COUNCIL OF THE EUROPEAN UNION

Brussels, 27 May 2009

10125/09

TELECOM 115
DATAPROTECT 39
JAI 319
PROCIV 78

NOTE

from :	Working Party on Telecommunications and Information Society
to :	Coreper/Council
No. Cion prop. :	8375/09 TELECOM 69 DATAPROTECT 24 JAI 192 PROCIV 46
Subject :	European Network and Information Security Policy - Guidelines for exchange of views

In view of the TTE Council on 11 June 2009, the delegations will find in annex for information the guidelines envisaged by the Presidency for the exchange of views of Ministers.

GUIDELINES FOR EXCHANGE OF VIEWS ON

THE FUTURE OF NETWORK AND INFORMATION SECURITY POLICY

TTE COUNCIL, 11 JUNE 2009

1. INTRODUCTION

Communication networks and information systems have become the nervous system of our modern society. Many services and processes in our economy and society are increasingly dependent on their well functioning, and their security and resilience are of rapidly growing concern.

Risks related to information and communication technologies constitute a constant challenge for Europe mostly due to the constantly evolving nature of cyber-threats, their increasing complexity, and globalisation. This challenge is exacerbated due to global infrastructure interdependencies, emerging technologies, ubiquitousness of information and communication technologies, a lack of minimum standards, and continued convergence of technologies.

Network and information security challenges will require a strong, coordinated European response. Recent cyber-attacks targeting individual countries have shown that one country on its own can be very vulnerable. An EU-wide approach that complements and adds value to national initiatives is a crucial element of network and information security policy.

2. ENISA – THE EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY

In order to tackle security challenges for the Information Society, in 2004 the European Community established the European Network and Information Security Agency[1] (ENISA) with the goals of ensuring a high and effective level of network and information security within the Community and developing a culture of network and information security for the benefit of EU citizens, consumers, enterprises and administrations.

[1] Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing ENISA, OJ L 77, 13.3.2004, p. 1–11.

ENISA was originally established for a period of five years (2004-2009). On 24 September 2008, the Council and the European Parliament adopted a Regulation extending the mandate of ENISA 'à l'identique' with three years till 13 March 2012.[1] For the period 2004-20012, ENISA has an annual budget of around eight million euro, and around 50 members of staff.

In order to assess the options for the future of ENISA after March 2009, the Commission launched an evaluation of the performance of the Agency since its establishment by an external panel of experts.[2] In June 2007, the Commission issued a Communication on the evaluation of ENISA,[3] which made an appraisal of the report of the external group of experts and presented the recommendations of the ENISA Management Board. The key findings of that expert report confirmed the validity of the policy behind the creation of ENISA and its original goals, and in particular its contribution to achieving a truly internal market in electronic communications.

The Management Board of ENISA issued recommendations regarding eventual appropriate changes to the ENISA Regulation.[4] The main recommendations stated that the ENISA Regulation should be revised to extend the mandate, that mandate should again have a review point, the scope of Agency should not be materially changed, and the Regulation should be revised to combine Articles 2 and 3[5] to set outcome-based key objectives that are realistic and within the scope of the Agency.

---

1 Regulation (EC) No 1007/2008 of the European Parliament and of the Council of 24 September 2008 amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration, OJ L 293 of 31.10.2008.

2 "Evaluation of the European Network and Information Security Agency," Final Report by the Experts Panel, IDC EMEA, 8.1.2007{Available at: http://ec.europa.eu/dgs/information_society/evaluation/studies/index_en.htm }

3 COM(2007) 285 final

4 Available at: http://enisa.europa.eu/pages/03_02.htm. Also discussed in COM(2007) 285 final.

5 On, respectively, Objectives and Tasks.

3. POLITICAL CONTEXT OF THE EXCHANGE OF VIEWS

On 2 September 2008, in her intervention during the Plenary Session of the European Parliament, the Commission called on the European Parliament and the Council "to open, early in 2009, an intense debate on Europe's approach to network security and on how to deal with cyber-attacks, and to include the future of ENISA in those reflections."

On 24 September 2008, in the recitals of the Regulation extending the mandate of ENISA, the Council and the European Parliament called for "further discussion about the Agency" and "on the general direction of the European efforts towards an increased network and information security."

