EUR – Scientific and Technical Research series – ISSN 1831-9424 (online), ISSN 1018-5593 (print)
ISBN 978-92-79-23171-1
doi:10.2788/14841

Abstract
The workshops on the Implementation and Application of the Directive 2008/114/EC have been an important activity for enhancing the communication of the Member States with the Commission Services with respect to the application of the Directive and also for exchange of relevant information. Six workshops have been organized since the adoption of the Directive in December 2008. This activity will continue to support the implementation and application of the Directive while it will also serve the review of the Directive that is due to kick off in January 2012

The mission of the JRC is to provide customer-driven scientific and technical support for the conception, development, implementation and monitoring of EU policies. As a service of the European Commission, the JRC functions as a reference centre of science and technology for the Union. Close to the policy-making process, it serves the common interest of the Member States, while being independent of special interests, whether private or national.

LB-NA-25232-EN-N