COUNCIL OF THE EUROPEAN UNION

Brussels, 8 December 2009

15841/09

TELECOM 240
DATAPROTECT 72
JAI 820
PROCIV 180

NOTE

from :	COREPER
to :	COUNCIL
No Cion prop.	8375/09 TELECOM 69 DATAPROTECT 24 JAI 192 PROCIV 46 + ADD1 + ADD2 + ADD3 +ADD4
No prev. doc.	14807/09 TELECOM 216 DATAPROTECT 65 JAI 713 PROCIV 155
Subject :	Council Resolution on collaborative European approach on Network and Information Security - Adoption

On 24 September 2008, the Council and the European Parliament adopted a Regulation extending the mandate of the European Network and Information Security Agency (ENISA) for three years till 13 March 2012[1]. In the recitals of the adopted 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."

On 30 March 2009, the Commission adopted a Communication on Critical Information Infrastructure Protection "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience".

[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.

The Communication launched a policy initiative to protect Critical Information Infrastructures (CIIs). As such are considered the Electronic Communication services and networks, as their disruption or destruction would have a serious impact on vital societal functions. Because they tend to be decentralised, highly interconnected and interdependent, failures of these infrastructures could cascade and spread beyond national borders. The Commission Communication proposes an action plan to tackle the challenges involved. The action plan focuses on preparedness and prevention and aims at strengthening the security and resilience of CIIs and at reinforcing the tactical and operational cooperation at the European level.

On 27 -28 April 2009 a Ministerial Conference on Critical Information Infrastructure Protection (CIIP) was held in Tallinn, Estonia under the auspices of the Presidency of the Council of the EU. The Presidency concluded that despite the progress achieved thus far in protecting CIIs, a number of challenges remain. There is an urgent need for Member States and all stakeholders to commit themselves to swift action in order to enhance the level of preparedness, security and resilience of CIIs throughout the European Union.

During the Council meeting on 11-12 June 2009, the Ministers held a political discussion concerning issues related to European network and information security policy on the basis of the guidelines proposed by the Presidency. The Ministers focused their discussions on the issue of critical information infrastructure protection, on the future of ENISA as well as on the general direction of European efforts in this field.

With the aim to strengthen the Network and Information Security in Europe and to build upon the work presented above, the Presidency now proposes the adoption of a Council Resolution on a collaborative European approach to Network and Information Security (in annex to the present document).

On 28 October 2009, Coreper examined the proposal which was acceptable to all Delegations. The Commission still has a reservation on point VII. 7.

The Council is invited to:

- examine the text in view of its adoption;
- after adoption, submit the Council Resolution for publication in the Official Journal of the European Union.

COUNCIL RESOLUTION
on a collaborative European approach to Network and Information Security

THE COUNCIL OF THE EUROPEAN UNION,

I. HAVING REGARD TO

1. The Commission communication of 31 May 2006 on "A Strategy for a Secure Information Society" putting forward a process of "dialogue, partnership and empowerment" engaging Member States and private sector stakeholders;
2. The Commission communication of 12 December 2006 on "The European Programme for Critical Infrastructure Protection (EPCIP)" aiming to improve the protection of critical infrastructures in the EU and creating an EU framework concerning the protection of critical infrastructures;
3. The Council Directive of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection;
4. The Council Resolution of 22 March 2007 on a Strategy for a Secure Information Society in Europe;
5. The Council conclusions of 19-20 April 2007 on a European Programme for Critical Infrastructure Protection;
6. The Commission communication of 30 March 2009 on Critical Information Infrastructure Protection (CIIP);
7. The ongoing debate, including the relevant public consultation, on the future of the European Network and Information Security Agency (ENISA) and its role in CIIP;
8. The Presidency conclusions on CIIP of the Tallinn ministerial conference of 27-28 April 2009;
9. The Lisbon goals of competitiveness and growth and the work currently underway to review the Lisbon strategy**;**
10. The security measures proposed in the review of the Regulatory Framework on Electronic Communications Networks and Services;

11. To ensure effective future policy on Network and Information Security, this resolution assumes that no conclusions have yet been reached on any amendments needed in the ENISA regulation. As the future of Network and Information Security policy is currently under review by the Commission, any outcome of this review, regarding any amendments to the ENISA regulation, should not be prejudiced by this resolution in advance of the publication by the Commission of its results.