4. PREPARATORY STEPS

In order to facilitate this debate, as a first step, the Commission services held a public consultation on the possible objectives of a strengthened NIS policy at EU level, and on the means to achieve those objectives, from 7 November 2008 through 9 January 2009. The Commission services also organised a workshop that took place on 15 December 2008 with experts in network and information security from competent bodies of the Member States to discuss the changing landscape of security challenges, possible policy priorities and objectives to deal with these evolving challenges, and the instruments and mechanisms needed for a strengthened network and information security policy at the European level.

In the scope of public consultation concerning the future of ENISA, a large majority of respondents supported an extension of the Agency mandate and advocated an enlarged role in cooperation of NIS activities at the European level as well as for an increase of its resources.

5. ONGOING ACTIONS ON CRITICAL INFORMATION INFRASTRUCTURE PROTECTION

In the context of the umbrella initiative on EPCIP (European Programme on Critical Infrastructure Protection), the European Commission has recently adopted a Communication on Critical Information Infrastructure Protection "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience."[1]

---

1 COM (2009) 149

The Communication proposes a series of short-medium term (until 2011) actions on security and resilience of CIIs, including: fostering pan-European cooperation between National/Governmental Computer Emergency Response; engaging the private sector in information sharing and dissemination of good practices with the public sector; supporting the sharing of information as well as good policy practices between Member States, thus stimulating a stronger European cooperation between Member States via national and multinational contingency plans and regular exercises for large scale networks security incident response, as well as disaster recovery and continuing the development of the criteria to identify European Critical Infrastructures for the ICT sector.

6. THE TALLINN MINISTERIAL CONFERENCE

On 27 and 28 April 2009, a Ministerial Conference took place on critical information infrastructure protection (CIIP) in Tallinn. The Conference was organised by Estonia under the auspices of the Czech EU Presidency.

The Conference conclusions supported ongoing work on the CIIP, and emphasised that this work should concentrate on actions enhancing security and resilience of CIIs, building effective Public-Private Partnerships at the EU level, and increasing cooperation and coordination in the EU and internationally. The Conference considered that the "last years have shown that cyber-attacks have reached an unprecedented level of sophistication and are increasingly performed for profit or political reasons" and the "huge number of viruses, worms and other forms of malware, the expansion of botnets and the continuous rise of spam confirm the severity of the problem. These threats require a strong, coordinated European response."

Regarding ENISA, the Conference concluded that the Agency "provides a valuable instrument for bolstering EU-wide cooperative efforts in this field. However, the new and long lasting challenges ahead require a thorough rethinking and reformulation of the Agency's mandate in order to better focus on EU priorities and needs; to attain a more flexible response capability; to develop European skills and competences; and to bolster the Agency's operational efficiency and overall impact. In this way, ENISA might be rendered a permanent asset for each Member State and the European Union at large."

The Conference also concluded that "a joint EU exercise on Critical Information Infrastructure Protection should be organised and staged by 2010, in line with the Commission's action plan." An expression of support for this exercise by the TTE Council would emphasise its significance as the first tangible step towards a strong coordination and cooperation among Member States and a means to help identify areas requiring immediate actions.

7. REVIEW OF THE REGULATORY FRAMEWORK FOR ELECTRONIC COMMUNICATIONS

According to the new regulatory framework for electronic communications, ENISA is given a role in supporting Member State bodies and the Commission on network and information security aspects.

8. QUESTIONS TO GUIDE THE EXCHANGE OF VIEWS

1. What should the two or three medium/long term main aims of a strengthened network and information security policy at EU level be to ensure trans-national cooperation of all stakeholders and permanent or long-term policy instruments?

2. Whereas an Agency seems to be an effective instrument to strengthen network and information security policy in Europe, should in the medium/long term other means be foreseen?

3. How should ENISA be reformed to better focus on the main challenges, with increased flexibility to adapt to the evolving landscape of cyber-threats, permanence or long-term assurance of continuity, adequate evaluations of its performance, and a reinforced governance structure? Would an increase of resources be needed in order to cope with these challenges?