EUROPEAN COMMISSION

Brussels, 30.9.2010
SEC(2010) 1126

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT

Accompanying document to the

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND THE COUNCIL

concerning the European Network and Information Security Agency (ENISA)

{COM(2010) 521 final}
{SEC(2010) 1127}

TABLE OF CONTENTS

TABLE OF ANNEXES

1. PROCEDURAL ISSUES AND CONSULTATION OF INTERESTED PARTIES

1.1. Scope

This impact assessment focuses on how a modernised network and information security (NIS) agency, which is broadly recognised to be an appropriate and needed policy instrument to deal with NIS challenges, should best be shaped to support Member State bodies and the Commission to achieve NIS policy objectives, after the expiry of the mandate of the European Network and Information Security Agency (ENISA) in March 2012.

1.2. Organisation and timing

Annex 1 contains a detailed table depicting the timetable of the consultation of interested parties, of the meetings of the inter-service steering group and of the Impact Assessment report itself.

1.3. Review by the Impact Assessment Board

An earlier draft of this impact assessment report was sent to the Commission's Impact Assessment Board on 22 February 2010. On 24 March 2010, representatives of DG Information Society and Media had a meeting with the Board. The Board issued a written opinion on the draft report on 26 March, inviting DG Information Society and Media to resubmit a new version of the impact assessment report. The Impact Assessment Board recommended providing more detail on how ENISA is currently dealing with network and information security related issues, and why this is not considered to be sufficient, as well as a more comprehensive overview of the main expected impacts of the options and clarification on the basis on which the scores were assigned. On the basis of the opinion of the Impact Assessment Board, the report was significantly strengthened and expanded on the requested points. In chapter two, the description of the problem drivers gives further detail with examples of how ENISA has already addressed them in its work. In chapter four, more details are provided on the analysis of the possible organisational formats for implementing the identified policy options. In chapter five, the methodology for qualitative assessment of the policy options was revised. The report now explains more thoroughly the main impacts and how each option contributes to achieve them. The revised impact assessment was submitted to the Board on 15 April 2010. On 27 April 2010, the Board issued written opinion on the revised impact assessment, indicating some areas in which the impact assessment needs to be strengthened. Namely, it asked for further details about the current functions and mandate of ENISA and how the mandate of the modernised Agency would be adapted to the constantly evolving NIS environment; more clarity about the content of the preferred option and how it deals with the problem drivers; strengthened assessment of international impacts and impacts on cyber crime. The recommendations of the Board have been duly taken into account and the relevant sections have been modified.

The opinion of the Board is one of the accompanying documents to this report and will be made public once the Commission adopts the proposal.

1.4. Consultation and expertise

During the preparation of this initiative, **DG INFSO sought the involvement of all relevant stakeholders**, i.e., Member States, national competent bodies and authorities, private sector, academia and citizens.

The different aspects of this policy initiative have been discussed with stakeholders as widely as possible following an inclusive approach and respecting the principles of participation, openness, accountability, effectiveness and coherence.

1.4.1. Consultations prior to the 2008 Regulation extending the mandate of ENISA

ENISA had been established in 2004 for a period of five years.[1] Before the expiration of the mandate of ENISA(March 2009), the Commission had started a process of determining what policy proposals would best serve the Community objectives in the field of network and information security (NIS) from 2009 onwards:

- In 2006, the Commission adopted a Communication aiming to further develop a dynamic, global strategy in Europe, based on a culture of security and founded on dialogue, partnership and empowerment[2]. The Communication foresaw that ENISA could serve as a centre for information sharing, cooperation amongst all stakeholders and exchange of commendable practices, both within Europe and with the rest of the world. ENISA was requested to examine the feasibility of creating a European multilingual information sharing and alert system, which would build upon existing or planned national public and private initiatives. ENISA was asked to develop a trusted partnership with Member States and stakeholders to develop an appropriate data collection framework for EU-wide data on security incidents and consumer confidence.
- In accordance with Article 25 of the ENISA Regulation, an evaluation of ENISA was carried out by an external panel of experts in 2006/2007, to provide a formative assessment of the Agency's working practices, organisation and remit and if appropriate, recommendations for improvements. It should be noted that this evaluation was carried out only one year after ENISA had become operational. The evaluation report[3] confirmed the validity of the original policy rationale behind the creation of ENISA, and raised issues to be tackled concerning the visibility of the Agency and its ability to achieve a high level of impacts. These issues included the organisational structure; the skills mix and the size of the operational staff of the Agency and organisational challenges due to the remote location.
- In March 2007, the Management Board of ENISA formulated recommendations on the future of the Agency and on changes to the ENISA Regulation.[4]
- In June 2007, the Commission issued a Communication to the European Parliament and the Council on the evaluation of ENISA,[5] underlining the need to review the policy instruments in the field of network and information security, including a possible extension of its mandate.
- From 13 June to 7 September 2007, DG Information Society and Media held a public consultation on the future of ENISA.[6]

---

1 Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency

2 COM(2006)251

3 See http://ec.europa.eu/dgs/information_society/evaluation/studies/s2006_enisa/docs/final_report.pdf

4 As foreseen in article 25 of the ENISA Regulation. The document adopted by the ENISA Management Board is available at the following website: http://enisa.europa.eu/pages/03_02.htm

5 Communication from the Commission to the European Parliament and the Council on the evaluation of the European Network and Information Security Agency (ENISA), COM(2007)285 final of 1.6.2007 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007DC0285:EN:NOT

6 http://ec.europa.eu/information_society/policy/nis/enisa/publiconsult/index_en.htm

- In November 2007, the Commission adopted a package of proposals to reform the regulatory framework for electronic communications. It contained a proposal to establish a European Electronic Communications Market Authority (EECMA), which would, in addition to other tasks, assume responsibility for the activities undertaken by ENISA. This proposal was withdrawn.
- In 2007/2008, the Management Board and the Executive Director of ENISA addressed the concerns raised in the evaluation report and took measures to implement the recommendations of the Management Board and the Commission Communication.

1.4.2. Consultations and debate following the 2009-2012 extension of the ENISA mandate

On 2 September 2008, in an intervention during the Plenary Session of the European Parliament, Commissioner Viviane Reding 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."

Following a Commission proposal, 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.[7] In the recitals of the Regulation, the Council and the European Parliament called for "further discussion about the Agency [and] the general direction of the European efforts towards an increased network and information security." In June 2008, the Council had asked the Commission to contribute to this discussion.[8]

- 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.[9] 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. The respondents identified a number of key priorities such as the need for a more coordinated approach to cyber threats across Europe, trans-national cooperation in order to respond to large scale attacks, building of trust and improved exchange of information among stakeholders. A European NIS agency was identified as an important instrument to contribute to the achievement of the objectives of such policy priorities.[10]
- The Commission services also organised a workshop that took place on 15 December 2008 with experts in NIS 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 NIS policy at the European level.

---

7 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

8 Draft minutes of the 2877th meeting of the Council of the European Union (Transport, Telecommunications and Energy), held in Luxembourg on 12 and 13 June 2008 (10641/08),

9 See the summary report from the Public Consultation "Towards a Strengthened Network and Information Security Policy in Europe" (Annex 11)

10 See question 6 of the Public Consultation "Towards a Strengthened Network and Information Security Policy in Europe", (Annex 11)

- On 30 March 2009, the Commission adopted a Communication on Critical Information Infrastructure Protection (CIIP)[11] the focus of which is on protecting Europe from cyber attacks and cyber disruptions by enhancing preparedness, security and resilience. The Communication launched an Action Plan that called on ENISA to play a key role.
- On 31 March 2009, an Exchange of Views was held at the Telecom Council Meeting on 'The Future of Network and Information Security in Europe.'
- On 27-28 April 2009, a Ministerial Conference on CIIP took place in Tallinn, organised by Estonia under the auspices of the Czech EU Presidency[12]. 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 future of ENISA was included in a further exchange of views at the Telecom Council on 11 June 2009, which highlighted the importance and the global dimension of NIS challenges and the need for a pan European approach to cross border issues as an effective way to increase security and resilience in the EU. Most Member States expressed support for extending the mandate of ENISA and increasing its resources.
- On 16 June 2009, a workshop was held of the European Forum of Member States on security and resilience of CII, defined in the Communication on CIIP.
- On 17 June 2009, a workshop took place on the European Public Private Partnership for Resilience (EP3R), the need of which was identified in the Communication on CIIP.
- The Swedish Presidency organised a conference on NIS entitled "Resilient Electronic Communications – A Multi-stakeholder Challenge" on 05 November 2009.
- Further workshops on the European Forum of Member States on security and resilience and on the European Public Private Partnership for Resilience (EP3R) were held 12-13 November 2009.
- The Swedish Presidency has further advanced the debate on the future of NIS in Europe and a Council Resolution[13] on a collaborative approach to NIS was adopted at the Telecom Council on 18 December 2009 which stressed, inter alia, that "ENISA, under a revised mandate, should serve as the EU's centre of expertise in EU related Network and Information Security matters." The Council recognised the role and potential of ENISA as well as the need to "further develop ENISA in an efficient body." It also stressed the need for the modernisation and reinforcement of the Agency in supporting the Commission and the Member States bridging the gap between technology and policy, serving as the EU's centre of expertise in EU related NIS matters.

---

11 Communication from the Commission to the European Parliament and the Council on Critical Information Infrastructure Protection, COM (2009)149 final of 30.3.2009

12 Discussion Paper: http://www.tallinnciip.eu/doc/discussion_paper_-_tallinn_ciip_conference.pdf Presidency Conclusions: http://www.tallinnciip.eu/doc/EU_Presidency_Conclusions_Tallinn_CIIP_Conference.pdf

13 Council Resolution of 18 December 2009 on a collaborative European approach to Network and Information Security, (2009/C 321/01)

- On 3 March 2010, the Commission adopted its Europe 2020 Strategy for smart, sustainable and inclusive growth.[14] One of the flagship initiatives of this strategy is the European Digital Agenda, in which NIS plays a central role.

The consultation process involved a wide variety of stakeholders and experts whose contributions have been very helpful in the development of the policy proposal. These contributions included (representatives of):

- Member States bodies, involved in the field of NIS;
- National Regulatory Authorities in the field of electronic communications networks and services;
- Telecommunications operators and Internet Service Providers and related sector associations;
- Sector and consumers protection associations;
- Manufacturers of hardware and software components for electronic communications networks and services and related associations;
- Public organisms involved in the field of NIS such as Computer Emergency Response Teams (CERTs);
- Academics and research communities;
- Major corporate users of information infrastructures from the financial, electricity and transport sector
- Other stakeholders and European citizens who replied to the public consultations.

1.4.3. Inter-service Steering Group

Within the Commission, an Inter-service Steering Group was set up. The following services participated in the group: DG JLS, DG BUDG, DG RTD, DG JRC, DG HR (DS), DG TREN, DG ENTR, DG MARKT, DG COMP, DG SANCO, DG ENV, DG EMPL, DG DIGIT, DG RELEX, DG SJ and DG SG.

The Inter-service Steering Group met three times: kick-off meeting on 10 September 2009, second meeting on 8 October 2009 and final meeting on 29 October 2009 to discuss the draft final impact assessment report.

2. PROBLEM DEFINITION

2.1. What is the issue or problem that may require action?

Information and Communication Technologies (ICTs) have become the backbone of the EU economy and society as a whole. The ICT sector is vital for all sectors of society. Businesses rely on the ICT sector both in terms of direct sales and of the efficiency and effectiveness of internal management and production processes. ICTs are also more and more pervasive for the functioning of governments and public administrations. European citizens increasingly rely on Information Society services and use ICTs in their daily activities.

ICTs are vulnerable to threats which no longer follow national boundaries and which have evolved with technology and market developments. As ICTs are global, interconnected and interdependent with other infrastructures, their security and resilience cannot be secured by purely national and uncoordinated approaches. Since the private sector owns most of the infrastructure used to provide ICT services to all kinds of players in the society, it is crucial

[14] COM(2010)2020

that a true culture of risk management and NIS is built up throughout Europe including the right incentives for all stakeholders to protect ICTs.

ENISA was initially created in 2004 in order to enhance the capacity of the Community, the Member States and consequently the business community to prevent, to address and to respond to major network and information security risks. Since then, the challenges related to NIS have evolved alongside with technology and market developments, and have been the subject of further reflection and debate. This allows today for an update and more detailed description of the precise problems identified and of how these are impacted by the changing landscape of NIS. Throughout the debate on the future NIS policy in Europe the Member States and various stakeholders have repeatedly shared the view that a modernised NIS agency is needed to best serve the goals of a renewed NIS strategy.

2.2. What are the underlying drivers of the problem?

There are a number of drivers which make stakeholders vulnerable to NIS threats and breaches. Some of these drivers have already been identified in recent impact assessments.[15] However, because of their evolving nature, which was also recognised by the stakeholders during the consultation process, it has become clear that a new, modernised and more efficient approach is needed to tackle them. Following the debate launched by the European Parliament and the Council on a reinforced NIS policy in Europe the Commission has taken stock of the full set of problems which needs to be addressed. They all show that there is a need for a reliable structure at EU level to tackle the problem and to be up to speed, throughout Europe, with the constantly evolving technology and market conditions around NIS. In this respect, the vast majority of stakeholders regarded an Agency as the most appropriate structure.[16] Indeed, it should not be overlooked that the key problems identified during the 2006/2007 evaluation of ENISA were due to the rigidity of the original mandate of ENISA that was conceived in a different policy context (before the 2004 enlargement) and it has shown not to correspond to present and evolving NIS needs and challenges. Indeed, the list of tasks defined in Art. 3 of the current ENISA Regulation has been considered to be insufficient to provide the Agency with the necessary flexibility and adaptability to respond to the challenges of the continuously evolving NIS environment. ENISA was established to help Member States, the Commission and the business community in addressing NIS issues mainly through providing support to information exchange and dissemination of good practices across the EU. In other words, ENISA was established as a platform for discussion among stakeholders. Therefore, it should be stressed that the Agency has no operational functions and is not equipped to carry out operational tasks of technical nature to enhance NIS..

The goal of this impact assessment is to examine the various policy options for the most appropriate institutional instrument, that is, a modernised NIS Agency, to support the European Union to attain the policy objectives that are identified as the priority ones to tackle the existing NIS problem drivers in the most efficient and effective way.

---

15 See Impact Assessment Report for the Communication on a Strategy for a Secure Information Society (SEC(2006) 656) and the one for the Communication on Critical Information Infrastructure Protection (CIIP), SEC(2009) 399 of 30.3.2009

16 See the results of the 2007 public consultation on the future of ENISA (see footnote 6), the results of the 2008/2009 public consultation on possible objectives of a strengthened NIS policy at EU level and on the means to achieve those objectives (see footnote 9) and the Council Resolution on a collaborative approach to network and information security policy of 18 December 2009 (see footnote 13).

2.2.1. Diversity and fragmentation of national approaches

NIS problems do not follow national boundaries and therefore cannot be effectively addressed at national level only. At the same time, there is a great diversity in how the problem is dealt with by public authorities in different Member States. This was outlined both in the impact assessment on CIIP[17] and the work of ENISA on stocktaking of national policy and regulatory environments.[18] The differences can constitute a major obstacle to the implementation of appropriate EU-wide mechanisms to enhanced NIS in Europe. Due to the interconnected nature of ICT infrastructures the effectiveness of measures taken at the national level in one Member State is still strongly impacted by the lower level of measures in other Member States and the lack of systematic cross-border cooperation. Insufficient NIS measures resulting in an incident in one Member State may cause disruptions to services in other Member States.

In addition, the multiplication of security requirements implies a cost burden on businesses which operate on EU level and lead to fragmentation and lack of competitiveness in the European internal market.

2.2.2. Limited European early warning and response capability

While dependence on network and information systems is increasing, preparedness to address incidents seems insufficient.

The current national systems of early warning and incident handling have important shortcomings. Processes and practices for monitoring and reporting network security incidents differ significantly across Member States. In some countries, the processes lack formalisation whereas in other countries, there is no competent authority for receiving and processing reports on incidents. European systems do not exist. As a result, the provision of basic necessities could be fundamentally disrupted through NIS incidents and appropriate responses should be prepared. The Commission Communication on CIIP also stressed the need for European early warning and incident response capability, potentially supported through European scale exercises.

There is a clear need for policy instruments which aim at proactively identifying NIS risks and vulnerabilities, establishing appropriate response mechanisms (e.g., through the identification and dissemination of good practices), and ensuring that these response mechanisms are known and applied by the stakeholders. So far, ENISA has been instrumental in supporting some Member States and stakeholders to establish CERTs and in assessing the state of CERT activities in Europe.[19] It has also examined the feasibility of a European-wide multilingual Information Sharing and Alerting System (EISAS).[20] However, under its current mandate ENISA would not be able to play a more prominent role in this area, e.g., by supporting the networking of governmental CERTs or guiding the Member States in developing EISAS. Such activities would require the deployment of operational functions requiring significant additional resources and technical expertise of an operational nature.

---

17 See annex 17 to the Impact Assessment on Critical Information Infrastructure Protection, SEC(2009) 399, Background paper on the Critical Infrastructure Protection in ICT sector which shows how the existing measures at national level are diverse, uncoordinated and sometimes insufficient

18 See http://www.enisa.europa.eu/act/res/policies/stock-taking-of-national-policies.

19 http://www.enisa.europa.eu/act/cert/background/inv

20 http://www.enisa.europa.eu/act/cert/other-work/eisas

2.2.3. Lack of reliable data and limited knowledge about evolving problems

There is very little reliable quantitative information available on the impact or even on the occurrence of NIS breaches. According to the recent IDC EMEA market study,[21] comparative security risks assessment, including an evaluation of potential damages, is still very rare.

The lack of a well developed framework for the collection of data on security incidents (occurrence of incidents, economic and societal impact…) makes it difficult for policy makers to adopt adequate policy measures and for businesses to make decisions on investing in security. Also, as stated in the Commission Communication on a strategy for a Secure Information Society, there is still only very limited insight in market forces and incentives ('economic rationale') for measures to enhance security and resilience. The aforementioned IDC EMEA market study confirmed in its conclusions the need for a greater knowledge base and defined a clear set of key indicators which would need to be monitored in order to ensure a balanced development of the European NIS market. In 2008, ENISA completed a report examining the feasibility of a data collection framework[22] in response to a request made by the Commission in the 2006 Strategy on a Secure Information Society. However, given its limited mandate, ENISA could not ensure development of the framework itself. The latter is a resource-intensive activity and, given the fixed budget and establishment plan of the Agency, would have to be performed at the detriment of other important activities. In addition, in order to achieve progress in this area the cooperation among ENISA, the Member States and the EU institutions and bodies in their efforts to collect and disseminate network and information security data needs to be improved.

2.2.4. Lack of awareness of NIS risks and challenges

Responsibilities in ensuring NIS lie with each stakeholder; however, they are not always clearly defined and communicated.

On the one hand, consumers often underestimate the risks involved and their personal responsibility in securing networks and information systems. On the other hand, businesses often mainly see the costs related to NIS and not the potential savings induced by it. More precisely, the IDC EMEA market study[23] found that "the incomplete and generic awareness of personal and business level IT security risks leads to overconfidence in basic level protection and the perception of security costs as too high and the missing business case for the return on investment on security investments." Security threat management is thus still not sufficiently developed.

Under these circumstances, without specific NIS education systems, curricula and trainings, no true culture of NIS risk awareness – which would lead to a more cooperative risk management at EU level – can emerge. ENISA has already done a considerable amount of work in the area of awareness raising, such as the establishment of an awareness raising community and the identification of good practices. However, the scale of the challenge is much bigger than what ENISA could handle with its current level of resources.

2.2.5. International dimension of network and information security problems

Threats to and possible subsequent breaches of NIS are furthermore international by nature (e.g., given the tight interconnection and invisible interdependencies between

---

21 IDC EMEA, The European Network and Information Security Market; Scenario, Trends and Challenges, April 2009

22 http://www.enisa.europa.eu/act/it/oar/data-collection/examining-the-feasibility-of-a-data-collection-framework

23 Cf. supra

communications networks and information systems) and thus the problem does not follow national or even European boundaries. The majority of consulted stakeholders acknowledge that threats to NIS have become a global issue and justify the need for enhanced EU and international cooperation and coordination.

Initiatives taken at the international level so far remain very high level and have only limited impact. As NIS problems are international by nature, the efficiency of efforts done by the EU may be diminished if NIS problems are not adequately addressed internationally. This is why the Action plan on CIIP[24] put special emphasis on international cooperation with a view to developing European priorities on long term Internet resilience and stability and principles and guidelines for Internet resilience and stability.

The development of an EU strategy and the availability of a European point of reference for NIS are needed to facilitate a better European positioning in the international context in order to shelter Europe from international threats. However, in this regard ENISA has under its current mandate a very limited capability to contribute to the Union efforts to cooperate with third countries and international organisations.

2.2.6. Need for collaboration models to ensure adequate policy implementation

Adequate implementation of NIS policies requires collaborative models at EU level. Responsibilities lie with every stakeholder but awareness and information sharing is limited. Stakeholders do not only need guidance in identifying NIS threats. They also need guidance as regards good practices in implementing existing NIS policies, taking into account the cross-border dimension of NIS threats.

The 2009 Communication on CIIP[25] stressed the need for improved coordination and collaboration between national CIIP approaches, and indicated that there was a clear need for a new European CII governance model, possibly supported through a Public-Private-Partnership (PPP).

These reflections and viewpoints were reiterated in the Presidency Conclusions from the Ministerial conference on CIIP in Tallinn,[26] which stressed ENISA's enabling role as a possible tool to bolster cooperative efforts.

2.2.7. Need for more efficient fight against cyber crime

NIS efforts have been predominantly organized under the former first pillar. However, with the entry into force of the Lisbon Treaty, the traditional distinction between the EU's three pillars (the European Community pillar; the Common Foreign and Security Policy; and the Police and Judicial Co-operation in Criminal Matters) disappeared. In particular, the ordinary legislative procedure that applies to the policies related to the establishment and the functioning of the internal market,[27] is now also applicable (with some exceptions) to the policies related to police and the judicial cooperation in criminal matters.[28] Obviously, NIS considerations are not inherently linked to former first pillar issues, and it is clear that a

---

24 COM(2009) 149, 30.3.2009

25 COM(2009) 149, 30.3.2009

26 See the EU Ministerial Conference on CIIP (Tallinn, 27-28 April 2009) Conference conclusions; http://www.tallinnciip.eu/doc/EU_Presidency_Conclusions_Tallinn_CIIP_Conference.pdf

27 See new Article 114 of the Treaty on the Functioning of the European Union, which replaces the previous Article 95 of the Treaty establishing the European Community. This Article 95 was the legal basis of the ENISA Regulation

28 See new Article 87 of the Treaty on the Functioning of the European Union for the police cooperation and new Article 88 on Europol. See new Articles 82-84 for the judicial cooperation and new Article 85 on Eurojust

consistent European NIS policy is needed in former second and third pillar areas as well, with key examples being the need for a strong cyber defence policy (traditionally a second pillar issue) and the need for dependable cooperation in combating cyber crime (former third pillar).