II. NOTING THAT

1. Given the importance of electronic communications, infrastructures and services as a basis of economic and social activity, Network and Information Security (NIS) contributes to important values and objectives in society, such as democracy, privacy, economic growth, the free flow of ideas, and economic and political stability;
2. Information and communication technology systems, infrastructures and services, including the Internet, play a vital role for society**,** and their disruption has the potential to cause huge economic damage, underlining the importance of measures to increase protection and resilience aimed at ensuring continuation of critical services;
3. Security incidents risk undermining user confidence. While severe disruptions of networks and information systems could have a major economic and social impact, everyday problems and nuisances also risk eroding public confidence in technology, networks and services;
4. The threat landscape is evolving and growing, which increases the need to provide end-users, businesses and governments with electronic communications infrastructures that are robust and resilient by default and to identify the right incentives for the providers to do so in a timely manner;
5. There is a need to enhance and embed Network and Information Security in all policy areas and sectors of society, and to address the challenge of ensuring sufficient skills via both national and European actions and raising awareness among users of information and communication technology (ICT);

6. The completion and functioning of the Internal Market will require that network owners and service providers cooperate across borders, given that possible disruptive events in one Member State may also affect other Member States and the EU as a whole;
7. New usage patterns, such as cloud computing and software as a service, put additional emphasis on the importance of Network and Information Security;
8. Network and Information Security serves the objective of all parties, in all sectors of society, to be able to trust the information systems, therefore a cross-sector and cross-border approach is needed;
9. With the increasing use of ICT in society, Network and Information Security is a prerequisite for the reliable, safe and secure delivery of public services, such as e-Government.
10. ENISA has the potential to build on the important role it already plays in Network and Information Security.

III. UNDERLINES THAT

1. A high level of Network and Information Security in the EU is needed in order to support:
   a. the freedoms and rights of citizens, including the right to privacy;
   b. an efficient society in terms of quality in information handling;
   c. the profitability and growth of trade and industry;
   d. citizens' and organizations' trust in information handling and ICT systems;
2. The ICT sector is vital to most sectors of society making Network and Information Security a joint responsibility of all stakeholders, including operators, service providers, hardware and software providers, end-users, public bodies and national governments.

IV. RECOGNISES

1. The importance of an active and knowledgeable European Network and Information Security community that contributes to the increased collaboration between Member States and the private sector;
2. The advantages of a harmonised use, where appropriate, of international security standards across the EU for the purpose of NIS;
3. The need for a collaborative European approach to Network and Information Security in the international arena as it is a global challenge;
4. The importance for the Member States and the EU Institutions of the availability of reliable statistical data on the state of Network and Information Security in Europe;
5. The need for increased awareness and tools for risk management for all stakeholders;
6. The importance of increasing efforts among Member States to raise awareness, to exchange good practice and to develop guidance for Member States;
7. The importance of multi-stakeholder models such as Public Private Partnerships (PPPs), built on a long term, bottom-up model to mitigate identified risks where such an approach delivers added value in helping to ensure a high level of network resilience;
8. The vital role providers play in providing robust and resilient electronic communication infrastructures to society;
9. The usefulness of exercises in Europe in the area of Network and Information Security, which can provide valuable lessons for network operators and service providers as well as for governments;
10. That National or Governmental Computer Emergency Response Teams (CERTs) or other response mechanisms that respond to threats and address vulnerabilities can contribute to a high level of resilience and a capability to withstand and remedy disruptions of Networks and Information Systems;
11. The importance of exploring the strategic effects, risks and prospects for establishing CERTs for the EU institutions and consider the possible future role of ENISA in this matter.
12. The work done by ENISA in the area of Network and Information Security to date and the need to further develop ENISA into an efficient body with clear benefits for the field of European Network and Information Security.