The necessity of taking into account a broader task package covering also former 2nd and 3rd pillar areas was also hinted at in the aforementioned Communication on Critical Information Infrastructure Protection, which noted that "The social and economic dimensions of the process of enhancing NIS in Europe as well as the needs and strategies of law enforcement and of the fight against cyber-crime and cyber-terrorism must complement and mutually strengthen each other."

2.3. Evolution of the problem

The problems related to the possible breaches of NIS have been present for some time, but it is widely agreed that these problems and their perception by the different stakeholders are continuously evolving and have become more complicated and more pressing.

Different factors in this evolution can be identified, the main ones being presented in the following paragraphs.

2.3.1. Dependence on network and information systems is increasing and preparedness across society is insufficient

The central role that communications networks and information systems have played in economy and society in the recent past is still continuously increasing, and critical infrastructures (such as utilities) heavily depend on it for their functioning. As a result, the provision of basic necessities (including food, water and energy) can be fundamentally disrupted through NIS incidents.

At the same time, cyber attacks are less than in the past the work of lone individuals who want to prove their technological prowess or demonstrate gaps in the security of communications networks and information systems, but are increasingly performed by organisations with criminal intentions for profit or political reasons. The trend is towards more sophisticated and profiled attacks and ever increasingly more tailored to specific targets. Computer-assisted crimes (such as spamming, piracy and identity theft) have been followed by criminal behaviours that are directed against computers and networks, as in the case of Denial of Services. ICT systems are not just the tools but also the target of disruption, and damages can be very high for target organizations. This led, inter alia, to the concept of cyber defence, i.e., the awareness that the defence strategy of a country should take into account the threats to its networks. Today, however, preparedness for incidents is still insufficient. For example not all Member States have put in place well-functioning national/governmental Computer Emergency Response Teams (CERTs) or similar bodies pursuing the same purpose. Moreover, since responsibilities in securing NIS lie with everyone, it is mandatory to develop and promote a true risk management culture engaging all stakeholders to play their part.

2.3.2. Technological evolutions create new risks

The use of mobile devices and mobile based network services is continuously increasing, thereby creating new opportunities for attacks, especially if the level of security used by mobile systems is not yet comparable to that of more traditional systems (such as personal computers). Secondly, there is a trend towards ambient intelligence and cloud computing, in which intelligent devices supported by computing and networking technology will become ubiquitous. This will further enhance the connectivity and interoperability of networks, resulting in a more extensive and systematic collection of potentially sensitive data, thereby creating new risks. Also, the need for increasing interoperability of networks has not lead to

proper investment in, and deployment of, diversified systems. As a consequence attacks will have a greater impact and will spread more readily. Finally, control over specific data, software or systems is much harder to determine than in the past because of new concepts such as cloud computing, virtualization and ubiquitous connectivity. It has become more complicated to assign responsibilities and liabilities and to identify which rules or principles should apply. As regards the expected diffusion of radio frequency identification (RFID) and related identification technologies, a cornerstone of the upcoming 'Internet of Things,' unsolved issues relate to public trust and the security and privacy problems associated with the management of the vast amount of sensitive data that is collected and stored.

2.3.3. Changes in usage of ICT increase the need for adequate protection of users

The use of information and communications technology is changing since individual users are growing more comfortable with seeking out data or sharing their own personal information on-line, both consciously (e.g., through social networking sites) and unconsciously (via cookies or less legitimate tracking instruments). Even if the net impact of this development would be considered as positive, this also means that there is a growing need for the adequate protection of these users and their fundamental rights (in particular privacy and freedom of expression), by ensuring that they behave responsibly, but also by protecting them more efficiently against malicious third parties.

2.4. Who is affected, in what ways, and to what extent?

Breaches of NIS could have a very large impact, in the first place because of the central role that communication networks and information systems play in current society.

This implies that possible failures or attacks could impact on a large number of stakeholders, comprising large and small businesses, public authorities and administrations and individual citizens. In other words, anyone is concerned with and responsible for NIS.

The main impacts for **businesses** (both traditional in the ICT and other sectors as well as 'e-commerce') include:

- Damage to hardware and software which needs to be resolved by reparation or the replacement of the material;
- Damage to assets that are linked to the communications networks and information systems which are compromised, which needs to be resolved by reparation or the replacement of the assets;
- Loss of confidential data and risk of misuse of these data;
- Loss of revenue and productivity during the breach;
- Loss of market capitalisation due to negative branding from successful attacks;
- Loss of customers and/or revenue by the attacked businesses due to the negative publicity of a breach;
- Loss of customers and/or revenue by the ICT sector due to the lower take up of ICT because of the negative publicity.

The main impacts for **public authorities and administrations** include:

- Damage to hardware and software which needs to be resolved by reparation or the replacement of the material;
- Loss of confidential data and risk of misuse of these data;
- Loss of productivity during the breach;
- Loss of service provisioning for critical government functions;

- Loss of confidence of citizens in the public authorities and administrations in general and in e-government in particular.

The main impacts for **citizens** include:

- Damage to hardware and software which needs to be resolved by reparation or the replacement of the material;
- Loss of confidential and personal data and risk of misuse of these data, potentially resulting also in direct or indirect financial losses (e.g., as a result of identity theft);
- Direct financial losses;
- Reduced level of service provision by business and public authorities and administrations;
- Transfer of NIS-related costs of businesses and public authorities (cf. supra) to consumers through retail prices and taxes.

2.5. What is the scale of the problem?

As indicated already in the Commission Communication on a strategy for a Secure Information Security,[29] there is little to no objective quantitative information available about the economics of NIS, in particular the impact that NIS breaches as well as security measures to prevent or remedy attacks would have.

The IDC EMEA market study[30] estimated that the EU NIS market value will reach a value of € 15.5 billion in 2010, with an average forecast growth rate (taking the financial and economic crisis into account) of 13.1% for the period 2007-2010. According to IDC, business demand represents 94% of total spending, but consumer demand remains critical because home systems are part of the overall security chain and are essential to maintain overall trust and confidence, e.g., in the Internet.

The table below provides some more indications on the importance of the ICT market in the economy as a whole.

Indicator	Score	Year
ICT expenditure		
Information Technology Expenditure as a percentage of GDP in the EU	2,7%	2007
Communications Expenditure as a percentage of GDP in the EU	3%	2006
ICT R&D expenditure as a percentage of total EU R&D business expenditure	26,4%	2005
ICT R&D expenditure as a percentage of total EU R&D public and private expenditure	18%	2005
Average IT security spending per PC installed in the EU (hardware, software and IT services)	€55.5	2007
EU NIS total security spendings	€10,756 M	2007
ICT uptake		
Households who have Internet access at home	60%	2008
Enterprises having access to the internet	93%	2008
Individuals regularly using the Internet	56%	2008
Use of public services through ICT		
Individuals using the Internet for interacting with public authorities	28%	2008
Enterprises using the Internet for interacting with public authorities	68%	2008
Use of commercial services through ICT		
Individuals having ordered/bought goods or services for private use over the Internet in the	24%	2008

[29] See COM(2006) 251, 31.5.2006

[30] IDC EMEA, The European Network and Information Security Market, Scenario, Trends and Challenges, April 2009, with reference to the Eurobarometer E-Communications Survey, pub. April 2007

last three months		
Enterprises having received orders on-line	16%	2008
Share of enterprises' turnover on e-commerce - Enterprises' receipts from sales through electronic networks as percentage from total turnover	12%	2008
Enterprises having purchased on-line	28%	2008
Enterprises who use the Internet for banking and financial services	78%	2008
Individuals who use the Internet for internet banking	29%	2008
Mobile ICT		
Average EU mobile penetration rate	119%	2008
3G mobile subscribers as a part of total mobile operator subscribers	15,5%	2008
Percentage of EU enterprises which adopt security solutions to mobile computers	80%	2007

Sources: Eurostat – Industry, Trade and Services – Information Society; 14th Report on the Implementation of the Telecommunications Regulatory Package; The 2009 report on R&D in ICT in the European Union – JRC Scientific and Technical Report; The European Network and Information Security Market - Scenario, Trends and Challenges(IDC EMEA)

The IDC EMEA market study further indicated that 28% of the households in the EU27 had suffered from problems with spam or viruses in the last 12 months. On average, approximately 7% of business users experienced a security breach in the last year.

The Flash Eurobarometer study on Confidence in the Information Society of May 2009[31] - although it did not attempt to explore and estimate the volume of financial losses related to online security – revealed that for individuals the most often mentioned consequence of Internet security problems was the loss of time, specifically because of virus infections (slow systems, time needed to reinstall, etc.). Loss of non-personal data (e.g. damaged files, etc.) was the second most frequently reported result of Internet security problems. Direct financial losses (e.g. money stolen, computer repair, loss of valuable data) were reported by 16% of all Internet users in the EU who encountered some security problem over the past five years.

We also refer to the Impact Assessment Report for the Communication on CIIP and a number of diverse recent studies for some more quantified indications of the scale of NIS breaches:

- In the United States, consumers paid as much as 7,8 billion USD over two years to repair or replace information systems infected with viruses and spyware;[32]
- In the UK, a major loss of citizens data occurred in October 2007 as two computer discs with 25 million child benefit records, complete with sensitive personal information, were lost from Her Majesty's Revenue and Customs department;[33]
- A study on the impact of cyber-attacks on stock prices shows that identified target firms suffer losses of 1 to 5% in the days after the attack.[34]
- The Global Risk Network Report 2008 and its update of 2009[35] estimated the global economic losses of an attack or system failure in CII as in the order of magnitude of 250 billion dollar with a likelihood of occurrence of 5-10%. The 2010 report, predicts both a higher likelihood (10-20%) and magnitude (well over 250 billion). It also stresses that, as new and existing technologies are applied to critical systems, ranging from smart grids to cloud computing, a new era of complexity and risk is opening up. Therefore, the appropriate regulatory frameworks and incentives have to be implemented to ensure that

---

31 Flash EB series #250, The Gallup Organization, Hungary, May 2009

32 See the September 2006 issue of "Consumer Reports", http://www.post-gazette.com/pg/06225/712889-96.stm

33 http://www.timesonline.co.uk/tol/news/uk/crime/article4211711.ece

34 See Working document 'The Economic Impact of Cyber-Attacks and Cyber-Disruptions' – June 2008 – Prepared by DG INFSO

35 http://www.weforum.org/en/initiatives/globalrisk/index.htm

the required security technologies are integrated from the outset, rather than as an afterthought.

- In the UK, the average cost of a security incident has risen by 25% between 2006 and 2008, with large businesses reporting the average cost of their worst incident in the year to be between £90K and £170K.[36]
- 72% of respondents in the Global Information Security Survey 2008 considered significant potential for revenue loss if information was to be lost, compromised or unavailable.[37]
- Respondents to the 2008 Computer Crime and Security Survey in the United States reported a variety of NIS incidents, including 50% reporting viruses, 21% suffering Denial of Service attacks, and 20% experiencing problems with bots.[38]
- It can be concluded that communication networks and information systems play a crucial role in today's society and economy, which implicates that the impact of possible breaches and thus the scale of the problem is at the least fairly high.

2.6. How would the problem evolve, all things being equal?

The baseline scenario would consist of an extension of ENISA's mandate *à l'identique*, after its expiry in March 2012. ENISA's resources and budget as well as its tasks would remain the same as today. This would hardly allow ENISA to further develop its activities as a centre of excellence in its domain, as the limited financial and people resources will not make possible for the Agency to keep up with future cooperation and collaboration challenges. However, under the current circumstances and budgetary restrictions, it is clear that ENISA will only be able to have an impact on a very limited number of issues whereas there is a clear demand for broadening the activities of ENISA in order to cover much more areas related to NIS (e.g. the organisation of pan-European exercises).

With regard to the constant evolution in ICT, and thus an evolution in possible threats thereto, as well as with regard to what has been identified as necessary in terms of NIS in recent policy developments, ENISA would not have the means, under the baseline scenario, to adequately respond to those necessities and to keep up with the speed at which ICT security issues evolve and to assume the responsibilities which have been identified as appropriate for ENISA in recent policy developments, namely in the Action Plan of the Commission Communication on CIIP.

Lastly, an extension of ENISA's mandate *à l'identique* would pass up the chance provided by the Lisbon Treaty. It is only an extended mandate which would allow ENISA to explore and thus to support Member States, Commission and stakeholders in achieving a more holistic approach towards NIS.

2.7. Does the EU have the right to act and is EU added-value evident?

2.7.1. Right to act (legal base)

In accordance with the European Court of Justice's jurisprudence,[39] before the entry into force of the Lisbon Treaty, **Article 95 of the EC Treaty** was to be considered the appropriate legal

---

36 BERR. 2008. 2008 Information Security Breaches Survey – Technical Report. Department for Business Enterprise & Regulatory Reform. April 2008. URN 08/788

37 Ernst & Young. 2008. Moving beyond compliance – Ernst & Young's 2008 Global Information Security Survey. EYG no. AU0162. Ernst & Young Technology Risk and Security Services. www.ey.com/security

38 Richardson, R. 2008. 2008 CSI Computer Crime & Security Survey. Computer Security Institute. www.gocsi.com

basis for the creation of a body for the purpose of ensuring a high and effective level of NIS within the Community.

Enhancing the security and resilience of ICT infrastructures is thus an important element contributing to the smooth functioning of the internal market.

Under the Lisbon Treaty, **Article 114 of the TFEU** (Treaty of the functioning of the European Union)[40] describes – almost identically - the internal market competence. It will continue to be the applicable legal basis for adopting measures to improve NIS. The internal market competence is now a shared competence between the EU and the Member States (Art. 4(2) a) TFEU. This means that the EU and the Member States may adopt (binding) measures and that the Member States will act if the EU has not exercised its competence or has decided not to act anymore (Art. 2(2) TFEU).

Measures under the internal market competence will require the ordinary legislative procedure (Art. 289, 294 TFEU), which will be mostly[41] identical to the former co-decision procedure (Art. 251 EC Treaty).

With regard to the need for a more efficient fight against cyber crime, the Lisbon Treaty provides for new possibilities. Under the Lisbon Treaty, preventing and combating crime becomes a (shared) competence of the Union. The former distinction between 1st, 2nd and 3rd-pillar competences disappears. The ordinary legislative procedure will be broadly applied. Since NIS represents an important aspect in preventing cyber crime, ENISA might become a platform to build the bridge and exchange views and best practices also with cyber defence and law enforcement authorities. In case that this activity is limited to knowledge sharing with a focus on enhancing network and information security through a more holistic approach, no additional legal basis is needed. To the extent that a regulation proposal for ENISA foresaw also operational tasks in preventing and combating cyber crime (this will be examined later, cf. Chapter 4) the measure could be considered to pursue a twofold aim: to support the functioning of the internal market and to prevent and combat crime. The latter could not be considered as being inherent to the former so that the measure would have to be founded on a second legal basis[42]. This could be found in Title V TFEU. For instance, Art.84 TFEU states that "The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, may establish measures to promote and support the action of Member States in the field of crime prevention, excluding any harmonisation of the laws and regulations of the Member States." Art. 87 TFEU provides for police and law enforcement cooperation and states in its paragraph 2 that "…the European Parliament and the Council, acting in accordance with the ordinary legislative procedure, may establish measures concerning (a) the collection, storage, processing, analysis and exchange of relevant information; (b) support for the training of staff, and cooperation on the exchange of staff, on equipment and on research into crime-detection; (c) common investigative techniques in relation to the detection of serious forms of organised crime."

2.7.2. Need for intervention at EU level

It results from the problem definition that NIS is a genuine Community issue and that a public (common) NIS policy is needed.

---

39 ECJ 02.05.2006, C-217/04, *United Kingdom of Great Britain and Northern Ireland v European Parliament and Council of the European Union*

40 Cf. supra

41 The ordinary legislative procedure differs in particular in terms of majority requirements in Council and EP

42 Cf. ECJ Case C-211/01 /Commission/ v /Council/, paragraph 40, and Case C-94/03 /Commission/ v /Council/, paragraph 36)

The interdependencies between networks and information systems make it extremely difficult, if not impossible, for individual actors to correctly judge the global economic and societal impact of their (lack of) measures taken to protect against NIS breaches. Furthermore, entities (public and private, including citizens) that are completely unrelated are impacting each other. Increasing globally the ability of network and information systems to resist threats therefore requires public intervention at the European level. Uneven national policies and practices are a clear disruption of the internal market, due to the clear negative externalities resulting from NIS incidents (inadequate policies impacting markets in other Member States), but also due to the positive externalities of good NIS practices (good practices in one Member State positively impact NIS as a whole, thus creating a clear societal good). In cases where such externalities exist across Member States, European policy intervention may be justified as it provides a real added value to the functioning of the internal market.

This justification is also clearly recognised in recitals 1, 3 and 10 of the existing Regulation (EC) No 460/2004 establishing ENISA. The internal market justification is also reiterated in Article 1.1 of the Regulation, stating that the competences of ENISA aim to contribute to the smooth functioning of the internal market.

The EU's right to act and the added-value of a common European NIS policy is therefore evident. With the problem constantly evolving from a technological and market perspective, it is crucial to have reliable structures in the EU that draw on high level expertise for specific EU concerns.

2.7.3. Subsidiarity principle

European intervention in NIS policy is also justified by the subsidiarity principle. As noted in the CIIP Communication, a European complete non-intervention strategy in national NIS policies is rather akin to asking each Member State to only guard its own backyard, with disregard of the aforementioned interdependence between existing information systems. An appropriate degree of coordination between the Member States to ensure that NIS risks can be well managed in the cross border context in which they also arise does therefore respect the subsidiarity principle. Furthermore, European action would improve the effectiveness (and thus add value) to any existing national policies.

In addition, it is clear that concerted and collaborative NIS policy action can have a strong beneficial impact on the effective protection of fundamental rights, and specifically the right to the protection of personal data and privacy. European citizens are increasingly entrusting their data to complex information systems, either out of choice or out of necessity, without necessarily being able to correctly assess the related data protection risks. When incidents occur, they will therefore not necessarily be able to take suitable steps, nor is it certain that the Member States would be able to effectively address any international incidents in the absence of European NIS coordination. For this reason too, further policy action at the European level seems amply justified.

3. OBJECTIVES

3.1. What are the general policy objectives?

When defining the policy objectives to be achieved in terms of improving EU wide NIS, a distinction is made between general objectives, specific objectives and operational objectives. All policy objectives are derived from the specific problem drivers which have been identified and described or been referred to in chapter 2 above. As such, the policy objectives are defined to orchestrate the European response to the NIS problems and challenges. Therefore, they are not specific to overcome the current inefficiencies of ENISA, since the existence of

the Agency is not a goal in itself but should be seen as part of the overall efforts in the area of NIS. The following analysis will, therefore, assess to which extent the instrument of a modernised NIS agency, which is broadly recognised to be the most appropriate organisational structure, could best be shaped to contribute, together with other Union instruments, to the achievement of the policy objectives.

The **general objective** of the initiative is *to reach a highly developed capability and preparedness of the Community, the Member States and stakeholders to prevent, detect and better respond to NIS problems*. This will contribute to the building of trust which is underpinning the development of the Information Society, the improvement in competitiveness of the European businesses and the well functioning of the Internal Market.

3.2. What are the more specific/operational objectives?

A total of seven **specific objectives** for ensuring EU wide NIS have been identified. They all translate into a number of **operational objectives** to which a **description** is provided in the tables below. This allows for a detailed evaluation of what measures or instruments will finally be best suited for attaining each objective.

Objective 1: Coherence of regulatory approaches – provide guidance and advice to the Commission and the Member States to update and develop a holistic normative framework in the field of NIS.

Operational objectives 1	Description
Ensuring the adequacy and effectiveness of the regulatory framework (including hard and soft law)	Assist in the establishment of an appropriate NIS regulatory framework at EU and national levels; Provide advice on the development of security breach notification protocols and of necessary interoperability of eSignature and future eIDs; Provide advice on self-regulatory or co-regulatory initiatives with a NIS impact, including through PPPs.
Ensuring the adequacy and effectiveness of the standardisation framework	Collect information on the standardisation landscape in relation to NIS; Disseminate information on the standardisation landscape in relation to NIS to European and national bodies; Identify gaps and inconsistencies in the standardisation landscape in relation to NIS and liaise with standardisation bodies to address them.

Objective 2: Prevention, detection and response – improve preparedness by contributing to a European early warning and incident response capability, pan-European contingency plans and exercises.

Operational objectives 2	Description
Assisting Member States in proactively identifying NIS risks and vulnerabilities	Support the process of defining a minimum level of capabilities and services for national/governmental CERTs; Coordinate network security curricula and trainings; Influencing of higher-level 'operators' who can then further distribute to e.g. SMEs and individuals;
Assisting Member States in monitoring and reporting NIS incidents	Develop an early warning system for emerging risks and attacks; Support open intelligence analyses of incidents that have occurred;
Assisting Member States in establishing appropriate response mechanisms	Support the cooperation between the national systems for response to network incidents and security flaws on an EU level; Organise NIS exercises at European level based on National exercises and engaging relevant stakeholders; Create and coordinate network security initiatives for all MS.

Objective 3: Knowledge enhancement for policy makers – provide assistance and deliver advice to the Commission and the Member States to reach a high level of knowledge, throughout the EU, on issues related to NIS and its application to the industry stakeholders.

This also includes the generation, analysing and making available of data regarding the economics and the impact of NIS breaches, drivers for stakeholders to invest in NIS measures, risk identification, indicators of the state of NIS in the EU, etc.

Operational objectives 3	Description
Collecting and disseminating NIS information for the benefit of policy makers	Collect information on current and anticipated NIS risks and risk prevention technologies; Analyse current and anticipated NIS risks; Provide indicators of NIS state in the EU; Disseminate information on current and anticipated NIS risks to European and national bodies.
Acting as a NIS knowledge center for the benefit of policy makers	Provide general advice on NIS and regulatory initiatives with a NIS impact to European and national bodies with or without prior request; Monitor EU consistency in strategic goals and implementation strategies.
Organising consultations with stakeholders to support NIS policy	Organise consultations for the benefit of EU and national bodies with the following stakeholders: NIS industry, non-NIS industry, academia, consumer representatives.
Organising data collection on NIS and its social and economic implications	Develop indicators for evaluating the state of NIS in the EU (frequency of incidents, nature, impact, etc.); Develop a European framework for organising collection and comparison of data on NIS in Member States; Analyse economic drivers and hurdles for investment in NIS; Analyse the economics of NIS breaches.
Guiding and promoting NIS research efforts	Collect information on the NIS research landscape; Disseminate outputs from the NIS research landscape to stakeholders; Identify and address gaps in the NIS research landscape by advising EU bodies on high priority NIS research areas; Promote and stimulate research in high priority NIS areas; Support pan-European NIS research; Identify application domains for NIS research and promoting NIS research results in these domains.

Objective 4: Empowering stakeholders – develop a culture of security and risk management by stimulating information sharing and broad cooperation between actors from the public and private sector, also for the direct benefit of citizens and developing a culture of NIS awareness.

Operational objectives 4	Description
Establishing information exchange networks between administrations, industry and end user representatives	Establishing and maintaining contact networks between national NIS bodies at the EU level and between national NIS bodies and European bodies; Establishing liaisons between EU bodies, national bodies and industry to identify and address NIS risks and vulnerabilities related to specific products or product groups; Establishing and maintaining contact networks between NIS industry (B2B), non-NIS industry, academia and consumer bodies at EU and national levels; Leveraging these contact networks to identify NIS vulnerabilities at EU and national levels.
Informing industry and citizens of NIS issues	Collecting information on NIS risks, vulnerabilities, risk management and incident response from the perspective of SMEs, larger enterprises, private citizens and national bodies and disseminating these thereafter; Stimulate activities and studies on NIS risks, vulnerabilities, risk management and incident response by SMEs, larger enterprises, private citizens and national bodies.
Raising awareness, including by identifying and disseminating NIS good practices	Raising awareness by identifying and disseminating accessible information on NIS risks, vulnerabilities, risk management and incident response. This applies to SMEs, larger enterprises, private citizens and national bodies; Promoting exchanges of current best practices to national bodies and

	enterprises; Defining best practices for national bodies and enterprises.

Objective 5: Sheltering Europe from international threats – reach a high level of cooperation with third countries and with international organisations to promote a common global approach to NIS and to give impact to high level international initiatives in Europe).

Operational objectives 5	Description
Developing a European NIS strategy	Contribute to a high impact of high level international NIS initiatives throughout the EU
Creating an effective forum for global NIS policy	Act as a contact point to assist in information and knowledge exchange between national and European bodies and non-European bodies; Be an authoritative body for NIS of the EU to international bodies, e.g. at international bodies, gatherings or working groups.

Objective 6: Towards collaborative implementation – facilitate collaboration in implementing NIS policies.

Operational objectives 6	Description
Facilitating collaboration in policy implementation at EU level	Act as a NIS policy expertise centre at EU level; Liaise with stakeholders at EU level to ensure that European NIS policies are well aligned with current NIS threats; Support the implementation of good EU-wide NIS practices, possibly through supporting the creation of PPPs; Conduct regulatory compliance assessments (make sure regulations are followed and implemented at national level).
Assisting in the correct implementation of applicable NIS norms	Assist in and promote the correct implementation of good NIS practices and standards within CII industry stakeholders; Assist in and promote the correct implementation of good NIS practices and standards at European and national level.

Objective 7: Fighting cyber crime – develop an effective response to cyber crime through cooperation with (past) 2nd and 3rd pillar authorities, e.g., with Europol.

Operational objective	Description
Establishing and maintaining contacts with current 2nd and 3rd pillar authorities, e.g. Europol	Establish and maintain contacts with current 2nd and 3rd pillar authorities; Identify and address gaps in the overall EU NIS policy in collaboration with current 2nd and 3rd pillar authorities.
Provide support related to law enforcement	Assist in the collection of traffic data, interception of content data, monitoring flows in case of denial-of-service (DoS) attacks; Provide expertise to MS for criminal investigation including NIS aspects.

3.3. Consistency of the objectives with other EU policies

The enhancement of the security and resilience of ICT infrastructures is an important element of EU policy on NIS.

Consistency with other regulatory initiatives

On the regulatory side, the Data Protection Directive[43] requires that the entity in charge of processing personal data implements appropriate technical and organizational measures to protect this data "against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the

[43] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

transmission of data over a network, and against all other unlawful forms of processing" (Article 17). In this way, the Directive (through its national transpositions) has indirectly created an obligation for appropriate risk management and NIS practices, at least insofar as personal data is being processed in areas that fall under the scope of the Directive.

The package for amendment of the electronic communications regulatory framework reinforces the provisions related to network security and integrity. It contains provisions to strengthen operators' obligations to ensure that appropriate security and integrity measures are taken to meet identified risks as well as mandatory breach notification. It further specifies the powers of National Regulatory Authorities (NRAs) regarding NIS (e.g. auditing security measures taken by public network providers), and provides an improved framework for cooperation between the NRAs (e.g. via the Body of European Regulators in Electronic Communications (BEREC) which replaces the loose cooperation between national regulators that existed in the "European Regulators Group" with a better structured, more efficient approach) and the Commission with ENISA on a number of security matters. The new provisions will come into force following the conciliation agreement reached on 5 November 2009.

With regard to the e-Signature Directive[44] a number of practical, technical and organisational requirements still need to be met to establish the interoperability of electronic signatures.[45] The Commission has proposed, willing to address the lack of a comprehensive political framework an Action Plan on electronic signatures and electronic identification[46] which aims at achieving such interoperability. This will contribute to enhancing the security of electronic communications and building trust.

Other regulatory initiatives have had a similar direct or indirect effect: the Convention on Cybercrime was one of the main inputs for the 2005 Council Framework Decision on attacks against information systems,[47] creating an obligation for Member States to implement a contact network available 24 hours a day and seven days a week to support the coordination of investigative initiatives.

Consistency with non-regulatory initiatives

EU initiatives with a NIS impact are of course not limited to strictly regulatory initiatives. For instance, there is security-related research in the European Community Framework Programmes devoted to Research and Development – e.g. FP7 European Security Research Program (ESRP), Safer Internet Plus programme, etc.

Coordination between existing national NIS organisations is also organised through the collaboration between the multitude of CERTs established at the national level[48]. The European Governmental CERTS Group (EGC)[49] was established as an informal group of

---

44 Directive 1999/93/EC, OJ L 13, 19.01.00, p.12 and the Report on the operation of e-Signatures Directive COM(2006)120 final.

45 Cf. Report from the Commission to the European Parliament and the Council: Report on the operation of Directive 1999/93/EC on a Community framework for electronic signatures, COM(2006)120, 15.3.06

46 Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions on an *Action Plan on e-signatures and e-identification to facilitate the provision of cross-border public services in the Single Market*, COM(2008)798 of 28.11.08

47 Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems

48 See http://www.enisa.europa.eu/cert_inventory/index_inventory.htm

49 See http://www.egc-group.org

governmental CSIRTs,[50] aiming to improve the effectiveness of its members by sharing good practices and guidelines. Similarly, the Trans-European Research and Education Networking Association (TERENA)[51] has established a Task Force[52] called TF-CSIRT that acts as a forum between CSIRTS, and the Forum for Incident Response and Security Teams (FIRST)[53] plays a similar role at the international level. ENISA has been active in the past to support these efforts[54] as well, including through the establishment of ad hoc working groups.[55]

Consistency with the objectives of initiatives under (former) 2nd and 3rd pillars

While ENISA was established within the former first pillar, there are also a number of (former) third pillar organisations addressing NIS issues, including the European Police Office (Europol)[56] and the European body for the enhancement of judicial co-operation (Eurojust),[57] whose tasks include the coordination of cooperation between respectively law enforcement agencies and judicial bodies in the Member States (including in NIS-related areas, i.e., cybercrime).

In the former second pillar (Common Foreign and Security Policy) as well, several initiatives exist which impact NIS concerns, including the European Defence Agency (EDA)[58] and the European Union Institute for Security Studies.[59] The EDA aims to support the development of European defensive capabilities, which will certainly include a greater focus on cyber defence mechanisms in the future, and acts as a think tank for a common European security culture.

The Stockholm Programme adopted by the European Council on 11 December 2009[60] considers that "the Union should promote policies and legislation that ensure a very high level of network security and allow faster reactions in the event of cyber attacks." The competences of Europol are enhanced. An Observatory for the Prevention of Crime should be set up, the tasks of which will be to collect, analyse and disseminate knowledge on crime and crime prevention and to support and promote Member States and EU institutions when they take preventive measures and to exchange best practices. In this context, the present initiative to enhance the security and resilience of networks and ICTs in the EU plays an important role.

Conclusion

All of these initiatives and their positive contributions to NIS awareness have been applauded in the past years. Regulations however focus on creating high level obligations, but leave a significant margin of appreciation for their actual implementations, leaving room for an uneven NIS landscape in practice, even within a strictly European context. There is an overall feel that further initiatives are needed in order to cope with the evolving challenges of NIS, and specifically to ensure that existing policies have a sufficiently high operational impact in practice.

This initiative is therefore fully coherent with the general debate on NIS and other policy initiatives that focus on the future of NIS. As pointed out earlier, it is one of the main

---

50 Computer Security Incident Response Teams
51 See http://www.terena.org
52 See http://www.terena.org/activities/tf-csirt/
53 See http://www.first.org
54 See http://www.enisa.europa.eu/cert_cooperation/index_cooperation.htm
55 See http://www.enisa.europa.eu/pages/03_04.htm
56 See http://www.europol.europa.eu
57 See http://www.eurojust.europa.eu
58 See http://www.eda.europa.eu
59 See http://www.iss.europa.eu
60 See http://www.consilium.europa.eu/uedocs/cms_Data/docs/pressdata/en/ec/111877.pdf

components of the European Digital Agenda, the latter being a flagship initiative of the Europe 2020 strategy.

3.4. Consistency with horizontal objectives

This initiative will contribute to the protection and the promotion to fundamental rights, in particular to the protection o personal data and privacy (due to the enhanced level of security infrastructures which are more and more used to store and process such data). It also contributes, by securing vital societal infrastructures and thus creating trust into modern means to communicate and also learn, to a competitive, dynamic and knowledge-based economy. Economies of scale may lead to reduced power consumption and thereby less emissions if investments in secure infrastructure follow a coherent, European approach. The initiative thus supports also the Sustainable Development Strategy.

4. POLICY OPTIONS

4.1. Preferred structure

A number of possible organisational formats to implement the above policy options have been examined in Annex IV, including i) an agency, ii) a more or less formalised Public Private Partnership (PPP), iii) an informal contact network, iv) a permanent network of competent bodies and v) a direct integration into Commission services.

A PPP would provide more flexibility and would be beneficial for ensuring that public policy efforts and innovative research efforts are brought in line. At the same time, the setting up of a PPP would be difficult if there are not sufficient benefits for the private sector to join. An informal contact network would also have the flexibility advantage; however, it would be difficult to exercise any policy guidance towards such network which makes it ill-suited for a high priority policy area like NIS.

A permanent network of competent bodies would serve well as a facilitator for cooperation among Member States on specific technical matters relevant to NIS. However, such network would have a complex legal framework, little flexibility; no direct involvement of the various stakeholders and, last not least, the European dimension of the NIS issues at stake may be overshadowed by the national priorities of individual Member States.

Informal contact networks are very flexible and well suited in contexts where the existing stakeholders have strong incentives to participate. However, due to their informal nature, it is difficult to exercise any policy guidance, which makes them ill suited for high priority policy areas. In addition, they are dependent on the commitment of their members, and over time risk becoming unstable and ineffective.

Integration of ENISA's tasks into the Commission's services would offer the benefit of direct control and better alignment with the EU policy priorities. On the other hand, due to the organisational set-up of the Commission and the specialised technical competences required, it would be very difficult to organise the Agency's tasks within the competence of a specific Directorate General.

The Agency format is best suited as the policy instrument of choice because it brings the following advantages:

– There is a clear legal basis for a use of the Agency format in Article 114 TFEU, which has been confirmed by the Court of Justice.[61] This is an important advantage in comparison to

[61] Judgment of 2 May 2006 in Case C-217/04

some of the other formats, as it makes the organisational structure less likely to be challenged on legal grounds.

– The advantages of an Agency format map well to the specific concerns in the NIS sector:
    - An Agency allows certain functions to be delegated to an external expert body, separate from the Commission and the Member States, which is has a certain degree of flexibility to develop its own agenda and working methods within the remit of its mandate using the know-how of specific experts in the field. An Agency has the possibility to establish its own unique identity and reputation towards the targeted stakeholders, and thus attract more easily the required expertise.
    - The Agency format helps to establish more easily close and permanent relationship with stakeholders and is therefore well suited for coordinating initiatives in the field of NIS.
    - An Agency format can be an advantage as regards sensitive policies that Member States are unwilling to delegate to the European level. This is particularly relevant in concepts where ENISA would be given a stronger operational role, since this is an area where Member States with strong NIS traditions are less likely to be willing to abandon their positive influence.
– As an Agency, ENISA has already found a significant degree of acceptance in the European NIS community, as shown in the 2007 evaluation.[62] This was also confirmed in the contributions to the public consultation on the future of ENISA. Most respondents agreed that an agency would still be the right instrument to deal with challenges in NIS. An Agency has been generally valued for providing information exchange on best practice, a useful platform for dialogue with stakeholders, particularly with industry and coordination with Member States.

4.2. Possible options for meeting the objectives and tackling the problem

Following a pre-screening of options, as described in annex 3, a list of five policy options is presented.

POLICY OPTION	**DESCRIPTION**
OPTION 1: No policy	ENISA mandate expires and leads to two sub-options: a) no more policy b) other mechanisms at EC/EU level (like task force etc.).
OPTION 2: Continuation à l'identique	On 14 March 2012, the mandate of ENISA is further extended à l'identique.
OPTION 3: Expansion of the functions currently defined for ENISA, adding law enforcement and privacy protection agencies as fully fledged stakeholders	The role of a NIS agency is expanded, focussing on: • Building and maintaining a liaison network between stakeholders and a knowledge network, to ensure that the NIS agency is comprehensively informed of the European NIS landscape; • Being a NIS support centre for policy development and policy implementation (in particular with respect to e-privacy, e-sign, e-ID and procurement standards for NIS); • Supporting of the EU CIIP & Resilience policy (e.g. Exercises, EP3R, European Information

62 http://ec.europa.eu/dgs/information_society/evaluation/studies/s2006_enisa/docs/final_report.pdf

	Sharing and Alert System, etc.) • Setting up an EU framework for the collection of NIS data, including develop methods and practices for legal reporting and sharing. • Studying and reporting on the economics of NIS. • Stimulating cooperation with third countries and international organisations to promote a common global approach to NIS and to give impact to high level international initiatives in Europe. • Non-operational tasks related to NIS aspects of law enforcement and judicial cooperation.
OPTION 4: Adding operational functions in fighting cyber attacks and response to cyber incidents	Same as OPTION 3, including operational functions: • Taking a more active role in EU CIIP; e.g. related to incident prevention and response, specifically by acting as an EU NIS CERT and by coordinating between national CERTs as a EU NIS Storm Centre (incl. both day-to-day management activities as well as handling emergency services)
OPTION 5: Adding operational functions in supporting law enforcement and judicial authorities in fighting cyber crime	Same as OPTION 4, including tasks related to: • Providing support related to procedural law (cf. Convention on Cybercrime): e.g., collection of traffic data, interception of content data, monitoring flows in case of denial-of-service (DoS) attacks; • Being a centre of expertise for criminal investigation including NIS aspects

5. QUALITATIVE ANALYSIS OF THE POLICY OPTIONS

5.1. Overall assessment of the policy options

5.1.1. Option 1: No policy

Under the option "No policy," ENISA will cease to exist on 14 March 2012 and no other EU institution or bodies will take over all or part of ENISA's current activities.

This would imply that the investments made so far in setting up an organisation that is capable of attracting highly specialised people, in building up experiences, in creating networks with and between stakeholders and with international institution would simply disappear a moment that they have reached a high potential.

The need for a strong European NIS agency to support the achievement of the EU NIS policy objectives has first of all been confirmed by the explicit role that was given to ENISA in the Action Plan in the Communication on CIIP and the reformed regulatory framework for electronic communications.[63] Furthermore, also for other NIS topics, general support was found among the stakeholders for a more important role for a European NIS agency.

[63] See http://eur-lex.europa.eu/JOHtml.do?uri=OJ:L:2009:337:SOM:EN:HTML

Finally, discontinuing a NIS agency as a policy instrument would give the wrong signal to the public at large, as it might lead to the conclusion that NIS is not regarded as an important topic.

5.1.2. Option 2: Continuation à l'identique

Option 2 represents the continuation of the same policy instrument in an identical form and with the same resources and thus the baseline scenario. As foreseen in the ENISA Regulation, an evaluation was made at the end of 2006. It should be noted that this evaluation was carried out only one year after ENISA had become operational.

The evaluation made by an independent panel of experts[64] confirmed the validity of the original policy rationale behind the creation of an agency and its original goals. Recommendations were made in the report of the panel of experts, by the ENISA Management Board and by the Commission to deal with the identified weaknesses and threats in the short and medium term. The implementation of these recommendations in the following years led to a stronger focus of the activities (amongst others through the introduction of Multi-annual Thematic Programmes or MTPs). Overall, there seems to be a general consensus that, since 2006, ENISA has matured in a very positive way and has become a centre of excellence in its domain.

However, the overall expectations of stakeholders regarding what a NIS agency should be doing seem to be continuously increasing. Despite the positive effect of the MTPs on ENISA's impact, this situation is threatening the confirmation of ENISA's reputation and its recognition as a European centre of excellence that is at the availability of all stakeholders. For example, if the situation today in which ENISA, already on cruising speed, needs to refuse regularly requests for assistance or advice would last for too long, stakeholders may end up by concluding that ENISA is not able to take on its role.

The current MTP is ending in 2010 and a new programme is currently being discussed. Referring to the role that is reserved for ENISA in, e.g., the Action Plan of the CIIP Communication, in the upcoming period high priority will further be given to activities related to resilience. However, the volume of work and resources required e.g. for the organisation of pan-European exercises would imply that very few possibilities are left for working on other topics that are also indicated as priorities in the draft proposal for ENISA's strategy for 2010-2012. These are:

– The creation of a knowledgeable and pro-active NIS community throughout Europe;
– The development of a secure infrastructure and services;
– The establishment of a framework for managing identity, accountability and trust;
– Ensuring an economically efficient approach to securing information systems.

Under the current circumstances and budgetary restrictions, it is clear that ENISA will only be able to have an impact on a very limited number of issues whereas there is a clear demand for broadening the activities of ENISA in order to cover much more areas related to NIS. This situation could make it extremely difficult for ENISA to further evolve and take up its role of centre of excellence.

---

64 http://ec.europa.eu/dgs/information_society/evaluation/studies/s2006_enisa/docs/final_report.pdf and COM(2007)285 final

5.1.3. Option 3: Expansion of the functions currently defined for ENISA and adding law enforcement and privacy protection agencies as fully fledged stakeholders

Under the third option, the Agency would dispose of the resources necessary to perform all activities foreseen in its strategic plan in a satisfactory in-depth way, i.e., allowing for a real impact. The tasks would however not include operational tasks, which is consistent with the Management Board recommendations regarding eventual appropriate changes to Regulation 460/2004[65]. In addition, a number of non-operational functions related to trans-pillar activities will be added. The building of bridges to the other former pillars would in practice boil down to the enlargement of the scope of the Agency's stakeholders with a whole range of mainly former 3rd pillar actors. Examples of non-operational tasks consist of e.g. bi-directional exchange of information and training (e.g., in cooperation with the European Police College CEPOL).

In general, it is felt that the adding of a number of non-operational tasks is needed in the process of evolving towards a more holistic approach to NIS and that a trans-pillar or "integrated" approach would be more efficient in the fight against cyber crime (cf 2.2.7).

The major difference with option 2 is thus that focusing on some priorities would not be done at the detriment of other activities. With more resources available, the Agency could take a much more pro-active role and take more initiatives to stimulate active participation by the stakeholders. Moreover, this new situation would allow for more flexibility to react quickly to changes in the NIS environment. In practice, this would also imply that the Agency would be able to better distribute its resources to the benefit of all categories of stakeholders. After all, it was pointed out by different stakeholders that ENISA is today mostly offering services to the European Commission and Member States. Relations with private stakeholders (businesses as well as citizens) have been much less frequent and rather at an ad hoc basis, often with individual organisations, and thus not systematically involving business sector federations or consumer interest groups. Under option 3, the Agency would be able to expand its activities in this direction in order to intensify European efforts to raise the awareness of all stakeholders about NIS risks and challenges (cf 2.2.4).

Under this option, the Agency would act as a NIS support centre for policy development and policy implementation, more specifically with respect to e-privacy, e-sign, eID and procurement standards for NIS, which would contribute to reducing the diversity and fragmentation of national approaches to NIS (cf 2.2.1).

Option 3 would also give the Agency a more prominent role in support EU dialogue and cooperation with third countries and international organisations. Such cooperation is a prerequisite for addressing efficiently NIS problems and challenges, insofar as they are global by nature (cf 2.2.5). Since different countries assign different importance to NIS issues, by intensifying international cooperation, the Agency could help promote EU policy priorities at the international level and advocate a common global approach to NIS.

Further examples of activities in which the Agency could play a much more important role in case its resources would be increased are presented below. A further cost-benefit analysis of some of them is presented in annex 7.

---

[65] See Recommendation 2: the scope of the Agency should not be materially changed http://www.enisa.europa.eu/about-enisa/structure-organization/management-board/minutes-decisions-1/decision_09.pdf

European PPP[66]

The Commission Communication on CIIP proposed the establishment of a European Public-Private Partnership for Resilience (EP3R)[67], which provides a collaborative approach for ensuring adequate policy implementation by engaging all relevant stakeholders (cf 2.2.6). As a neutral European platform, the Agency could play the role of a mediator in bringing together parties with common interests but which do not have the kind of bi-lateral relationship that makes direct contact obvious (e.g. competitors in the same business sector). Taking up this role, the Agency will first of all need to build up trust with all parties involved, obtain a good understanding of the real need of both public and private partners and thus of the actual interest a party has in participating to the EP3R. The Agency could also play a role in raising the awareness of stakeholders regarding what is at stake and what could be the benefits for them.