V. STRESSES THAT

1. An enhanced and holistic European strategy for network and information security, with clearly delineated roles of the European Commission, the Member States and ENISA, is of vital importance to tackle current and future challenges;
2. After appropriate consultation and analysis consideration should be given in the legislative process to modernising and reinforcing ENISA with a mandate that ensures flexibility and oversight by Member States and the Commission, as well as an efficient role for private sector stakeholders' representation. Its mandate should take into account the Regulatory Framework on Electronic Communications, Networks and Services and be in line with the ambitions set out in the Lisbon Agenda and include goals related to research, innovation, competitiveness, economic growth and ensuring trust;
3. ENISA could support the policy development and implementation roles of the Commission and the Member States, in particular in bridging the gap between technology and policy and should work closely with Member States and other stakeholders to ensure that its activities are well aligned with EU priorities;
4. ENISA, under a revised mandate, should serve as the EU's centre of expertise in EU related Network and Information Security matters. As such European institutions should seek and take the utmost account of its opinion when developing and implementing policies having a potential impact in this field.
5. ENISA could also be able, upon request, to assist Member States to improve their own Network and Information Security capabilities and their ability to cope with security incidents.

VI. INVITES THE MEMBER STATES TO

1. Continue work to increase end-user confidence in ICTs through awareness-raising campaigns;
2. Organise national exercises and/or participate in regular European exercises in the area of Network and Information Security, noting the need for extensive planning due to the complexity of the area and the involvement of the private sector. ENISA could, upon request, assist the Member States in this regard. The scope and geographical dimension of exercises should naturally evolve over time and should be based on recognised risks;
3. Create Computer Emergency Response Teams (CERTs) in Member States that have not yet developed such a capability and to reinforce the cooperation between national CERTs on a European level**.** ENISA could assist the Member States in this regard;
4. Increase efforts on education**,** training and research programmes in Network and Information Security in order to ensure the availability in the EU of the necessary technical skills and professionals as well as increase the professionalism of those in that field;
5. To jointly react when there is a cross-border incident and to increase their ability to do it appropriately, which requires strengthening the dialogue between the decision makers involved, especially on confidentiality issues.

VII. INVITES THE COMMISSION TO

1. Support Member States, as appropriate, in the implementation of this Resolution;
2. Regularly inform the European Parliament and the Council on initiatives taken at EU level relating to Network and Information Security;
3. In collaboration with ENISA, initiate an awareness raising campaign among European public and private actors regarding the importance of appropriate risk management with regard to Network and Information Security;
4. Continue, in collaboration with the Member States, to identify incentives for providers of electronic communication infrastructures to deliver default robust and resilient infrastructures to end-users, businesses and governments;

5. In collaboration with the Member States, develop methods that will allow for a comparable evaluation to take place at EU level of the socio-economic impact of incidents and of the efficiency of preventive measures;
6. Encourage and improve multi-stakeholder models, which need to have a clear added value benefiting end-users and industry;
7. Come forward with a holistic strategy on Network and Information Security,[2] including proposals on a reinforced and flexible mandate for ENISA as well as strengthened oversight of the Member States and the Commission;
8. Carry out an analysis, in collaboration with the Member States, on Computer Emergency Response Teams (CERTs) in order to identify in which areas further cooperation is called for;
9. Continue investigation towards a common or interoperable approach for EU institutions in the procurement of secure ICT systems and services.

VIII. CALLS ON ENISA TO

1. Continue to actively support Member States, the European Commission, and other relevant stakeholders in implementing European network and information security policies and the action plan on CIIP;
2. Work in collaboration with Member States, the Commission and statistical bodies, on the development of a framework of statistical data on the state of Network and Information Security in Europe.

[2] The Commission suggests to add here the word "possibly".

IX. INVITES STAKEHOLDERS TO

1. Intensify efforts to enhance the level of Network and Information Security, in particular with regard to delivering reliable, trustworthy and easy to use products and services;
2. Inform users properly on security risks associated with products and services and how they can protect themselves;
3. Take all appropriate technical and organisational measures to safeguard the continuation, integrity and confidentiality of electronic communications networks and services;
4. Continue to work on standardisation of Network and Information Security to strive to find harmonised and interoperable solutions;
5. Participate with Member States on exercises to provide appropriate responses to emergencies.