Stimulating the creation of an EP3R and facilitating its functioning can soon get very time and resource consuming, so a well-considered selection of subjects for a EP3R and of the exact model of collaboration will be of the utmost importance. Topics in which private partners could be particularly interested in are related to e.g. risk management and the development of secure software.

There is a real opportunity for the Agency to come up with a state of the art model for a well-functioning EP3R. Being a pioneer regarding such an initiative, the Agency could then easily increase its reputation, become an example for other regions and thus easier establish international relations and also become more attractive to highly qualified staff.

Organisation of pan-European exercises

A number of European countries are already organising national exercises or even involve neighbouring countries for setting up cross-border or regional exercises. Exercises are an important step towards improving European early warning and incident response capability (cf 2.2.2). There remains however an important role to be played at the European level since not all MS are organising exercises yet whereas pan-European exercises still do not exist. The role of the Agency could thus be related to both helping MS to set up exercises e.g. by assisting in the development of scripts and scenarios as well as to supporting the organisation of pan-European exercises. These latter will of course not involve all MS at once, but different exercises could focus on specific regions on the interdependencies between specific MS. Also, a gradual approach would allow the Agency to fully benefit from experiences based on some smaller exercises first, while building up a team that would at the end be in a position to support the organisation of regular exercises in different regions.

Setting up of a framework for the collection of data on NIS

Very little data is available today on the actual impact of NIS and of the measures taken to prevent threats. The Agency could contribute to improve the availability of reliable data and increase knowledge about evolving NIS problems (2.2.3) by setting up of a framework for systematic data collection with full respect to any possible confidentiality issues. The contributions could consist in defining and structuring of quantitative parameters for the assessment of specific impacts, ensuring comparability of information regarding different MS, aggregation of trends at the EU level, etc. The need to put NIS at the higher strategic level is

---

66 See COM(2009)615, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Mobilising private and public investment for recovery: developing Public Private Partnerships

67 See COM(2009)149

getting more and more widely shared. The availability of more detailed data on NIS should provide the required information to policy makers and business managers in order to develop economically efficient approaches to securing information systems. This implies that research needs to be performed regarding the definition and categorisation of risk profiles since e.g. the nature of the activity of a company could have a much higher impact on the security risks of a company than the actual size of the company.

Providing support to national CERTs

Finally, under the third option, the Agency would also continue facilitating the setting up of national CERTs, in order to strengthen further the European early warning and response capability (cf 2.2.2). Currently, a study is being prepared by ENISA regarding the role of national CERTs and identifying best practices related to possible models. In addition, WPKs for 2010 consist of further facilitating cooperation between CERTs and stimulating information sharing. It can be expected that in 2012, most countries will have their governmental CERTs as well as CERTs for the main sectors or businesses in place. A big majority of the stakeholders interviewed shares however the opinion that also after this initial set-up phase, an important role for ENISA as a platform for exchange of information and provision of expert advice for the national CERTs will remain.

On the organisational side, option 3 is intended to provide more flexibility, adaptability and capability of the Agency to focus. A list of functions would replace the detailed and exhaustive list of tasks under the current Regulation. The positioning of the Agency in the EU regulatory process would be improved by providing the possibility for the EU institutions and bodies to refer to the Agency for assistance and advice. The Agency would have a strengthened governance structure whereby the supervisory role of the Management Board of the Agency, in which the Member States and the Commission are represented, would be enhanced. Certain procedures that have shown to be unnecessarily burdensome would be simplified in order to give the Agency more flexibility in its activities.

5.1.4. Option 4: Adding operational functions in fighting cyber attacks and response to cyber incidents

Compared to the previous options, Option 4 would imply that an important operational pillar of activities is added to the Agency's task package. The operational tasks could relate to the EU institutions (e.g. being the CERT for EU bodies), but could also be with respect to the Member States. They could consist of both day-to-day management activities, such as monitoring and collection of data on trends in attacks, and handling emergency services.

Interviews with stakeholders have shown that there are clear advantages of having operational capacity at the European level, e.g. in terms of speeding up communication among Member States in case of a cross-country attack, including overcoming language issues, etc.

One of the main questions is whether or not NIS-related operational activities at the EU level should be included in a separate entity (forming a kind of operational equivalent for ENISA) or if they should be integrated in a much bigger Agency. An important factor when reflecting on this question is the fact that the people involved in the operational activities do have quite a different mindset and profile then the current staff working at ENISA. Depending on the exact operational functions that would be defined, it cannot be excluded that e.g. vetting[68] would be required for people having access to certain networks and information. This would further

[68] Vetting refers to a process of examination and evaluation, generally referring to performing a background check on someone before offering him or her employment

complicate the practical organisation of an integrated institution that has both non-operational and operational responsibilities.

5.1.5. Option 5: Adding operational functions in supporting law enforcement and judicial authorities in fighting cyber crime

Option 5 includes, in addition to the functions attributed to the Agency under option 4, both non-operational and operational functions related to trans-pillar activities. The non-operational trans-pillar functions would be the same as under option 3.

The operational tasks would mainly relate to the law enforcement domain. Referring to the Convention on Cybercrime,[69] they could relate to Procedural law at the European level[70] and include, e.g.:

- real-time collection of traffic data;
- search and seizure of stored computer data;
- interception of content data.

The Agency could also function as a centre of expertise for criminal investigation including NIS aspects (e.g., phishing attempts, hacking of e-banking applications, cyber terrorism). The Agency could then put experts at the disposal of MS for contributing to complex investigations by providing for example specific encryption expertise.

5.2. What are the likely economic, social and environmental impacts of each of the short-listed options?

The impact on the different stakeholders of the specific role a modernised Agency would have under each shortlisted policy option is assessed in three different dimensions: economic, social and environmental.

The determination of the expected impacts per policy option is the result of expert assessment based on desk research of data from the stakeholder consultations and other publicly available information, as well as on a number of face to face and telephone interviews with diverse stakeholders selected on the basis of their expertise in the NIS domain. The assessment of all of the impacts under each of the options is done by analysing the magnitude of the expected impact expressed as follows:

---	very negative impact
--	negative impact
-	slightly negative impact
0	no impact
+	slightly positive impact
++	positive impact
+++	very positive impact

Option 2 ‘continuation of ENISA à l’identique’ is taken as the ‘baseline scenario’ against which the impacts of all options are assessed as it represents a situation in which the current state of affairs is maintained.

---

69 See http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm

70 See Section 2 of the Convention on Cybercrime http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm

Impacts / Options	Option 1	Option 2	Option 3	Option 4	Option 5
Economic					
Increased availability of information on current and future challenges and risks for security and resilience	--	0	++	++	++
Non-duplication of efforts in collecting relevant information on risks, threats and vulnerabilities by each individual Member State	--	0	+	+	+
Increased level of informedness of policy makers when making decisions	-	0	++	++	++
Increased quality of NIS policy provisions in Member States due to dissemination of best practices	-	0	++	++	++
Economies of scale in responding to incidents at EU level	-	0	++	+++	+++
More investments triggered by common policy objectives and standards for security and resilience at EU level	-	0	+	++	++
Lower operational risks for business due to higher level of security and resilience	-	0	+	++	++
More coherent measures to fight cyber-crime	-	0	++	++	+++
Social					
Higher trust of users in Information Society services and systems	-	0	+	+	++
Increased trust in the functioning of the EU Internal market by achieving higher levels of consumer protection	-	0	+	+	++
Increased exchange of information and knowledge with non-EU countries	-	0	++	++	++
Better safeguarding of EU fundamental human rights through ensuring equal levels of protection of EU citizens' personal data and privacy.	-	0	++	++	+++
Environmental					
Reduced impact of CO2-emmissons due to, e.g., less travel resulting from higher reliance on the use of ICT systems and services and lower power consumption resulting from economies of scale in implementing security obligations.	-	0	+	+	+

The largest impacts resulting from the initiative are to be seen at the economic and social level. The environmental impacts are indirect and their scale would be marginal for all options.

The analysis reveals that option 1 would produce negative impacts across all dimensions. While the actual severity of these impacts is hard to estimate, it is evident that the situation would worsen vis-à-vis the baseline scenario.

For the purpose of comparison, the value of the impacts for the second (baseline) option has been set to zero. However, it has to be noted that in reality this option would lead to worsening of the NIS situation in the long run. Because of the evolving nature of the identified problem drivers the Agency would need to address them in a flexible manner in order to preserve the current status quo. However, the mandate and the resources available to the Agency do not give it sufficient degree of flexibility to adjust its activities to actual needs. The Agency would not be able to keep up with the need to provide information or best practices on all relevant aspects of security and resilience, as a result of which policy makers would not be informed adequately when making decisions. This would reduce the availability of reliable data and the awareness of NIS risks and challenges and may result in greater diversity and fragmentation of national approaches to NIS.

The preferred policy option should therefore be sought among options 3 to 5 which all bring a number of positive impacts especially at the economic level.

Under option 3, by acting as a NIS support centre for policy development and policy implementation a modernised Agency would contribute to increased availability of information on current and future challenges and risks; more efficiency in the collection of relevant information on risks, threats and vulnerabilities by each individual Member State; better information-based policy making and higher quality of NIS policy provisions in Member States. This would help to reduce the fragmentation of national approaches and increase the overall awareness about NIS risks and challenges.

The role of a modernised Agency in helping MS to set up pan-European exercises would contribute to achieving economies of scale in responding to incidents at EU level thereby enhancing the early warning and response capability in Europe.

By facilitating the functioning of EP3R, which brings together public and private stakeholders, a modernised Agency would contribute inter alia to better information-based policy making by all stakeholders about NIS issues; to more investments triggered by common policy objectives and standards for security and resilience at EU level. The Agency would ensure the running of adequate collaboration models whereby stakeholders would be empowered to participate efficiently in resolving NIS problems.

The setting-up of a EU framework for the collection of NIS data and the study of the economics of NIS will bring additional economic impacts and would directly contribute to improve the availability of reliable data and increase the awareness of NIS risks and challenges.

The role of a modernised Agency in stimulating cooperation with third countries and international organisations to promote a common global approach to NIS would result in increased exchange of information and knowledge with non-EU countries and will ensure that Europe is better protected from international threats. Conversely, third countries will benefit from the positive externalities of having a more secure European cyberspace and increased availability of good NIS practices.

The non-operational tasks related to NIS aspects of law enforcement and judicial cooperation would lead to coherent measures to fight cyber-crime.

In addition to the impacts to be achieved under option 3, option 4 would produce stronger impact at the operational level. By acting as an EU NIS CERT and by coordinating between national CERTs the Agency would contribute to e.g. higher economies of scale in responding to incidents at EU level and lower operational risks for business due to higher level of security and resilience. This means that option 4 would address more adequately the objective of ensuring prevention, detection and response at EU level.

With the addition of operational functions in supporting law enforcement and judicial authorities option 5 would achieve higher effectiveness in fighting cyber crime compared to options 3 and 4.

It has to be noted, however, that while options 4 and 5 would have stronger positive impacts compared to option 3 there are certain considerations which make them less acceptable. Including operational tasks into a broadened mandate for a modernised Agency under option 4 could very soon create new ambiguities on the main objectives and priorities as well as regarding the positioning of the Agency. Moreover, since ENISA is still in the process of reaching its full potential as a centre of excellence for non-operational tasks, adding new and completely different operational responsibilities would be very challenging in the short run. Most of the stakeholders interviewed, confirmed that adding major operational responsibilities should be considered with the utmost caution. A few stakeholders did however mention the possibility of adding limited operational tasks to a modernised Agency; mainly on a project basis. These could be related to the set-up of a European platform, linking

MS databases and facilitating interoperability of eID. Finally, having operational in-house capacity would lead to a further transfer of core technical expertise between practitioners and engineers providing assistance to policy makers.

Concerning option 5, adding a "trans-pillar" operational role to the responsibilities of a modernised Agency would further reinforce the disadvantages of combining operational with non-operational responsibilities pointed out under option 4. It is to be expected that at this stage, the agency would not be best suited to take up these additional responsibilities. There is a significant risk that the Agency would not be able to fulfil these kinds of tasks properly in a reasonable time-span for getting operational and becoming the reference point for this assistance.

6. COST EFFECTIVENESS ANALYSIS

The objective of the cost-effectiveness analysis is to evaluate if the potential impacts of the short-listed policy options presented above can justify the costs of their implementation. To that end, an assessment is made with reference to the current budget attributed to ENISA.

6.1. Assumptions taken for estimating the future budget

The following general assumptions were taken when estimating the required budget for all of the possible future options for the Agency. In addition, the analysis of budgetary estimates for the different options for the Agency will take into account, where appropriate, the need to ensure continuity with the current ENISA:

- The estimations for the budgetary requirements for the Agency are provided for a period of 5 years (2012-2016). As regards 2012 and 2013, the budget estimations for the different options are aligned with the amounts set in the financial framework. This poses certain constraints, since the maximum allowed margin for deviation from the financial framework is 10%. Therefore, the actual implementation and impact of those policy options which foresee extension of the tasks of the Agency, and respectively of its resources, would start only in 2014. This would mean a dynamic evolution of resources between the estimated situation in 2013 and the targeted situation at the end of 2016;
- The average staff expenditure (excluding recruitment expenditure) in 2009 is EUR 90.659 for an operational full-time equivalent (FTE) and EUR 55.906 for an administrative FTE[71];
- It is assumed that the Greek Authorities will continue to cover the lease cost of the Agency's offices;
- the Agency will not generate itself any revenues based on e.g. fees charged to stakeholders that make use of its services to offset a part of its costs;
- An annual deflator[72] of 2% is applied on the fixed costs in the budget;
- Since staff members will move to higher steps and higher grades in the establishment plan, an additional yearly 2% increase of the salary cost is assumed in order to take into account career evolution;
- Third country contributions from EFTA account for 2,4% on top of the budget that is allocated by the European Union to the Agency. This corresponds to a contribution by the EFTA countries of 2,34% of the total budget for the Agency.

---

[71] This estimation is based on the indication given that today, the cost related to the administrative staff (representing 20 persons out of a total staff of 57) corresponds approximately to 25% of the total staff expenditure as the people from the administrative staff have usually lower grades

[72] The annual deflator reflects the estimated impact of inflation

– The estimations are based on the assumption that the meetings of the Management Board, the Permanent Stakeholders Group and various stakeholders will take place in ENISA's premises in Athens.

6.2. Estimation of budget requirements for the policy options

6.2.1. Option 1: No policy

The direct costs for the EU budget of not extending the mandate of ENISA after March 2012 would be EUR 0, which implies thus a cost saving of approximately EUR 8,5 to 9 million yearly. Abstraction is made of any possible cost of e.g. re-allocating staff and the removal of infrastructure and all miscellaneous administrative requirements for ending ENISA's activities.

Evaluation of the effectiveness of the budget

The positive effects on the EU budget are only one aspect of the assessment. Given the nature of the problem and its evolution, the Member States would need to ensure at least a minimum coordination at EU level. The current coordination efforts made by working together through ENISA would need to be replaced by more multilateral contacts between Member States. This would lead to a duplication of efforts and costs, missed synergies and a loss of economies of scale.

Even a rough estimation confirms that the direct extra costs for the individual Member States would be quite high. Each Member State would have to dedicate at least 2 FTE having a coordination role. This implies that at least (2 * 27) = 54 FTE would be dedicated in total, which already exceeds the current staff of ENISA. In addition, Member Sates would need to commit a certain number of national experts to assist on technical matters, and possibly an additional budget for the involvement of external experts or outsourcing of projects. Therefore, it can be expected that the sum of costs to be borne by the Member States in case ENISA is discontinued, will exceed the budget required currently for Agency.

Moreover, keeping in mind the need for intervention at the EU level, the national NIS representatives would not be in a position to pursue the EU NIS policy objectives and ensure coherence of the regulatory approaches in the same way a European Agency could do this.

6.2.2. Option 2: Continuation à l'identique

The current establishment plan foresees 44 posts. This number is further completed by 13 contract agents. Out of the 57 FTE's in total, 20 staff members are administrative. Under this option, the number of staff will not change. The total EU budget attributed to the Agency would remain approximately the same after March 2012 as it is today, i.e. 8,4 to 9,1 million EUR in total.

The total budget is adjusted with an overall annual deflator of 2%. At the same time, the salary costs increase by additional 2% in order to reflect career evolution. This leads to a further reduction in the share of the budget that remains for Title 3 (Operational activities). Moreover, a number of costs under Title 3, related to "Group Activities" and "Other Operational Activities" can be considered to be fixed. Therefore, the balance that remains for operations of the Cooperation & Support and Technical Department becomes very limited (See annex 5 for a more detailed overview). This remaining balance amounted to EUR 1.150 thousand in 2009, and is expected to gradually decrease from EUR 1.320 thousand to EUR 991 thousand between 2012 and 2016.

Overview of budget under OPTION 2										
	Budget 2012	**%**	**Budget 2013**	**%**	**Budget 2014**	**%**	**Budget 2015**	**%**	**Budget 2016**	**%**
Administrative staff	20		20		20		20		20	
Operational staff	37		37		37		37		37	
TOTAL	**57**		**57**		**57**		**57**		**57**	
Breakdown of total budget										
EU Budget	***8.420.000***		***8.590.000***		***8.755.361***		***8.930.468***		***9.109.077***	
Third country contributions (EFTA)	*202.080*		*206.160*		*210.129*		*214.331*		*218.618*	
Total budget for the Agency	**8.622.080**		**8.796.160**		**8.965.489**		**9.144.799**		**9.327.695**	
Breakdown of total expenditure										
Title 1 - Staff expenditure (including recruitment expenditure)	5.497.417	64%	5.717.314	65%	5.946.007	66%	6.183.847	68%	6.431.201	69%
Title 2 - Costs associated to the functioning of the Agency	536.417	6%	547.145	6%	558.088	6%	569.250	6%	580.635	6%
Title 3 - Costs related to operational activities	2.588.246	30%	2.531.701	29%	2.461.395	27%	2.391.703	26%	2.315.860	25%
Total expenditure	**8.622.080**	**100%**	**8.796.160**	**100%**	**8.965.489**	**100%**	**9.144.799**	**100%**	**9.327.695**	**100%**

Evaluation of the effectiveness of the budget

Keeping the same budget level for the period after 2012 would not allow the Agency to perform all its functions satisfactorily. Moreover, as the Agency is currently still confirming its role while further evolving towards a centre of excellence, there is a real risk that a lack of resources in this crucial phase would turn back the positive trend that was observed in recent time, as well as endanger the continuity of ENISA and would weaken its reputation and role as a point of reference on NIS issues. At the end, the rational behind the Agency's existence could be questioned. This would clearly be at the detriment of the stakeholders given the increased importance of NIS at the EU level and no other organisations being available to take over the Agency's functions.

6.2.3. Option 3: Expansion of the functions currently defined for ENISA, and adding law enforcement and privacy protection agencies as fully fledged stakeholders

Under option 3, it is assumed that after 2013 the Agency disposes of all required resources for the satisfactory fulfilment of its functions. The extensive consultation process with stakeholders at all levels shows a general agreement that a significant increase of resources is required. The outcome of the analysis is presented below for each of the 3 titles in the Agency's budget.

Title 1 – Costs related to staff expenditure

Compared to the other European Regulatory Agencies (see annex 6), the budget and staff available to the Agency is relatively small. Even if the different mandates and tasks of the EU Agencies make it rather difficult to make a detailed benchmarking exercise, such comparison shows that, there is a minimum required to be efficient. The required critical mass for effective action seems to be around 100 FTEs[73], with the administrative and support personnel representing about 25-30% of the total (compared to 35% today).

[73] See IDC Evaluation report of 2007 – Recommendations for the new mandate after 2009

Another interesting benchmark is to compare the resources of the Agency and their evolution over time with those of the national agencies in charge of security in the Member States. The resources of those national agencies have increased substantially over the last years. For instance in Germany, the Federal Office for Information Security (BSI)[74] had in 2007 a budget of EUR 64 million, out of which EUR 24 million for staff expenditure, EUR 33 million for non-personnel expenditures and EUR 6.8 million for investment. This represents a sharp increase since the 1997 budget of circa EUR 33.5 million. Over the same period, the staff has increased from 300 to 500 persons.[75] The recently set-up French Network and Information Security Agency [76] plans for a budget of EUR 90 million in 2012 with a staff of 250, which represent a doubling of the current staff.[77] A similar evolution can also be observed in some other Member States. Obviously, such comparison should be done with care as the competences of the different national security agencies, and of the Agency are not the same, but there is a strong trend in the Member States to take the security in information systems more seriously and devote more resources to this issue.

Interviews with stakeholders stressed the need for increase in the operational staff of the Agency. Indications were provided that the staff should approximately be doubled compared to the current situation or that the total number of FTE should be at least 120 to 140 FTEs.

Combining these indications with the information that is currently available on scope of work related to future issues the Agency would be dealing with after 2012, it seems reasonable to foresee doubling of the operational staff and small increase in the administrative staff in order to maintain an optimal proportion between administrative and operational staff.

The 5 year budgetary forecast foresees limited growth in 2012-2013 (due to the constraints of the current financial framework) and a more dynamic growth of the number of staff up to 99 FTE, reflecting the need to allow the Agency to continuously mature, by building further upon current activities and initiating new functions. This includes additional FTEs to deal with non-operational trans-pillar functions as well as budget under "Title 3 Operational activities" related e.g. to the organisation of trans-pillar trainings.

Title 2 – Costs associated to the functioning of the Agency

A detailed analysis of the costs under Title 2 in recent years reveals that approximately one third of the costs under Title 2 is fixed (e.g. costs for security equipment and security services) and two thirds of the costs vary with the number of FTEs (e.g. post and telecommunications, ICT hardware and software). Based on the evolution of the number of FTEs under Title 1, the resulting costs associated to the functioning of the Agency have been derived.

Title 3 – Costs related to operational activities

In order to evaluate what a good level of budget for operational activities could be, it is useful to compare the proportion between the costs of Title 1, 2 and 3 with other Agencies. While the differences in activities between Agencies make it very difficult to come to generally applicable ratios, it can be observed that the costs related to operational activities are rather significant and represent easily around *one third* of the total budget. An average proportion of approximately one third was also respected in the Agency budget for past periods.

---

74 Bundesamt für Sicherheit in der Informationstechnik (BSI), www.bsi.de

75 BSI Annual Report 2006-2007, Section 1.1

76 Agence nationale de la sécurité des systèmes d'information (ANSSI), http://www.ssi.gouv.fr

77 Dossier de presse relatif à la création de l'Agence nationale de la sécurité des systèmes d'information, p. 7

These global indications lead to the conclusion that operational expenditure of approximately one third of the total budget would enable the Agency to have a satisfactory level of logistic sources and outsourcing possibilities in order to further strengthen the expertise and know-how built up internally and to have the flexibility of reacting on unexpected changes in the NIS environment. For instance, it would allow sufficient budgetary room for e.g. operational costs related to specific more important roles for the Agency such as e.g. exercises.

The combination of all assumptions and estimates presented above, leads to the following 5 year budget for the Agency:

Overview of budget under OPTION 3										
	Budget 2012	**%**	**Budget 2013**	**%**	**Budget 2014**	**%**	**Budget 2015**	**%**	**Budget 2016**	**%**
Administrative staff	21		21		23		23		23	
Operational staff	40		40		49		60		76	
TOTAL	**61**		**61**		**72**		**83**		**99**	
Breakdown of total budget										
EU Budget	***9.262.000***		***9.449.000***		***12.409.087***		***14.948.281***		***18.824.525***	
Third country contributions (EFTA)	*222.288*		*226.776*		*297.818*		*358.759*		*451.789*	
Total budget for the Agency	**9.484.288**	**100%**	**9.675.776**	**100%**	**12.706.906**	**100%**	**15.307.040**	**100%**	**19.276.313**	**100%**
Breakdown of total expenditure										
Title 1 - Staff expenditure (including recruitment expenditure)	6.031.824	64%	6.239.860	64%	7.866.298	62%	9.528.461	62%	12.073.953	63%
Title 2 - Costs associated to the functioning of the Agency	559.017	6%	570.256	6%	647.328	5%	727.256	5%	841.176	4%
Title 3 - Costs related to operational activities	2.893.447	31%	2.865.660	30%	4.193.279	33%	5.051.323	33%	6.361.183	33%
Total expenditure	**9.484.288**	**100%**	**9.675.776**	**100%**	**12.706.906**	**100%**	**15.307.040**	**100%**	**19.276.313**	**100%**

Evaluation of the effectiveness of the budget

The increase of the total budget of the Agency from approximately 8 million per year in the period 2009–2012 to a total of approximately EUR 19 million (including EFTA contributions) in 2016 would have a very positive impact on the effectiveness of the Agency as it would allow the Agency to fully take up the new functions is has currently been attributed in recent policy documents or that are indicated in the new strategic plan 2010-2012 and dispose of sufficient budget for operational expenditure.

6.2.4. Option 4: Adding operational functions in fighting cyber attacks and response to cyber incidents

Title 1 – Costs related to staff expenditure

Under option 4, the adding of operational functions would require further increase of staff in addition to the 99 FTEs considered under option 3.

For the operational role for the Agency related to acting as the CERT for EU bodies and institutions, an additional number of 40 operational staff was estimated. This corresponds to 3 to 4 shifts of a team of up to 10 to 12 people in order to ensure 24/7 service availability. Furthermore, in order to obtain a sufficient critical mass of technical experts for other operational tasks such as the ones related to CIIP or specific projects such as the linking of eID databases in order to facilitate interoperability, another 33 operational staff is foreseen. Finally, to respect the overall proportion between administrative and operational staff, the

estimated increase of 75 operational staff is further completed with 21 extra administrative staff members. This brings the total number of staff members for the Agency in 2016 to **195**.

The increase in staff during the period 2012-2013 will be limited to the numbers foreseen under option 3. Half of the 75 additional staff needed for the operational activities, as well as a proportionate number of administrative staff, would have to be recruited in 2014. For the subsequent years, it is assumed that the staff would increase gradually until the estimated maximum number of 195 FTE is reached.

Title 2 – Costs associated to the functioning of the Agency

As under option 3, it is assumed that the variable costs in the current budget for the Agency will depend on the number of staff[78]. In addition to the extrapolation of the current infrastructure costs of the Agency, costs related to specific equipment required for the operational tasks will also need to be added. The precise equipment that is required would strongly depend on the exact operational tasks of the Agency. Also, the costs depend on whether the equipment is to be bought (e.g. workstations for the day-to-day monitoring EU CERT tasks) or rented (e.g. the usage of a simulation suite for exercises could be bought as a service). For 2012 and 2013, the annual equipment cost is foreseen to be 0.5 million EUR. Since the operational activities would develop more rapidly in the subsequent years, it is assumed that the specific equipment cost for operational activities would further increase to 2,5 million EUR in 2016.[79]

Title 3 – Costs related to operational activities

Referring to the overall assumption that approximately one third of the total budget relates to the costs of "Title 3 – Operational activities," the Agency would dispose of an operational budget limited to approximately EUR 2.6 million in 2012, which would reach EUR 13 million in 2016.

[78] Please note that operational staff in this context relates to all staff that is not administrative. They can thus perform operational as well as non-operations functions

[79] In Germany, the Bundesamt für Sicherheit in der Informationstechnik (BSI) invested EUR 5 million in 2006 and EUR 6,9 million in 2007. The number of employees in 2006 was 480 in 2006 and 500 in 2007

Overview of budget under OPTION 4										
	Budget 2012	**%**	**Budget 2013**	**%**	**Budget 2014**	**%**	**Budget 2015**	**%**	**Budget 2016**	**%**
Administrative staff	21		21		33		39		44	
Operational staff	40		40		86		116		151	
TOTAL	**61**		**61**		**119**		**155**		**195**	
Breakdown of total budget										
EU Budget	***9.262.000***		***9.449.000***		***24.085.495***		***31.159.272***		***40.699.021***	
Third country contributions (EFTA)	*222.288*		*226.776*		*578.052*		*747.823*		*976.777*	
Total budget for the Agency	**9.484.288**	**100%**	**9.675.776**	**100%**	**24.663.547**	**100%**	**31.907.094**	**100%**	**41.675.798**	**100%**
Breakdown of total expenditure										
Title 1 - Staff expenditure (including recruitment expenditure)	6.031.824	64%	6.220.376	64%	13.844.519	56%	18.214.025	57%	23.985.356	58%
Title 2 - Costs associated to the functioning of the Agency	1.059.074	11%	1.070.256	11%	2.680.057	11%	3.163.728	10%	3.937.429	9%
Title 3 - Costs related to operational activities	2.393.390	25%	2.385.144	25%	8.138.971	33%	10.529.341	33%	13.753.013	33%
Total expenditure	**9.484.288**	**100%**	**9.675.776**	**100%**	**24.663.547**	**100%**	**31.907.094**	**100%**	**41.675.798**	**100%**

Evaluation of the effectiveness of the budget

The strong increase of the Agency's budget and human resources as of 2014 raises concerns about the absorption capacity of the Agency. In a very short period of time, the Agency would have to recruit a large number of new staff, revise its organisation structure and processes, and ensure the implementation of a work program which is much more ambitious than its current one.

The effectiveness of allocating the additional budget required for performing extra tasks will largely depend on the ability of the Agency to successfully take up its operational tasks. In order to do so, the Agency will need to succeed in convincing stakeholders of its added value and thus become an organisation that stakeholders spontaneously turn to for operational support. This will require the Agency to attract a number of highly experienced and renowned operational experts that would be able to build up an operational competence centre with high visibility in a very short time period. If this would not be possible, stakeholders would most probably continue to develop own operational capacity rather than relying on the Agency to ensure sufficient service delivery.

6.2.5. Option 5: Adding operational functions in supporting law enforcement and judicial authorities in fighting cyber crime

Under Option 5, an additional team is added, responsible for operational activities in supporting law enforcement and judicial authorities at the European and Member State level. It is assumed that 10 extra operational staff would be required, implying 3 additional administrative staff in order to keep the optimal proportion in operational and administrative staff members. As for the operational staff under Option 5, half of the staff would be recruited immediately. After 2012, an annual increase of approximately 25% per year is assumed until the targeted number of staff is reached.

For 2012 and 2013, the annual equipment cost is foreseen to be 0.5 million EUR. Since the operational activities would develop more rapidly in the subsequent years, it is assumed that

the specific equipment cost for operational activities would further increase to 2,5 million EUR in 2016.[80]

Regarding Title 2 costs, an extra annual cost of EUR 100.000 is added as of 2014 on top of the costs for specific equipment or software requirements estimated under option 4. The total amount for option 6 will therefore reach EUR 2.6 million at the end of the examined period. This additional cost is estimated to be rather limited as it is assumed that for many operational functions (e.g. data collection), the Agency could collaborate with ISPs.

In 2012 and 2013 the budget available under Title 3 is limited due to the budget ceiling set by the current financial framework. As of 2014, the proportion of one third of operational expenditure compared to the total budget is to be respected.

Overview of budget under OPTION 5										
	Budget 2012	**%**	**Budget 2013**	**%**	**Budget 2014**	**%**	**Budget 2015**	**%**	**Budget 2016**	**%**
Administrative staff	21		21		35		41		47	
Operational staff	40		40		91		124		161	
TOTAL	**61**		**61**		**126**		**165**		**208**	
Breakdown of total budget										
EU Budget	***9.262.000***		***9.449.000***		***25.490.605***		***33.228.806***		***43.316.593***	
Third country contributions (EFTA)	*222.288*		*226.776*		*611.775*		*797.491*		*1.039.598*	
Total budget for the Agency	**9.484.288**	**100%**	**9.675.776**	**100%**	**26.102.379**	**100%**	**34.026.297**	**100%**	**44.356.191**	**100%**
Breakdown of total expenditure										
Title 1 - Staff expenditure (including recruitment expenditure)	6.031.824	64%	6.220.376	64%	14.669.733	56%	19.470.563	57%	25.600.477	58%
Title 2 - Costs associated to the functioning of the Agency	1.059.074	11%	1.070.256	11%	2.818.861	11%	3.327.056	10%	4.118.171	9%
Title 3 - Costs related to operational activities	2.393.390	25%	2.385.144	25%	8.613.785	33%	11.228.678	33%	14.637.543	33%
Total expenditure	**9.484.288**	**100%**	**9.675.776**	**100%**	**26.102.379**	**100%**	**34.026.297**	**100%**	**44.356.191**	**100%**

Evaluation of the effectiveness of the budget

Option 5 raises similar absorption capacity concerns as the ones expressed under option 4. In addition, as the increase in staff in the first two years of the examined period will be limited, the Agency would be able to take up tasks related to supporting law enforcement and judicial authorities only from 2014 onwards. Therefore, the positive impacts of this option which have been identified earlier will be delayed in time, thereby reducing its overall effectiveness.

7. COMPARING THE OPTIONS

The estimated budget impact of each of the policy options can be compared both on an annual and on a 5 year basis. The figures presented below do not take into account the contribution of EFTA countries to the Agency budget as the aim is to examine the net impact on the EU budget of each policy option. Regarding the budget for option 1, reference is made to the remarks raised during the evaluation of the effectiveness of this budget.

(EU budget)	**Evolution of costs per annum (beginning vs end of the examined 5-year period)**	**Average annual costs**	**Total costs for the 5-year period**

[80] In Germany, the Bundesamt für Sicherheit in der Informationstechnik (BSI) invested EUR 5 million in 2006 and EUR 6,9 million in 2007. The number of employees in 2006 was 480 in 2006 and 500 in 2007

	2012	2016		
Option 1 – No policy	0 €	0 €	0 €	0 €
Option 2 – Continuation à l'identique	8.420.000 €	9.109.077 €	8.760.981 €	43.804.906 €
Option 3 – Expansion of the functions for the Agency and adding law enforcement and privacy protection agencies as fully fledged stakeholders	9.262.000 €	18.824.525 €	12.978.579 €	64.892.893 €
Option 4 – Adding operational functions in fighting cyber attacks and response to cyber incidents	9.262.000 €	40.699.021 €	22.930.958 €	114.654.789 €
Option 5 – Adding operational functions in supporting law enforcement and judicial authorities in fighting cyber crime	9.262.000 €	43.316.593 €	24.149.401 €	120.747.003 €

The previous chapters presented a detailed assessment of the five shortlisted policy options. This consisted of (1) a qualitative assessment and (2) the assessment of the impact of the options on the EU budget. Furthermore, a cost/benefit analysis has been made of three case studies related to specific functions that are part of the policy options (annex 7).

The qualitative analysis showed that option 1 "no policy" would produce a number of negative consequences with adverse impacts across all dimensions. While it would not have an impact on the EU budget it would create extra costs for Member States as described above.

Option 2 would be sub-optimal as ENISA would not have the necessary resources to address adequately the challenges of the constantly evolving NIS landscape. The current situation would actually be aggravated as the Agency would not be able to keep up with the rising expectations of stakeholders as regards its activities.

Options 4 and 5 would achieve the largest qualitative impacts; however, the additional costs for their implementation are disproportionately high compared to the additional benefit they bring. In addition, there are a number of concerns expressed by stakeholders regarding the actual feasibility of these options as noted in 5.2.

Option 3 provides the best balance. It achieves the core aim of having a modernised Agency which, together with other NIS instruments, can contribute to achieve the goals of a reinforced NIS strategy in Europe. It addresses adequately all of the identified problem drivers within a reasonable increase of the resources. Moreover, all the activities foreseen under this option have received the support of NIS stakeholders during the consultation process. Option 3 is therefore the preferred policy option.

Remark on the duration of ENISA's mandate

Article 27 of Regulation 460/2004 indicated that ENISA would be established for a period of five years. Regulation 1007/2008 further extended this period to a total of eight years. When comparing with other Agencies, it can be concluded that it is rather exceptional to have a situation in which an Agency has a mandate that is limited in time. The limited duration of the mandate of ENISA is generally considered to be an important constraint for developing a long term vision and for attracting the relevant and qualified profiles for performing the highly specialized long-term nature tasks and a major reason for personnel turnover. Therefore, prolonging the mandate for an indefinite period, with regular review mechanisms, needs to be considered.

8. MONITORING AND EVALUATION

8.1. Core indicators of progress towards meeting the objectives

The following core indicators have been identified:

Objective	Indicators
Coherence of regulatory approaches	• Number of Member States having made use of the Agency recommendations in their policy making process • Number of studies aimed at identifying gaps and inconsistencies in the standardisation landscape in relation to NIS • Reduced divergence of Member States' approaches to NIS
Prevention, detection and response	• Number of network security trainings organised • Availability of a functioning early warning system for emerging risks and attacks • Number of NIS exercises at EU level coordinated by the Agency
Knowledge enhancement for policy makers	• Number of studies to collect information on current and anticipated NIS risks and risk prevention technologies • Number of consultations with public bodies dealing with NIS • Availability of a European framework for organising data collection on NIS
Empowering stakeholders	• Number of identified good practices for industry • Level of investment in security measures by private stakeholders
Sheltering Europe from international threats	• Number of conferences/meetings between EU Member States to define commonly agreed goals for NIS • Number of meetings between European and international NIS experts
Towards collaborative implementation	• Number of regulatory compliance assessments • Number of EU-wide NIS practices
Fighting cyber crime	• Regularity of interactions with former 2nd and 3rd pillar agencies • Number of instances in which expertise was provided in criminal investigations

8.2. Broad outline for possible monitoring and evaluation arrangements

The Commission should undertake periodic evaluations, taking into account the views of all relevant stakeholders and on the basis of terms of reference agreed with the Management Board of the Agency. The evaluations should assess the effectiveness of the Agency in achieving its objectives, whether an Agency is still an effective instrument and whether any changes should be made to the Agency's mandate and/or other aspects of its establishing Regulation. The evaluation findings should be forwarded by the Commission to the European Parliament and the Council and be made public. Following an evaluation, the Management Board should issue recommendations regarding eventual appropriate changes to the establishing Regulation to the Commission. The Management Board and the Executive Director of the Agency should take the results of the evaluations into consideration in the Agency's multi-annual planning.

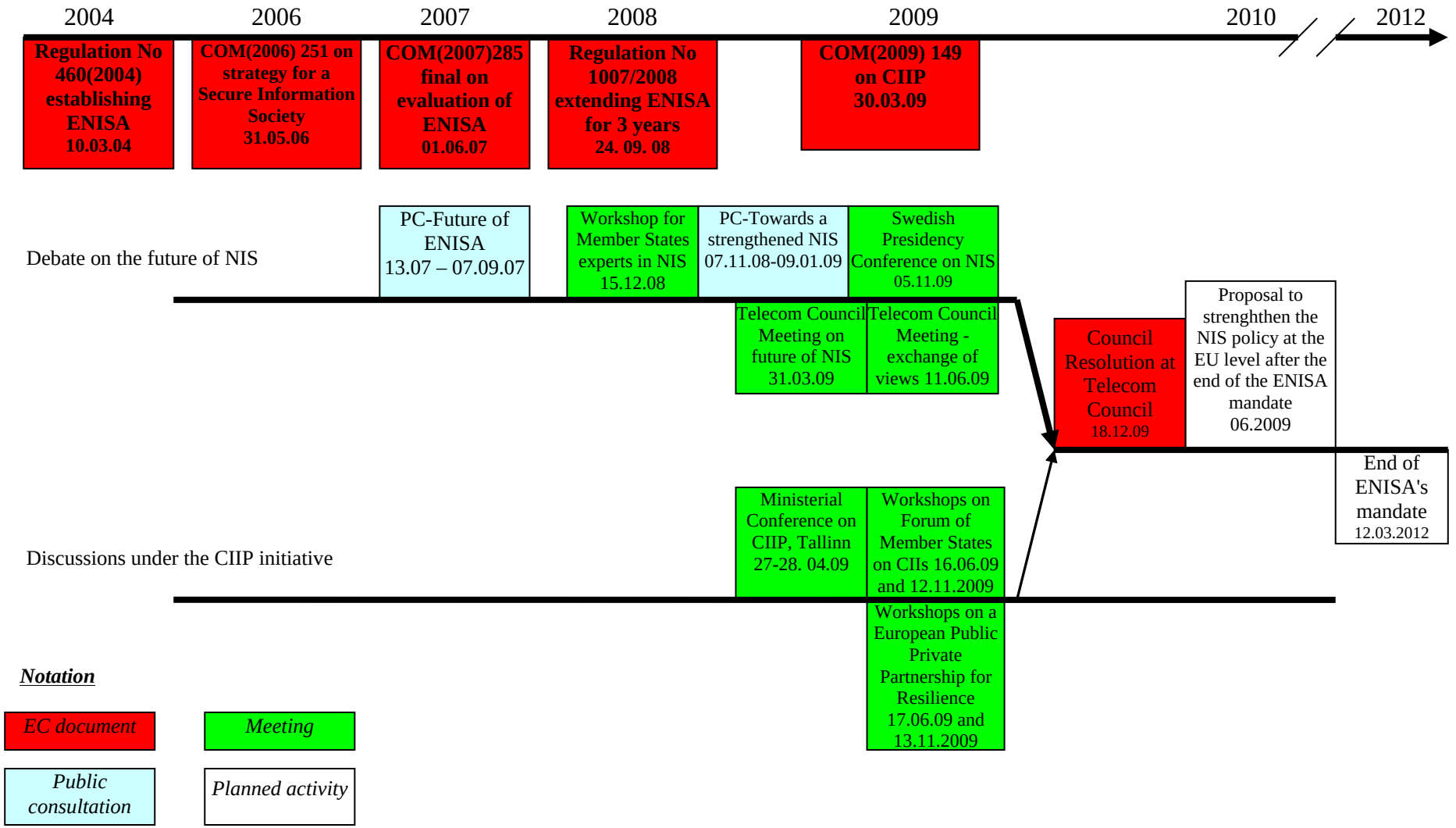
The operations of the Agency are subject to the supervision of the Ombudsman in accordance with the provisions of Article 228 of the Treaty.

TABLE OF ANNEXES

ANNEX 1: ORGANISATION AND TIMING

Period/Activity	Jun 2007	Sep 2007	Nov 2008	Dec 2008	Jan 2009	Mar 2009	Apr 2009	Jun 2009	July 2009	Aug 2009	Sep 2009	Oct 2009	Nov 2009	Dec 2009	Jan 2010	Feb 2010	Mar 2010	Apr 2010	May 2010	Jun 2010
CONSULTATION PROCESS:																				
Public Consultation on the future of ENISA	13th	7th																		
Public Consultation "Towards a strengthened NIS Policy in Europe"			7th		9th															
Workshop on NIS for experts from Member States				15th																
Ministerial Conference on CIIP in Tallinn							27th-28th													
Telecom Council meeting, Exchange of views on NIS						31st														
Workshop on the Forum of Member States on security and resilience of CIIs								16th												
Workshop on the EP3R								17th												
Second workshop on the Forum of Member States on security and resilience of CIIs													12th							
Second Workshop on the EP3R													13th							
Council Resolution on a collaborative European approach to Network and Information Security														18th						
INTER-SERVICE STEERING GROUP:											10th	8th 29th								
IA STUDY (The process of preparing the IA was assisted by an external contractor – Van Dijk Management Consultants):																				
1st (kick-off) meeting with the contractor									16th											
Report on the proposed policy options and an initial assessment										26th										
Draft final report											29th									
Final Report submitted by the contractor												16th								
Draft IA report sent to IAB																24th				
IAB opinion																	26th			
Resubmission of the IA report sent to IAB																		15th		
Final IAB opinion																		27th		
Inter-service consultation with IA report, executive summary and citizen's summary																		tbc		
Submission of the draft proposal + IA summary to DGT																				
Adoption by the Commission																				

ANNEX 2: TIMELINE OF COMMISSION ACTIVITIES RELATED TO ENISA



ANNEX 3: OVERVIEW OF A BROAD RANGE OF POSSIBLE CONCEPTS FOR A EUROPEAN NIS ORGANISATION

The main concepts and resulting packages of functions presented below can be considered as possible avenues for the future. Their identification is based on an internal brainstorming session on a broad range of roles ENISA could play, without taking into account at this stage the priorities identified previously and the effectiveness of these concepts for attaining these priorities. Please note that whenever reference is made to 'ENISA', this should be taken to mean any organisation that will act as a successor to the current ENISA (i.e. not necessarily in the form of an Agency).

1. No policy and ENISA à l'identique

In this policy option, the **concept** covers the two basic scenarios to be considered in any policy assessment, namely the hypothesis of no ENISA existing, and the hypothesis of continuing *à l'identique*, i.e. using the same structure, tasks and goals.

The corresponding **packages of functions** are then of course trivial to define, comprising respectively nothing (no ENISA) and the current tasks as enumerated in the Regulation (*à l'identique*).

2. ENISA as a liaison network

In this policy option, the **concept** is a flexible and light organisation which is used mainly to facilitate the establishment of contacts between NIS stakeholders, most notably public administrations, NIS industry, academia and end user organisations. The main **goal** of ENISA would be to collect contact information on these stakeholders and stimulate an exchange of know-how between them. In a modern day context, one could characterise this as ENISA acting as a NIS social network.

The corresponding **package of functions** focuses exclusively on objective 4: empowering stakeholders. However, it takes a passive approach to this objective, as the main focus is on facilitating contacts and information exchange, and not on seeking out and actively disseminating this information.

3. ENISA as a knowledge collection and dissemination network

In this policy option, the **concept** extends the aforementioned liaison network option by adding an active component: in addition to facilitating contacts between NIS stakeholders, ENISA would itself actively seek out information and disseminate it to the relevant stakeholders. In addition to the NIS social network component, ENISA would thus also retain its role as an expertise centre for these stakeholders, albeit without any public policy involvement (i.e. it would identify existing practices, but without extensive analysis or recommendations to policy bodies).

The corresponding **package of functions** still focuses exclusively on objective 4, but takes a more holistic approach: in addition to merely facilitating contacts, ENISA would seek out and disseminate NIS information.

4. ENISA as a NIS policy support centre

In this policy option, the **concept** focuses on ENISA providing clear and specific NIS information to support any policy initiatives with a NIS impact. In this concept, ENISA would act as an expertise centre that could provide knowledge or recommendations to policy makers involved in any initiatives with a NIS impact (comparable to the supporting role that the EDPS plays towards European bodies in the field of data protection). Liaising with existing European bodies that touch upon NIS issues (such as the EDPS, BEREC, Europol etc) would

of course be crucial in this respect. This is the concept that is thus most closely related to the basic model proposed by the updated Telecoms regulatory package (which foresee such a policy support role for ENISA vis-à-vis the BEREC already), and also covers some of the suggestions noted in the Communication on CIIP (although this communication admittedly also hints at the need for a stronger operational role, which will be further examined below).

The corresponding **package of functions** focuses strongly on objective 3 (Knowledge enhancement objective for policy makers), and specifically on the clusters of functions regarding knowledge collection (including through stakeholder consultations) and providing policy recommendations. The cluster of functions focusing on research efforts would not be extensively covered by this policy option.

5. ENISA as a NIS research coordination centre

In this policy option, the **concept** focuses on ENISA establishing an overview of research initiatives with a potential European NIS impact, identifying gaps in these research efforts, and in ensuring that research priorities are followed up on (either by making recommendations on research needs, or by directly being able to organise research efforts, including e.g. by leveraging a PPP-model).

The corresponding **package of functions** focuses on the research functions of objective 3 (Knowledge enhancement objective for policy makers). Objective 4 (Empowering stakeholders) would also be implicated, due to the need to get appropriate feedback from the stakeholders on research needs.

6. ENISA as a EU NIS CERT

In this policy option, the **concept** focuses on the need for coordination between national CERTs, and the need for an internal EU CERT. ENISA would play both roles, acting as an internal NIS policy and incident response body towards European institutions (which presently have no such body to assess, monitor and correct their own NIS policies), and as a coordinator between national CERTs, ensuring that they have a common network for internal communication and knowledge exchange.

The corresponding **package of functions** combines a small operational component (objective 6) that focuses on assisting European bodies with a networking component (objective 4) that focuses on interconnecting existing CERTs.

7. ENISA as a European NIS storm centre

In this policy option, the **concept** builds on the EU NIS CERT scenario above, but adds two new components: the pro-active identification of NIS risks (including through operational exercises at the European level) and the coordination of incident response efforts when an incident has a potential cross border scope. It thus aims to leverage the experience of national bodies optimally by requiring them to interact, which will help in the identification of any strengths and weaknesses, in particular to address CII vulnerabilities. This also covers the operational aspect which was suggested in the Commission Communication on CIIP, which was based on five pillars, the 2nd and 3rd of which focused on operational impact:

(1) Preparedness and prevention: to ensure preparedness at all levels;

(2) Detection and response: to provide adequate early warning mechanisms;

(3) Mitigation and recovery: to reinforce EU defence mechanisms for CII;

(4) International cooperation: to promote EU priorities internationally;

(5) Criteria for the ICT sector: to support the implementation of the Directive on the Identification and Designation of European Critical Infrastructures

The corresponding **package of functions** combines a larger operational component (objectives 1 and 2) that focuses on assisting European bodies and on incident response coordination with a networking component (objective 4) that focuses on interconnecting existing CERTs.

8. ENISA as a European NIS representative

In this policy option, the **concept** is based on the need for global NIS coordination to achieve an optimal NIS impact. In this case, ENISA would function as a contact point to non-European governmental NIS bodies, communicating European NIS policies and good practices, and identifying action points to ensure global effectiveness. This covers the fourth pillar that was suggested in the Commission Communication on CIIP: "*International cooperation: to promote EU priorities internationally*".

The corresponding **package of functions** focuses on objective 5 (sheltering Europe from international threats), with a smaller policy oriented component (objective 3) since ENISA would also need to collect and disseminate NIS policy information to foreign bodies and inversely aggregate feedback from those foreign bodies to the relevant European instances.

9. ENISA as a NIS normative support centre

In this policy option, the **concept** is aimed at ensuring that the normative (regulatory and non-regulatory) framework in relation to NIS issues is known, complete and coherent (including its implementation). ENISA's function would be to chart applicable norms (Directives, Decisions, standards, codes of conduct, industry good practice guidelines etc), disseminate them, analyse them to identify gaps and take the necessary steps to ensure that these gaps are addressed by the competent bodies (regulatory bodies, standardisation bodies, industry groups, etc). Supporting the implementation of the Directive on the Identification and Designation of European Critical Infrastructures[81] would obviously be one of the key domains to be covered in this concept.

The corresponding **package of functions** focuses on objective 1 (Coherence of regulatory approaches objective), with a smaller policy oriented component (objective 3) since ENISA would also need to collect and analyse NIS normative information.

10. ENISA as a NIS compliance expertise centre

In this policy option, the **concept** focuses on the effectiveness of NIS norms and policies, requiring ENISA to build an expertise network that can assess the effectiveness of NIS practices within an organisation (including specifically organisations managing CII), and provide accreditations and/or recommendations for improvement. This would require either the development of internal assessment expertise, or the creation of a network of assessment bodies (including e.g. in the academic/consulting/accreditation industries) that could perform these services. In this way, assessment processes could be used to increase the dependability and trustworthiness of European network and information infrastructure.

The corresponding **package of functions** focuses strongly on the compliance assessment cluster of functions within the regulatory compliance objective (objective 6), with a smaller

[81] Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection

component related to empowering stakeholders (objective 4) due to the need to liaise with existing assessment bodies.

11. ENISA as a Trans-pillar NIS policy expertise centre

In this policy option, the **concept** is built on the likelihood of the entry into force of the Lisbon Treaty, which will abolish the current pillar structure of the European Union. In a post-pillar policy environment, an ENISA concept focusing on first pillar issues may not be the most effective. This concept would therefore extend ENISA's range of NIS activities to a trans-pillar (post-pillar) scale. ENISA's main role would be to provide clear and specific NIS information to support any policy initiatives with a NIS impact, irrespective of the pillar in which this initiative would have fallen, and in liaising with existing European bodies that touch upon NIS issues (including also current 2nd and 3rd pillar bodies, such as the European Defence Agency, Europol, Eurojust, etc).

The corresponding **package of functions** prioritises objective 7 (Fighting cyber crime), thus extending the scope of objective 3 (knowledge enhancement objectives for policy makers), and specifically on the clusters of functions regarding knowledge collection (including through stakeholder consultations) and providing policy recommendations. The functions focusing on research efforts would not be extensively covered by this policy option.

ANNEX 4: OVERVIEW OF POSSIBLE FORMATS FOR IMPLEMENTING THE SHORTLISTED POSSIBLE CONCEPTS FOR A EUROPEAN NIS ORGANISATION

This section describes and evaluates a number of possible organisational formats for the implementation of the shortlisted policy options.

1. FORMAT 1: AGENCY

	AGENCY
Description	There are two types of agencies: so-called *regulatory agencies*, whose tasks are established in a specific legal framework established on a case-by-case basis, and *executive agencies* which have the much more narrowly defined task of helping to manage Community programmes[82]. While executive agencies are established in Brussels or Luxembourg, regulatory agencies – like ENISA – can be established anywhere in the Union, which is an additional potential benefit of the agency structure, due to the possibility of connecting with local communities and leveraging any local expertise.
Legal basis	The Regulation establishing ENISA is based on Article 95 of the Treaty establishing the European Community. This implies that the activities of ENISA are contributing to regulatory measures[83] of which the objectives are the establishment and the functioning of the Internal Market. This legal basis has been confirmed by the European Court of Justice, following an action brought by the UK[84].
Advantages	The main benefit of an Agency is the possibility of creating a *legal entity* that stands separate from the European Commission with a mandate supported by the European Parliament. This allows certain policy tasks to be delegated to an external expert body, which is granted a certain degree of manoeuvring space to develop its own agenda and working methods (within the remit of its mandate, of course) based upon its intimate knowledge of the domain in which it operates. In addition, the Agency structure offers the possibility of establishing its own unique identity and reputation towards the stakeholders being targeted, thus more easily attracting the required expertise. The main benefit of the agency *structure* lies in the inherent flexibility in determining the scope of its tasks and its organisational model, which is particularly beneficial in domains where cooperation with Member States or expert stakeholders is crucial. Member States can retain close control of an Agency, which can be an advantage when the Agency is intended to address sensitive policies that Member States are unwilling to delegate

[82] See also COM (2008) 135 – Communication of the Commission to the European Parliament and the Council entitled '*European Agencies – the way forward*".

[83] "Measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States."

[84] See ECJ Judgment of 2 May 2006 in Case C-217/04.

	AGENCY
	immediately to the European level. This makes agencies very suitable in areas where specific expertise is required, e.g. to provide regulatory or policy recommendations, especially when Member States wish to retain a substantial degree of national control. In addition, it is possible to grant agencies with directly binding decision making powers in relation to technical areas where there is little to no possibility to exercise discretion. These may obviously only pertain to specific cases, i.e. they cannot be given regulatory powers.
Disadvantages	Delocalisation outside of Brussels/Luxembourg runs the risk of an Agency becoming established in a region which has a limited access to the resources (technical/operational/human) that are needed to develop the services of the Agency, which appears to be the case for ENISA as it stands. In addition, the possibility of Member States retaining a substantial degree of national control in the policy area being covered also includes the risk of insufficient harmonisation, which can negatively impact the way NIS risks are managed. Finally, the powers that may be given by a Regulation or a Directive to a regulatory agency are limited as they may not impinge to the institutional balance of powers between EU Institutions that is set up by the founding treaties.[85] In particular, the Agency may not be given the powers that the Treaties reserve to the Commission. Thus, it is possible to grant agencies with directly binding decision making powers in relation to technical areas where there is little to no possibility to exercise discretion. These may obviously only pertain to specific cases, i.e. they cannot be given regulatory powers.
Examples in other domains	Similar agencies include Eurojust and Europol in the Netherlands, and the European Institute for Security Studies in Paris[86].

2. FORMAT 2: A MORE OR LESS FORMALISED PUBLIC PRIVATE PARTNERSHIP (PPP)[87]

	PUBLIC PRIVATE PARTNERSHIP
Description	Public Private Partnership (PPP) is an umbrella term for the organised collaboration between the public and private sector for their mutual benefit. The EU relies on PPPs in several domains, most recently especially to support research and development activities. In this case, the role of the Union focuses on supporting the efforts of private actors, e.g. via funding or a common administrative support framework, but where key strategic decisions on direction are taken by the private stakeholders. Thus, costs are typically partially borne by the public sector, with

[85] See Case 9/56 Meroni v High Authority.
[86] See also http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/08/159
[87] Draft Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Mobilising private and public investment for recovery: developing Public Private Partnerships

	PUBLIC PRIVATE PARTNERSHIP
	expertise being delivered by public and private stakeholders in a format that ensures that research efforts are sufficiently market-oriented.
Legal basis	PPPs can be established in a variety of ways. Generally speaking, the legal basis for EU supported PPPs is Article 171 of the EC Treaty. This allows the Community to set up Joint Undertakings for the "efficient execution of Community research, technological development and demonstration programmes". Article 172 of the Treaty specifies that Joint Undertakings can be decided by the Council after consulting the European Parliament and the Economic and Social Committee.Joint Technology Initiatives (JTIs – see below) are one example of Joint Undertakings, which are funded under the Seventh Framework Programme, and can be established via a Council Regulation following a proposal from the Commission.Other Joint Undertakings (like e.g. ITER, The European Joint Undertaking for ITER and the Development of Fusion Energy or 'Fusion for Energy', or SESAR, SESAR (the Single European Sky ATM Research Programme)) were similarly established through a Commission Decision or a Council Regulation on the basis of article 171 of the EC Treaty.
Advantages	PPPs ensure that public policy concerns are translated into innovative research efforts, supported in part by public funding. The shared funding model can be crucial to ensure the stability of research work, especially in a period of economic downturn where innovation is both necessary and difficult to fund privately. The model allows the intervention of private experts in determining research priorities and appropriate implementation paths, "going from basic and applied research through to validation and large-scale demonstration, with an increased emphasis on impact and exploitation"[88]. This ensures that the research is not purely academic in nature and has a practical impact in real economic terms. PPPs can be established as independent legal entities, which can be given relative autonomy to determine their own agenda. Finally, the organisation of PPPs with a broad mandate via a single procurement process ensures that administrative overhead (both in terms of time and financial resources) is kept to a minimum.
Disadvantages	One of the main difficulties of setting up a PPP is that it requires sufficient incentive for the private sector to join. If the benefits for the private sector are too distant or imprecise, it may not join the PPP, although a public intervention may be justified. Disadvantages of PPP models are also related to the complexity of ensuring the relevance of the research and the possibility for the partners in the PPP to share and re-use the results in a fair way. The former question (relevance of the research) is mainly linked to the concern that the PPP should ultimately also serve public policy

[88] See also http://ec.europa.eu/research/industrial_technologies/lists/list_114_en.html

	PUBLIC PRIVATE PARTNERSHIP
	goals, in consideration of the public funding invested in the PPP. This means that PPPs cannot be used to disproportionately serve the commercial interests of one or more private partners in the PPP, at the exclusion of other private partners or the public interest. In short, research in the PPP must be well defined to avoid unduly favouring private interests. Similarly, the terms of use of the research outcome must be well defined, including specifically in terms of intellectual property rights and protection of know-how, to ensure that the results of the PPP can be used for public benefit. This would be particularly important in the field of NIS as well, where it should be avoided that positive results which were co-funded by public means can only be exploited by a select group of parties.
Examples in other domains	Examples mentioned in the aforementioned Communication[89] include ITER (for nuclear fusion) and SESAR (for air traffic management). In addition, the Commission is currently launching three large scale PPPs as a part of its European Economic Recovery Plan, which will cover three themes: Factories of the Future (€1.2 billion for R&D), Energy-efficient Buildings (€1 billion for R&D); and Green Cars (€5 billion, of which €1 billion for R&D). These follow in the footsteps of earlier examples, including European Technology Platforms (ETPs[90]) as a framework to define research priorities, implemented in some cases through Joint Technology Initiatives (JTIs[91]) as a part of the 7th Framework Programme. EU funding has thus been set aside in various high-innovation research areas, including Fuel Cells and Hydrogen (FCH), Aeronautics and Air Transport (Clean Sky), Innovative Medicines (IMI), Nanoelectronics Technology 2020 (ENIAC), and Embedded Computing Systems (ARTEMIS).

3. FORMAT 3: AN INFORMAL CONTACT NETWORK

	INFORMAL CONTACT NETWORK
Description	Informal contact networks are established on an ad hoc basis, and are centered around the voluntary participation of stakeholders, rather than around any formal framework of cooperation. They can e.g. take the form of expert forums, in which the participants have an almost complete autonomy to establish their own agenda.
Legal basis	The key characteristic of informal networks is the lack of a formal instrument that serves as a basis for their governance. Informal networks operate as a factual reality, not as an instrument of formal policy.

[89] See also COM (2008) 135 – Communication of the Commission to the European Parliament and the Council entitled '*European Agencies – the way forward*".

[90] See http://cordis.europa.eu/technology-platforms/

[91] See http://cordis.europa.eu/fp7/jtis/

	INFORMAL CONTACT NETWORK
Advantages	The main advantage of informal networks is their flexibility in establishing their own agenda and modus operandi. This makes them well suited in contexts where the existing stakeholders have a strong will and/or incentive to create and maintain a contact network, and where they have sufficient means (in terms of funding and manpower) to organise and maintain their operations at an appropriate level.
Disadvantages	Due to their informal nature, it is difficult to exercise any policy guidance towards contact networks (e.g. to alter their mandate or areas of focus), which makes them ill suited for high priority policy areas where a stronger degree of control is needed. In addition, they are dependent on the goodwill and commitment of their members to remain operational, which may be difficult to maintain over an extended period of time. Without clear governance, contact networks can become unstable and ineffective.
Examples in other domains	An example is the European Governmental CERTS Group (EGC), which operates as an informal group of governmental CSIRTs.

4. FORMAT 4: PERMANENT NETWORK OF COMPETENT BODIES

	PERMANENT NETWORK OF COMPETENT BODIES
Description	A permanent contact network would consist of high-level representatives from national competent bodies/authorities designated by each Member State. The proper functioning of the network is usually to be ensured by a Secretariat, which may be formed ad hoc or provided by the Commission.
Legal basis	There is no common formal instrument or provision at EU level that regulates the establishment of such networks.
Advantages	By bringing together National Competent bodies, such a network could facilitate the cooperation as well as the exchange of information and best practices between Member States on specific technical matters relevant to NIS (i.e. standards, certification, contingency planning, risk assessment, exercises, etc.). Given that the national/governmental CERTs in Member States are often an operational function/unit of the National competent body in the area of NIS, a permanent network may also serve as a mechanism for operational cooperation.
Disadvantages	Whereas competent bodies exist in nearly all Member States, it should be noted that in a number of Member States there is more than one competent body. In addition, the nature of such bodies differs across Member States. Some are of regulatory nature (i.e. FICORA, PTS or ANACOM)[92], others are in the area of national

[92] National Regulatory Authorities in Finland, Sweden and Portugal

	PERMANENT NETWORK OF COMPETENT BODIES
	security (i.e. BSI[93], ANSSI[94], OCS[95] or NCC[96]), others in that of infrastructure protection (i.e. CNAIPIC[97] or CNIPIC[98]) or defence (i.e. Estonian Informatics Centre), yet others are technical/operational bodies (i.e. Governmental/National CERTs). Cooperation across Member States may have to rely on various configurations of such networks. This might become a major problem for the sustainability of the network. In addition, a permanent network in the area of NIS will have a complex legal framework insofar as it will have to take into account the national legal frameworks applicable to the participating bodies. To operate efficiently such network would need certain flexibility which, however, may be impeded by the complexity of the legal framework. Also, there would be no direct involvement of the various stakeholders. Their involvement would be left to the individual Member States and there are likely to be widely different views among the Member States regarding their participation. Within such a network, it would be difficult to grasp the European dimension of the NIS issues at stake, as it would always be filtered though the national perspectives. Last but not list, there is a risk that a network of this kind would be reduced to a "talking shop", i.e. without leading to any significant results.
Examples in other domains	Examples of networks of competent bodies in other domains are: the Body of European Regulators for Electronic Communications (BEREC) which brings together the National Regulatory Authorities in the Member States; the Network of Competent Authorities in regard to the health information and knowledge strand of the EU Public Health Programme 2003-2008; the Permanent Network of National Correspondents in the area of civil protection; the European Crime Prevention Network.

5. FORMAT 5: DIRECT INTEGRATION INTO COMMISSION SERVICES

	DIRECT INTEGRATION INTO COMMISSION SERVICES
Description	A fifth and final possible format would be to assign ENISA's tasks directly to the Commission, for instance as a part of an existing Directorate-General, or a separate body (like an observatory or a task-force) within a DG, such as e.g. DG DIGIT.
Legal basis	Assignment of ENISA's tasks to a DG principally requires a political consensus to substantially change the responsibilities of that DG while fully remaining within the scope of the responsibilities assigned to the Commission in the EC Treaty.

[93] Federal Office for Information Security in Germany
[94] "Agence Nationale de la Sécurité des Systèmes d'Information" in France
[95] Office of Cyber Security in the UK
[96] National Cyber Security Centre in Hungary
[97] Centro Nazionale Anticrimine Informatico per la protezione delle infrastrutture critiche in Italy
[98] Centre for the Protection of National Critical Infrastructures in Spain

	DIRECT INTEGRATION INTO COMMISSION SERVICES
Advantages	Integration of ENISA's tasks into the Commission's services would offer the significant benefit of offering direct control over ENISA's activities, enabling greater harmonisation and potential effectiveness. In addition, this integration could be organised in the form of specific programmes (like the IDABC programme) or even an initiative within such a programme (like the Open Source Observatory within the IDABC Programme), which would allow increasing degrees of stakeholder involvement.
Disadvantages	The reorganisation of ENISA's tasks in this manner is likely to be politically highly complex, especially given the existing definition of the various DGs' tasks, which do not mesh well with some of the ENISA concepts defined above. E.g. if ENISA is redefined as a strictly internal Commission NIS expertise / implementation / assessment centre without external ambitions (e.g. in relation to Member States or private NIS industry stakeholders), then this may fit in the remit of DG Informatics. A broader task package however would no longer fit this type of organisation. It may be very difficult to organise ENISA within the competence of a specific DG.
Examples in other domains	Apart from the existing DGs[99], an example of an existing observatory with an information society focus is the OSOR, the Open Source Observatory and Repository for European public administrations (see www.osor.eu), financed by the IDABC programme of the European Commission – DG Informatics.

[99] See http://ec.europa.eu/dgs_en.htm

ANNEX 5: ESTIMATION OF BUDGET REQUIREMENTS FOR THE POLICY OPTIONS

Overview of budget under OPTION 2										
	Budget 2012	**%**	**Budget 2013**	**%**	**Budget 2014**	**%**	**Budget 2015**	**%**	**Budget 2016**	**%**
Administrative staff	20		20		20		20		20	
Operational staff	37		37		37		37		37	
TOTAL	**57**		**57**		**57**		**57**		**57**	
Breakdown of total budget										
EU Budget	***8.420.000***		***8.590.000***		***8.755.361***		***8.930.468***		***9.109.077***	
Third country contributions (EFTA)	*202.080*		*206.160*		*210.129*		*214.331*		*218.618*	
Total budget for ENISA	**8.622.080**	**100%**	**8.796.160**	**100%**	**8.965.489**	**100%**	**9.144.799**	**100%**	**9.327.695**	**100%**
Breakdown of total expenditure										
Title 1 - Staff expenditure	***5.497.417***	***64%***	***5.717.314***	***65%***	***5.946.007***	***66%***	***6.183.847***	***68%***	***6.431.201***	***69%***
Chapter 11 - Staff in active employment	4.615.600	54%	4.800.224	55%	4.992.233	56%	5.191.922	57%	5.399.599	58%
Chapter 12 - Recruitment expenditure	487.362	6%	506.856	6%	527.131	6%	548.216	6%	570.145	6%
Chapter 13 - Socio-medical services and training	164.578	2%	171.161	2%	178.007	2%	185.127	2%	192.532	2%
Chapter 14 - Temporary assistance	229.878	3%	239.073	3%	248.636	3%	258.581	3%	268.924	3%
Title 2 - Costs associated to the functioning of the Agency	***536.417***	***6%***	***547.145***	***6%***	***558.088***	***6%***	***569.250***	***6%***	***580.635***	***6%***
Title 3 - Costs related to operational activities	***2.588.246***	***30%***	***2.531.701***	***29%***	***2.461.395***	***27%***	***2.391.703***	***26%***	***2.315.860***	***25%***
Chapter 30 - Group Activities	727.830	9%	742.387	8%	757.235	8%	772.379	8%	787.827	8%
Chapter 32 - Other Operational Activities	495.856	6%	505.773	6%	515.889	6%	526.207	6%	536.731	6%
Remaining budget for Operations of Cooperation and Support Department and the Technical Department	1.364.560	15%	1.283.541	15%	1.188.272	13%	1.093.117	12%	991.302	11%
Total expenditure	**8.622.080**	**100%**	**8.796.160**	**100%**	**8.965.489**	**100%**	**9.144.799**	**100%**	**9.327.695**	**100%**

Overview of budget under OPTION 3										
	Budget 2012	**%**	**Budget 2013**	**%**	**Budget 2014**	**%**	**Budget 2015**	**%**	**Budget 2016**	**%**
Administrative staff	21		21		23		23		23	
Operational staff	40		40		49		60		76	
TOTAL	**61**		**61**		**72**		**83**		**99**	
Breakdown of total budget										
EU Budget	***9.262.000***		***9.449.000***		***12.409.087***		***14.948.281***		***18.824.525***	
Third country contributions (EFTA)	*222.288*		*226.776*		*297.818*		*358.759*		*451.789*	
Total budget for ENISA	**9.484.288**	**100%**	**9.675.776**	**100%**	**12.706.906**	**100%**	**15.307.040**	**100%**	**19.276.313**	**100%**
Breakdown of total expenditure										
Title 1 - Staff expenditure	***6.031.824***	***64%***	***6.239.860***	***64%***	***7.866.298***	***62%***	***9.528.461***	***62%***	***12.073.953***	***63%***
Chapters 11, 13, 14 – incl. staff in active employment, socio-medical services and training, temporary assistance	5.668.891	60%	5.895.647	61%	7.316.466	58%	8.933.847	58%	11.295.145	59%
Chapter 12 – Recruitment expenditure	362.933	4%	344.213	4%	549.832	4%	594.614	4%	778.809	4%
Title 2 - Costs associated to the functioning of the Agency	***559.017***	***6%***	***570.256***	***6%***	***647.328***	***5%***	***727.256***	***5%***	***841.176***	***4%***
Title 3 - Costs related to operational activities	***2.893.447***	***31%***	***2.865.660***	***30%***	***4.193.279***	***33%***	***5.051.323***	***33%***	***6.361.183***	***33%***
Chapter 30 - Group Activities	727.830	8%	742.446	8%	824.133	6%	908.791	6%	1.028.113	5%
Chapter 32 - Other Operational Activities	495.856	5%	505.773	5%	515.889	4%	526.207	3%	536.731	3%
Remaining budget for Operations of Cooperation and Support Department and the Technical Department	1.669.760	18%	1.617.440	17%	2.853.257	22%	3.616.326	24%	4.796.340	25%
Total expenditure	**9.484.288**	**100%**	**9.675.776**	**100%**	**12.706.906**	**100%**	**15.307.040**	**100%**	**19.276.313**	**100%**

Overview of budget under OPTION 4										
	Budget 2012	**%**	**Budget 2013**	**%**	**Budget 2014**	**%**	**Budget 2015**	**%**	**Budget 2016**	**%**
Administrative staff	21		21		33		39		44	
Operational staff	40		40		86		116		151	
TOTAL	**61**		**61**		**119**		**155**		**195**	
Breakdown of total budget										
EU Budget	***9.262.000***		***9.449.000***		***24.085.495***		***31.159.272***		***40.699.021***	
Third country contributions (EFTA)	*222.288*		*226.776*		*578.052*		*747.823*		*976.777*	
Total budget for ENISA	**9.484.288**	**100%**	**9.675.776**	**100%**	**24.663.547**	**100%**	**31.907.094**	**100%**	**41.675.798**	**100%**
Breakdown of total expenditure										
Title 1 - Staff expenditure:	***6.031.824***	***64%***	***6.220.376***	***64%***	***13.844.519***	***56%***	***18.214.025***	***57%***	***23.985.356***	***58%***
Chapters 11, 13, 14 – incl. staff in active employment, socio-medical services and training, temporary assistance	5.668.891	60%	5.895.647	61%	12.340.761	50%	16.842.359	53%	22.310.572	54%
Chapter 12 – Recruitment expenditure	362.933	4%	324.730	3%	1.503.758	6%	1.371.666	4%	1.674.784	4%
Title 2 - Costs associated to the functioning of the Agency	***1.059.074***	***11%***	***1.070.256***	***11%***	***2.680.057***	***11%***	***3.163.728***	***10%***	***3.937.429***	***9%***
Title 3 - Costs related to operational activities:	***2.393.390***	***25%***	***2.385.144***	***25%***	***8.138.971***	***33%***	***10.529.341***	***33%***	***13.753.013***	***33%***
Chapter 3 0 - Group Activities	727.830	8%	742.387	8%	1.111.782	5%	1.352.884	4%	1.634.789	4%
Chapter 3 2 - Other Operational Activities	495.856	5%	505.773	5%	515.889	2%	526.207	2%	536.731	1%
Remaining budget for Operations of Cooperation and Support Department and the Technical Department	1.169.703	12%	1.136.984	12%	6.511.300	26%	8.650.250	27%	11.581.494	28%
Total expenditure	**9.484.288**	**100%**	**9.675.776**	**100%**	**24.663.547**	**100%**	**31.907.094**	**100%**	**41.675.798**	**100%**

Overview of budget under OPTION 5										
	Budget 2012	**%**	**Budget 2013**	**%**	**Budget 2014**	**%**	**Budget 2015**	**%**	**Budget 2016**	**%**
Administrative staff	21		21		35		41		47	
Operational staff	40		40		91		124		161	
TOTAL	**61**		**61**		**126**		**165**		**208**	
Breakdown of total budget										
EU Budget	***9.262.000***		***9.449.000***		***25.490.605***		***33.228.806***		***43.316.593***	
Third country contributions (EFTA)	*222.288*		*226.776*		*611.775*		*797.491*		*1.039.598*	
Total budget for ENISA	**9.484.288**	**100%**	**9.675.776**	**100%**	**26.102.379**	**100%**	**34.026.297**	**100%**	**44.356.191**	**100%**
Breakdown of total expenditure										
Title 1 - Staff expenditure	**6.031.824**	**64%**	**6.220.376**	**64%**	**14.669.733**	**56%**	**19.470.563**	**57%**	**25.600.477**	**58%**
Chapters 11, 13, 14 – incl. staff in active employment, socio-medical services and training, temporary assistance	5.668.891	60%	5.895.647	61%	13.026.861	50%	17.984.029	53%	23.794.743	54%
Chapter 12 – Recruitment expenditure	362.933	4%	324.730	3%	1.642.872	6%	1.486.534	4%	1.805.734	4%
Title 2 - Costs associated to the functioning of the Agency	**1.059.074**	**11%**	**1.070.256**	**11%**	**2.818.861**	**11%**	**3.327.056**	**10%**	**4.118.171**	**9%**
Title 3 - Costs related to operational activities	**2.393.390**	**25%**	**2.385.144**	**25%**	**8.613.785**	**33%**	**11.228.678**	**33%**	**14.637.543**	**33%**
Chapter 3 0 - Group Activities	727.830	8%	742.387	8%	1.151.271	4%	1.417.330	4%	1.716.957	4%
Chapter 3 2 - Other Operational Activities	495.856	5%	505.773	5%	515.889	2%	526.207	2%	536.731	1%
Remaining budget for Operations of Cooperation and Support Department and the Technical Department	1.169.703	12%	1.136.984	12%	6.946.626	27%	9.285.142	27%	12.383.855	28%
Total expenditure	**9.484.288**	**100%**	**9.675.776**	**100%**	**26.102.379**	**100%**	**34.026.297**	**100%**	**44.356.191**	**100%**

ANNEX 6: COMPARISON OF ENISA'S BUDGET AND STAFF WITH THAT OF OTHER EUROPEAN REGULATORY AGENCIES

Agencies of the 1st pillar (Community policies)

	Name of the Agency	Place	Agency estimated revenues 2008 (Thousands €)	Community contribution (thousands €)	Staff 2008 (authorised under Community budget)
OHIM	Office for Harmonisation in the Internal Market	ES- Alicante	300 610	pm	643
EMEA	European Medicines Agency	UK-London	164 480	38 000	475
EASA	European Aviation Safety Agency	DE-Koln	85 330	30 000	452
FRONTEX	European Agency for the Management of Operational Cooperation at the External Boarders	PL-Varsovie	69 000	68 000	69
ECHA	European Chemicals Agency	FI-Helsinki	66 425	62 619	220
EFSA	European Food Safety Authority	IT- Parma	63 500	63 500	335
EMSA	European Maritime Safety Agency	PT-Lisbon	44 435	44 300	165
CDT	Translation Centre for the bodies of the EU	LU- Luxemburg	42 252	--	233
ECDC	European Centre for Disease Prevention and Control	SE-Stockholm	39 100	39 100	130
EEA	European Environment Agency	DK-Copenhagen	36 414	31 672	123
EURO FOUND	European Foundation for the Improvement of Living and Working Conditions	IE-Dublin	21 200	20 000	101
EAR	European Agency for Reconstruction	EL- Thessaloniki	20 000	0	91
ERA	European Railway Agency	FR-Valenciennes	18 000	18 000	116
ETF	European Training Foundation	IT-Torino	17 984	17 984	96
Cedefop	European Centre for the Development of Vocational Training	EL- Thessaloniki	17 162	17 060	99
FRA	Fundamental Rights Agency	AT-Viena	15 000	15 000	49
EU-OSHA	European Agency for Occupational Safety and Health	ES-Bilbao	14 697	14 400	44
EMCDDA	European Monitoring Centre for Drugs and Drug Addiction	PT-Lisbon	14 078	13 400	82
CPVO	Community Plant Variety Office	FR-Angers	12 352	pm	43
GSA	European GNSS Supervisory Authority	BE-Brussels	10 560	10 560	50
ENISA	**European Network and Information Security Agency**	**EL-Heraklion**	**8 160**	**8 160**	**44**
CFCA	Community Fisheries Control Agency	ES-Vigo	7 300	7 300	49
EIGE	European Institute for Gender Equality	LT-Vilnius	6 430	6 430	20

Agencies of the 2nd pillar (Common Foreign and Security Policy)

	Name of the Agency	Place	Agency estimated revenues 2008 (Thousands €)	Staff 2008 (authorised under Community budget)
EDA	European Defence Agency	BE-Brussels	27 000	120
EUSC	European Union Satellite Centre	ES-Torrejon de Ardoz	14 500	99
ISS	European Institute for Security Studies	FR-Paris	3 800	26

Agencies of the 3rd pillar (Police and Judicial Cooperation in Criminal Matters)

	Name of the Agency	Place	Agency estimated revenues 2008 (Thousands €)	Community contribution (thousands €)	Staff 2008 (authorised under Community budget)
Europol		NL-Den Haag	21 000		101

Comparison of Title 1 and Title 3 expenditures of a sample of 1st pillar Agencies

	Name of the Agency	Staff expenditures		Operational expenditures		Total budget
		In Tsd EUR	In % of total	In Tsd EUR	In % of total	
ERA	European Railway Agency	13.403	63,8%	5.200	24,8%	21.000
EFSA	European Food Safety Agency	30.084	57,1%	23.104	35,1%	65.900
ECHA	European Chemicals Agency	38.134	53,2%	22.696	31,7%	71.635
EMEA	European Medicines Agency	64.360	34,1%	80.281	42,5%	188.689
EMSA	European Maritime Safety Agency	19.266	39,4%	26.335	53,9%	48.885

ANNEX 7: CASE STUDIES

Three case studies regarding additional roles for ENISA were selected for a more in-depth Cost-Benefit Analysis (CBA) with the aim to provide a more detailed and an as far as possible quantified analysis of the likely impact of specific functions that are part of policy options on the European market as a whole. More precisely, the costs and benefits of each of the functions described in the case studies will be weighted against a situation in which ENISA does not take up this function.

For each of the case studies, the comparison between the adding or not of a specific function to the task package of ENISA will be developed according to the following steps:

- Recapitulation of the problem and likely effect of adding or not the specific function to ENISA's task package;
- Qualitative comparison
- Estimation of costs and benefits
- Final assessment: advantages and disadvantages

Ideally, the CBA should be based on significant and reliable quantitative data. The specific nature of the case studies however will often make it very difficult to actually quantify the economic impacts as the required information sources are often not existent, or at least incomplete and non exhaustive. Moreover, since the CBA is forward looking, the unpredictability of future evolutions and events introduces an additional level of uncertainty. Therefore, the values presented in the CBA will mainly consist of estimates of an order of magnitude.

Case study 1: ENISA becomes a facilitator in the organisation of European scale (and global) NIS exercises

Recapitulation of the problem

Security exercises are an important means to prepare all stakeholders to deal efficiently and effectively with security incidents. Those exercises can be very costly but are indispensable to enable stakeholders to avoid that they incur even more costs in case they are ill-prepared. At the national level, some Member States are already performing regular exercises on an annual or multi-annual basis.

At the regional or at the European level, a couple of exercises are starting to be developed. For instance, there is a project of a pan Nordic exercise. At the European level, the Commission (in particular Directorate-General Justice, Liberty, Security) is supporting Financial programme related to security exercise. ENISA is also stimulating initiative on CERT security exercise[100]. The NATO is also conducting NIS annual exercises among the military forces of its members. In this case, the role of the NATO is to identify the players in

[100] ENISA has already started to work on CERT security exercises in the context of the WPK 2.2.: Security competence and good practice sharing for CERT communities

the exercise, participate in the drafting of the mission plan and crisis scenario and disseminate results amongst participants.[101]

However, given the European scale of security issues and the importance of exercises to improve the handling of security incidents, additional pan-national exercises are needed in the medium term. Indeed the Action Plan in the Communication on CIIP[102] indicated that the Commission will financially support the development of pan-European exercises on Internet security incidents[103]. These operational platforms could then also be used for participating in other international exercises.

ENISA could play an important role in the EU in stimulating and supporting such exercises without having an operational role. ENISA would strengthen the cooperation between National/Governmental CERTs (incl. the leveraging and expansion of existing cooperation mechanisms like the EGC). ENISA could also contribute to identifying the participants to the exercises, participate in the drafting of the crisis scenario, and disseminate the results of the exercises. In addition, ENISA would be the main contact point for organising the participation of the EU in international exercises. In this respect, ENISA will also be contributing to the proposition on a roadmap to support European involvement and participation in these global exercises on recovery and mitigation of large-scale Internet incidents.

Qualitative comparison

Today, the number of European civil NIS exercises is clearly insufficient as they are only emerging on a regional basis. The number of exercises is sub-optimal because, on the one hand, many security issues are of European dimension, hence need a European approach but there is no institution at the European level that is facilitating or coordinating these. On the other hand, the effectiveness of the exercises to prevent or improve the management of security incidents has clearly been demonstrated with the national exercises or with the international exercises (the NATO, US CyberStorm ...)

As the number of regional and European security exercises is sub-optimal, there is a need for additional exercises. ENISA is particularly well suited to stimulate, support and possibly coordinate such exercises because of its characteristics. ENISA has build and is currently building relationships with Member States via the Management Board and the National Liaison Officers and with private sector via the PSG. This allows ENISA to set-up exercises between parties for which it is very difficult to set-up comparable exercises between themselves (e.g. cross-sector or companies belonging to other parts of the value chain) and thus create real added value for the private parties involved. Furthermore, ENISA has expertise in NIS and is starting to acquire expertise in the particular issue of security exercises[104] and has access to a large network of world-class experts. This implies that ENISA cannot only bring public and private parties together, but can add the inputs and advice of independent academics and practitioners. Finally and most importantly, ENISA by its

[101] Based on information provided during the interviews with stakeholders, the cost of the NATO annual exercise has been estimated to 100 million dollars.

[102] COM(2009) 149 final, 30.3.2009.

[103] The Financial support for the actual development of these exercises is part of the EC Programme "*Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks*" (http://ec.europa.eu/justice_home/funding/cips/funding_cips_en.htm), whose total budget envisaged for the year 2009 is € 17,7 million EUR.

[104] ENISA has already started to work on CERT security exercises in the context of the WPK 2.2.: Security competence and good practice sharing for CERT communities

composition and experience always adopts a European perspective to the issue it has to deal with, hence would be suited to stimulate exercises of pan-European nature.

Thus from a qualitative perspective, there is a need to increase the number of pan-European exercises in information security, and there is an opportunity to give ENISA the function to ensure the development of the required exercises. To ensure feasibility and efficiency, the approach of ENISA should be gradual, i.e. ENISA should first support exercises at limited regional level and for which there is demand of the specific Member States. In a later stage, ENISA could then identify gaps regarding the MSs and regions where no exercises took place yet, develop exercises between MSs with less strong bi-lateral relations or facilitate exercises with a larger geographical scope.

Estimation of costs and benefits

Regarding the costs, the support provided to regional or European NIS exercises would require additional resources for ENISA. It would also require important resources for the participating national bodies[105] and private firms. However, if regional or European exercises would replace national exercises, the cost of running and participating to national exercises should be deduced from the cost of pan-national exercises.

Regarding the benefits, such regional or European security exercises will improve prevention of security breaches as well as the management of the breaches that could not be prevented. Given the limited availability of data regarding the costs of security incidents[106], the benefits of additional prevention and better management of incidents, and in particular the precise effect of security exercises on the prevention and improved management, it is very difficult to give a precise assessment of the benefits of the regional or European exercises. However, it may be expected that the benefits of regional or European security exercises are larger than the benefits of similar national exercises as the participation base (hence the knowledge and good practices to be exchanged) will be broader, and because European exercises may internalize the externalities existing between the networks of the Member States. Moreover, the benefits will be particularly important for the Member States that do not currently run security incidents.

	ENISA stimulates and supports regional or European security exercises	**ENISA does not stimulate and support regional or European security exercises**
Cost for the EU budget	Additional costs for ENISA. Those may be limited at the beginning if ENISA focuses first on a limited number of regional exercises. Moreover, ENISA will merely support the exercises, but will not have an operational role.	No additional cost.

[105] Based on the information provided during interviews with stakeholders, the cost of the recent national security exercise in a Member State has been estimated at 50 * 200 working hours in preparing and planning such exercises. This relates to 6 to 7 FTEs.

[106] The vast majority of security incidents (93% in some cases) are not reported. However for some estimates of the cost of security incidents see section 2.2.2 of this Report.

[107] The operational cost of running one E3P on exchange of information has been assessed by some stakeholders at 250kEUR.

	ENISA stimulates and supports regional or European security exercises	ENISA does not stimulate and support regional or European security exercises
	The cost of a team of e.g. 2 FTEs would correspond to approx. 200kEUR a year (staff expenditure) to which another 750kEUR[107] of operational expenditure should be added.	
Cost for the Member States and undertakings	Additional costs for the Member States authorities and private firms in participating in the regional and European exercises. However, if regional or European exercises would replace national exercises, the cost of running and participating to national exercises should be deduced from the cost of pan-national exercises.	No additional cost.
Benefits related to an improved prevention of security breaches	Exercises will improve the prevention, and decrease the number (and hence the costs) of incidents.	No additional benefit.
Benefits related to an improved management of security breaches	Exercises will ensure a better and more efficient management of incidents.	No additional benefit
Distributional effects	Public authorities will benefit from better security, in particular the Member States that do not currently run security incidents or the Member States that would gain substantially of an improved EU coordination. ICT firms, especially the small ones will benefit from information and exchange of best practices. Citizens will benefit from better information security.	

Final assessment

The potential benefits of supporting regional and European exercises are important in terms of better prevention and better management of security incidents as they will contribute to

decrease the important and growing costs of security incidents[108]. Those benefits will accrue to the Member States and their public sector (in particular those that are not currently familiar with security exercises), the ICT and non ICT firms, as well as to the citizens who will at the end enjoy more secure services. There will be additional costs for ENISA, but these can be limited at the beginning as ENISA could first concentrate on only a few regional exercises. The costs for the Member States and the industry in participating to such exercises may be important, but if regional exercises would replace national exercises, those costs of participating to pan-national exercises should be offset against the cost of participating to national exercises.

It is reasonable to assume that the net benefit for the European economy of giving ENISA the function and the means to support regional and pan-European exercises is positive, and is therefore a better option than not giving ENISA the mandate and the means to perform such a function.

Case study 2: Stimulate the establishment of European Public Private Partnership in the field of NIS

Recapitulation of the problem

Most of the issues related to information security cannot be dealt efficiently by the public authorities alone and should involve the private sector, in particular the ICT firms, because private firms control most of the critical infrastructure, develop most of the service applications and thus have the relevant expertise.

Therefore, an increasing number of Member States are setting up PPP at the national level to deal with security issues, currently in particular related to the resilience of networks. Examples are:

- In the UK, the CPNI set up 12 information exchanges with several sectors of the economy (finance, defense, SCADA, water supply, vendors, security researchers, network security, space industry, Northern Ireland cross sector, managed service provider, transport and pharmaceutical);[109]
- The Netherlands follow a similar approach of PPP with the different cybercrime Information Exchanges involving 8 industry sectors (banks, water, energy, airports, rail, Port of Rotterdam, Multi-nationals, and SCADA);[110]
- Germany, in the context of the CIP Implementation Plan (UP KRITIS) of 2007, set up a PPP made of public authorities (including BMI, BMWi, BSI, BNetzA) and several private companies.[111]

With the multiplication of PPP at the national level, experience shows that this approach is very promising. In practice, the functions of the national PPP may be diverse: exchange of

[108] See Section 2.2.2 of the Report.
[109] See the presentation of A. Powell of CPNI at the Commission workshop on European PPP for Resilience on 17 June 2009.
[110] See NICC paper on PPP in the Cybercrime Information Exchange.
[111] See the presentation of M. Pilgermann of BMI at the Commission workshop on European PPP for Resilience on 17 June 2009.

confidential and not confidential information related to security incidents, awareness raising, security exercises, etc.

At European level, some PPP are starting to emerge (such as the information sharing networks that are bringing together some important European banks) [112], but their number remains very limited and there is no systematic evaluation of their need nor a specific authority in charge of the establishment of E3P when necessary. In that regard, ENISA could play an important role in supporting European PPP, in particular to ensure the resilience of networks.

Indeed in the Communication on CIIP, the importance of a stronger cooperation between the public and private sector by means of a partnership at European level EP3R (European Public Private Partnership for Resilience) was stressed. The primary focus of the EP3R would be on the European dimension from strategic (e.g. good policy practices) to tactical/operational (e.g. industrial deployment perspectives).

Related to this point of the CIIP Action Plan, ENISA could provide assistance in fostering such cooperation on security and resilience objectives, baseline requirements, good policy practices and measures. In order to facilitate, ENISA could contribute to the development of a roadmap and plan for the establishment of an EP3R.

Qualitative comparison

Today, the number of European PPP in information security is clearly insufficient as their absolute number is very limited, often only emerging and not always stable in time, and their relative number compared to the number of national PPP is negligible. Thus, the number of E3P is sub-optimal because, on the one hand, many security issues are of European dimension, hence need a European approach, and on the other hand, the efficiency of the PPP approach to deal with security issues has clearly be demonstrated with the national PPP.

Therefore, there is a need to identify the areas where the establishment of additional E3P would be beneficial for the European economy and the citizens. Given its characteristics (expertise, flexibility, relationship with stakeholders), ENISA is particularly well suited to fulfill this function. Thus from a qualitative perspective, there is a need to increase the number of E3P in information security, and there is a need to give ENISA the function to ensure the establishment of the needed E3P. To ensure efficiency, the approach of ENISA should be bottom-up, ENISA should support initiatives for which there is demand of the private sector. ENISA should first determine first priority PPP in a dialogue with the PSG, do a feasibility study,[113] and then only participate in the setting up of the E3P. At the beginning at least, participation should be made voluntary and only, after some times and if necessary, could be made compulsory.

It is thus preferable to give ENISA the function and the means to stimulate E3P compared to not involving ENISA in EP3.

Estimation of costs and benefits

[112] See the presentation of W. Hafkamp at the 2009 ENISA Summer School.
[113] See the ENISA feasibility studies related to customers' confidence or to European alert system

Regarding the costs, the identification, and the support or even the coordination of European PPP would require additional resources for ENISA. However, those additional resources may be limited at the beginning and increase over time proportionality to the success of the realized PPP. Following a bottom-up and evolutionary approach, ENISA should first focus on the most important and most demanded PPPs (first priority) and then, if and as the role of ENISA is successfully recognized, focus on second priority PPPs. Establishing PPPs would also require some resources for the participating national bodies and private firms, but if participation is voluntary, it is expected that the benefits would outweigh its costs (otherwise, the national body or private firm will not join the PPP).

Regarding the benefits, such European PPP will improve prevention of security breaches as well as a decrease of the impact of the breaches that could not have been prevented. Given the limited data regarding to the costs of security incidents, the benefits of additional prevention and better treatment of incidents, and in particular the precise effect of PPP on the prevention and improved handling of incidents, it is impossible to give a precise assessment of the benefits of the E3P. However, it may be expected that the benefits of European PPP are larger than the benefits of national PPPs because the participation base (hence the knowledge and good practices to be exchanged in the PPP) will be broader, and because European PPP may internalise the externalities existing between the networks of the Member States.

	ENISA stimulates the establishment of EP3	**ENISA is not Involved in EP3**
Cost for the EU budget	Additional Costs for ENISA. However, those costs may be limited at the beginning as ENISA should focus on the most demanded PPPs and will merely support the European PPPs, but will not have an operational role. The initial cost can be estimated to estimated to 2 FTEs and 750kEUR.[114] Over time, if the approach is successful, the cost will increase.	No additional cost.
Cost for the industry	Costs for the firms participating in the PPP. However, if the participation is voluntary, participation will imply that the benefit exceeds the cost. Moreover if the EP3 replace national PPP, increased participating costs to an EP3 may be offset by the decreasing cost due to the disappearance of	No additional cost.

[114] The operational cost of running one E3P on exchange of information has been assessed by some stakeholders at 250kEUR.

	ENISA stimulates the establishment of EP3	ENISA is not Involved in EP3
	national PPP. A harmonised approach to NIS prior to the deployment of new initiatives or measures, could avoid costs related to an "ex-post" harmonisation.	
Benefits related to an improved incident handling.	Exchange of information and good practices among the EP3 will improve the prevention, and decrease the number (hence the costs) of incidents.	No additional benefit.
Benefits related to an improved treatment of security breaches	Exchange of information and good practices among the EP3 will ensure a better and more efficient treatment of incidents.	No additional benefit
Benefits related to a preventive harmonised approach to NIS	E3P enables directly a harmonised approach to NIS prior to the deployment of new initiatives or measures. That could avoid posterior European intervention to harmonise divergent national approaches and the related costs of such harmonisation.	
Distributional effects	Public authorities will benefit from better security. ICT firms, especially the small ones will benefit from information and exchange of best practices. Citizens will benefit from better information security.	

Final assessment

The potential benefits of supporting European PPP are substantial in term of better prevention and better handling of security incidents. Those benefits will accrue to the public sector, the ICT and non ICT firms, as well as the citizens. New costs will be supported by ENISA, but those can be limited at the beginning if ENISA follows a progressive approach focusing first on the most demanded PPPs and if ENISA will not have an operational role. There are costs for the industry to participate in European PPP, but if participation is made voluntary, we may expect that the benefits exceed the costs.

It is reasonable to assume that the net benefit for the European economy of giving ENISA the function and the means to identify the need for E3P in security and to support the establishment of such E3P is positive, and is therefore a better option that not giving ENISA the mandate and the means to perform such a function.

Case study 3: ENISA becomes the cert for EU Bodies

Recapitulation of the problem

At the national level, an increasing number of Member States are setting up governmental CERT/CSRIT that are competent horizontally for all activities of the government[115].

At the European level, there is currently no common EU CERT. This reflects the decentralisation culture among EU institutions and bodies (and for the large institutions the decentralisation inside each institution). The European institutional landscape is made of several bodies having different tasks and consequently different risk profiles: the Council, the Parliament, the Commission including its delegations spread around the world, the Court of Justice, the Court of Auditors, the Committee of Regions, the Economic and Social Committee, the Ombudsman, the EDPS, the European Central Bank, the European Investment Bank, the regulatory and executive agencies, etc. Today, each institution organises its network security according to an individual IT policy. For instance, the IT security policy at the Commission is ensured by several Directorates-General such as DS/5 in DG Personnel and Administration and DG Informatics. The creation of an EU CERT has been discussed at the political level, but the idea has not enjoyed full support.

Given the growing importance of security threats to the national and international public institutions and the growing complexity of NIS responses, the future issues are (i) whether all the EU institutions and bodies should follow a common security policy, (ii) whether such common policy should be ensured by a single body, (iii) how extensive the functions of this common body should be (alert, intervention, policy compliance), and (iv) whether ENISA should play this role[116].

Qualitative comparison

Today, the Computer Emergency Policies in the different EU institutions and bodies are different, and in some cases, insufficient to deal with the security threats that are growing in importance and complexity. Thus some institutions should clearly improve their emergency and crisis policies to ensure business continuity. However at this stage of coordination between EU institutions, it is not clear that it is necessary and appropriate to adopt a common crisis policy. The advantages of such a common policy are economies of scope and scale, as well as exchange of good practices. Drawbacks of a common approach may be duplication of tasks, or lack of flexibility with the difficulty to deal with different levels of risk. To maximize the advantage and minimize the drawbacks, the role of ENISA may be limited to be a CERT for the European agencies, whose size is often too small (see Annex 7) to set up a dedicated CERT.

Even if a common approach would be preferable, it is not clear that ENISA should play the CERT role for the EU institutions. Currently, ENISA has a policy support role but no operational role. If ENISA should become a CERT in addition to its policy function, that would radically change the institution. This change would of course imply that additional operational expertise becomes available and which could be beneficial for ENISAs policy

[115] See http://www.enisa.europa.eu/act/cert/background

[116] ENISA has already a role of coordination between the CERTs active in the Member States or of contributing to the capacity building of such CERTs. See the WPK 2.2. Security competence circle and good practice sharing for CERT communities.

function. On the other hand, it will require ENISA to develop new expertise and to attract a large volume of new staff with new profiles.

Estimation of costs and benefits

Regarding the costs, ENISA will have to recruit a lot of new operational staff able to ensure security and incident handling on a 24/7 basis. Moreover, the different needs and risk profiles of the EU institutions will require, in some cases, an adapted and tailor-made security policy[117]. The exact cost will of course depend on the exact functions the CERT would take up (e.g. top-level monitoring and reporting and guidance but no real-time response or detailed monitoring, analysis and timely response). Other factors that would determine the precise cost for ENISA becoming the EU CERT are the scale of the networks and information systems for which ENISA would become a CERT, the geographical distribution of the networks and the complexity (e.g. in terms of different technology platforms used).

Regarding the benefits, the CERT capacity of the EU institutions should improve, especially for the institutions that have the weakest CERT capability. However in the absence of a clear evaluation of the CERT capability of each EU institution, it is impossible to quantify such benefits. Furthermore, the improved expertise that ENISA will gain with its new operational function will surely improve its policy support function. However, such beneficial spill-over effect is extremely difficult, if not impossible, to quantify.

	ENISA is the common CERT for the EU institutions and bodies	**ENISA is not the common CERT for the EU institutions and bodies**
Cost for the EU budget	Substantial additional cost for ENISA as it will require recruiting a large staff (up to 40 FTE)[118] with operational skills and additional technical equipment.	No additional cost.
Costs to the EU institutions due to the centralised NIS security procedures	The centralisation of part of the security policy may increase the cost of coordination among institutions and create a lack of flexibility.	No additional cost.
Benefits to the EU institutions and bodies related to an improved	Having a common EU CERT may improve the prevention and management of security (hence the costs) of incidents, especially	No additional benefit.

[117] For a study on the cost of CERTs, see http://www.cert.org/archive/pdf/03tr001.pdf, in particular Section 3.3

[118] Based on information provided during the interviews with stakeholders, we estimate that a team of 10-12 people is needed on a 24/7 basis (which requires 3 to 4 shifts). Some stakeholders have made a first global assessment that establishing a CERT for the European Commission alone would require approximately 14 FTE and equipment cost of 2 500kEUR for the setup phase and 400kEUR for the maintenance phase, supposing however that this team can immediately benefit from specific technical expertise on-demand and from standard corporate services.

prevention and management of security breaches	for EU institutions having the weakest CERT capability.	
Benefits related to an improved operational expertise for ENISA	Giving an operational role to ENISA will increase its expertise; hence improve the quality of its policy support activities.	No additional benefit
Distributional effects		

Final assessment

The additional costs for ENISA of being an EU CERT are clearly identifiable, at least in part. They will be substantial as they will require a near doubling of ENISA current budget. The benefits are however less certain. They may be important, but at this stage, it is not possible to obtain evidence for this.

Given the certainty of the important costs and the uncertainty of the benefits, it is reasonable to assume at this stage that the net benefit of having ENISA as a common EU CERT is negative, and is not therefore a better option than not giving ENISA the mandate and the means to perform such a function.

ANNEX 8: LIST OF PERSONS INTERVIEWED

Name	Organisation	Function
People within ENISA		
Mr. A. Pirotti	ENISA	Executive Director
Mr. S. Purser	ENISA	Head of Technical Competence Department
Mr. A. Mitrakas	ENISA	Head of Administration
People outside ENISA (in alphabetical order)		
Mrs. A. Buchta	DG INFSO/B1	Policy Officer / Developer Privacy, trust and related areas
Mr. C. Brookson	Department for Business Innovation and Skills (BIS)	Director, Standards & Technology at Department
Mr. J. Chatzimarkakis	European Parliament	Member of the European Parliament
Mr. P. Dorey	CSO Confidential	Co-Founder and Director
Mr. A. Esterle	Esteral Consulting	
Mr. F. García Morán	DG Informatics	Director General
Dr. W. Hafkamp	Rabobank	Group ICT Policy & Architecture
Mr. Ilias Chantos	Symantec	Director EMEA & APJ - Government Relations SYMANTEC
Mr. P. Hustinx	European Data Protection Supervisor (EDPS)	Supervisor
Dr. C. Vishik	Intel Corporation UK	Security & Privacy Technology & Policy Manager
Dr. S. van Merkom	Ministry of Economic Affairs The Netherlands	Section ICT Security Senior policy advisor

ANNEX 9: LIST OF ABBREVIATIONS

BEREC	Body of European Regulators in Electronic Communications
CEPOL	European Police College
CERT	Computer Emergency Response Teams
CII	Critical Information Infrastructures
CIIP	Critical Information Infrastructures Protection
CII	Critical Information Infrastructures
CIIP	Critical Information Infrastructures Protection
CIWIN	Critical Infrastructure Warning Information Network
CSIRT	Computer Security Incident Response Team
DNS	Domain Name System
DoS attacks	Denial-of-service attack
EDA	European Defence Agency
EDPS	European Data Protection Supervisor
EECMA	Electronic Communications Market Authority
EFTA	European Free Trade Association
EGC	European Governmental CERTs Groups
eID	Electronic Identification
EISAS	European Information Sharing and Alert System
ENISA	European Network and Information Security Agency
EP3R	European Public Private Partnership for Resilience
EPCIP	European Programme for Critical Infrastructure Protection
ERG	European Regulators Group
ESRP	European Security Research Program
FIRST	Forum for Incident Response and Security Teams
FP7	7th Framework Programme
ISO	International Standardisation Organisation
ICT	Information and Communication Technologies
ITU	International Telecommunication Union
JRC	Joint Research Center
NIS	Network and Information Security
NISSG	Network and Information Security Steering Group
NRA	National Regulatory Authority
OECD	Organisation for Economic Co-operation and Development
PPP	Public Private Partnership
R&D	Research & Development
SME	Small and Medium Enterprises
SOX	Sarbanes-Oxley Act
TERENA	Trans-European Research and Education Networking Association
TFEU	Treaty on the functioning of the European Union

ANNEX 10: PUBLIC CONSULTATION ON THE FUTURE OF THE EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY - SUMMARY OF THE RESULTS

EUROPEAN COMMISSION
Information Society and Media Directorate-General

Brussels, 27 November 2007

SUMMARY OF RESULTS OF THE PUBLIC CONSULTATION ON THE FUTURE OF THE EUROPEAN AND NETWORK AND INFORMATION SECURITY AGENCY

1. BACKGROUND

In order to enhance the capacity of the Community, the Member States and consequently the business community to prevent, to address and to respond to major network and information security risks, the European Network and Information Security Agency (ENISA) was established in 2004 for a period of five years.[119] The Agency was established with the main goal of "ensuring a high and effective level of network and information security within the Community, (..) in order to develop a culture of network and information security for the benefit of the citizens, consumers, enterprises and public sector organisations of the European Union, thus contributing to the smooth functioning of the internal market."

In accordance with Article 25 of the ENISA Regulation, the Commission carried out an evaluation of the Agency, taking into account the views of all relevant stakeholders. In June 2007, the Commission issued a Communication to the European Parliament and to the Council on the evaluation of ENISA.[120] The Communication presented the findings of an external panel of experts that carried out an evaluation of the Agency and the recommendations of the ENISA Management Board regarding the ENISA Regulation.[121] It also made an appraisal of the evaluation report and launched a public consultation.

The public consultation was available on-line from 13 June to 7 September 2007. 44 Contributions were received during this period. After the possibility to reply on-line was closed, 2 more contributions were received to reach the total of 46 contributions. This Working Paper analyses all these responses.

The responses came from a variety of stakeholders and interested parties, including Member States' ministries, regulatory bodies, industry and consumer associations, academic

119 Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency - OJ L 77, 13.3.2004, p. 1 (hereinafter "ENISA Regulation")
120 COM(2007)285 of 1.6.2007
121 See Article 25 of the ENISA Regulation

institutions, companies, and individual citizens. A list of respondents is annexed. 15 Out of the 46 respondents requested that their name would not be published.

2. OVERVIEW OF CONTRIBUTIONS

1. What are currently the most important challenges to network and information security? What has changed since 2004, when ENISA was established? To which issues is a European response most needed? Is an Agency still the right instrument or would another mechanism be better suited to deal with these issues?

Highlights

The majority of respondents considered that the threat landscape has evolved since ENISA was established: challenges have changed in nature and increased in complexity. Attacks have become more targeted and more difficult to detect. Hackers have become motivated by financial means or political motivation rather than 'show-off'. Increased use of networks, emerging technologies, the need to improve the level of security in software, and vulnerability of important IT infrastructures pose further challenges. In addition, the globalisation of threats and global interdependencies have magnified a need for enhanced international cooperation and coordination. Most respondents agreed that an Agency would still be the right instrument to deal with these challenges.

The majority of respondents highlighted a change in the threat landscape, with cyber-attacks being increasingly driven by financial or political motivations (e.g., the recent DDoS attacks against targets in Estonia) rather than to show off hacking skills. Attackers have become more sophisticated and their attacks more targeted and more difficult to detect. The nature of activities has changed also in the sense that the threats have intensified (e.g., SPAM) and can include malicious code as well as lead to identity theft and commercial espionage.

A majority of respondents also acknowledged that threats to network security have become a global issue and justify the need for enhanced EU and international cooperation and coordination.

Many respondents felt that a main challenge regards awareness raising particularly towards end-users and SMEs who remain the vulnerable point as computer technology advances and by "failing to adopt a security minded approach when making use of ICT services." At the same time, there has been an increased use of and reliance on ICTs and the Internet.

Several respondents noted the following challenges at technical level: tackling vulnerability of important infrastructure, including direct reference to Critical Information Infrastructure Protection (CIIP), security problems arising from the use of emerging technologies, ubiquitous ICTs, change in distribution channels of malware, increased use of P2P networks. The need to improve the level of security in software and then to a lesser extent in hardware was also mentioned by one company and several individual respondents. Whilst it is recognised that new ICT technologies bring many opportunities, they also bring security challenges which will need to be addressed.

Several respondents highlighted that as networks are continuously become more complex and interconnected, new security challenges are arising from convergence of technologies, increased networking, and information sharing. A few respondents also indicated that a security framework would have to face the challenge of properly addressing personal data protection issues.

Most respondents agreed that an agency would still be the right instrument to deal with challenges in network and information security. An Agency has been generally valued for providing information exchange on best practice, a useful platform for dialogue with stakeholders, particularly with industry and coordination with Member States. One specific area in which several respondents thought an Agency could play a particularly useful role was in promoting interoperability of security solutions. However, there were a few responses that put question marks to an agency as the instrument. One Member State response suggested a renewal of ENISA for 2 to 5 years. Another Member State response stressed the need for a cost/benefit analysis that would compare an agency with other entities or ways. A regulatory body suggested that an Agency should have more operational or regulatory responsibilities if it is to have an impact on NIS. An industry association advocated fundamental changes in the existing rules, in particular concerning organizational structure and location, and considered that not extending ENISA would be preferable over the status quo.

2. **How should ENISA adapt its activities to the current requirements of network and information security? What should be changed in the remit of the Agency in order to ensure maximum added value for the EU institutions and Member States? How should the strategic role of the Agency be reflected? How could its profile as an expertise centre providing assistance and advice be clarified? With which activities does the Agency most contribute to the smooth functioning of the internal market?**

Highlights

Most respondents that provided an opinion on the remit, including most Member States that replied, either advocated no changes or only minor changes in the remit of ENISA. The core tasks of ENISA were generally considered to be useful and should continue to be part of its remit. Several respondents indicated that there is room for improvement so that there is more focus and impact of existing tasks. There should be flexibility in the regulation so as to allow ENISA to adapt to new challenges in the security environment.

A majority of respondents foresee ENISA acting as a facilitator to increase cooperation among Member States and help reach a consensus. Some respondents acknowledged the different expertise needs of Member States and suggested that ENISA is well placed to play a 'security evangelism role' for new Member States and reduce the capacity gaps in this field.

Many respondents expected ENISA to continue to provide information on threats and best practices to Member States and establish itself as a respected centre of expertise. In addition, ENISA could facilitate information exchange and provide expert advice to the EU

institutions. It was recommended by several respondents that there should be focus and higher reactivity on providing information and expertise on future trends and needs.

Many respondents supported the task of ENISA to respond to requests for assistance from Member States. A company suggested that ad-hoc requests from Member States and EU institutions should be prioritized and will lead to 'establish ENISA as a natural authority'. Being more approachable and providing information upon request also to end-users (short reports) were also suggested.

Many respondents considered awareness raising and building trust by increasing the level of security as important activities of ENISA, leading to both a better public confidence in using the networks and a decrease in opportunities for criminals. One company proposed ENISA to undertake more specific education and training programmes in the areas where stakeholders, particularly SMEs, lack information and expertise (e.g., risk management). An industry association supported the awareness raising function to include production of content and proposed that ENISA works together with Member State organisations 'to customize material for companies, organisations and individual users.'

Many respondents considered that ENISA should play a network builder role by supporting enhanced dialogue and interaction with stakeholders on network and information society issues. Some respondents referred to ENISA acting as a 'broker and catalyst' and 'enabling' partners to cooperate and develop projects in network security.

Many respondents foresaw that ENISA should develop a more strategic role and provide leadership in establishing a European culture of network and information security. One industry association supported the establishment of a task force to develop high level strategic roadmaps (followed by multi-annual actions plans to assess impact of proposed actions) addressing the most important pan-European security issues and that the Permanent Stakeholders Group (PSG) itself should focus more on strategic planning. Another respondent believed strategic support could be provided for long-term activities such as risk assessment and management.

Some responses pointed out that the activities and results of ENISA should be more recognisable, more focused and create greater impact.

Some respondents believed risk management activities should include incidents analysis, playing a networking and catalyst function to support European actors and risk assessment activities to assist the EU institutions.

Some respondents believed that ENISA could mostly contribute to the internal market by coming closer to EU policy and legislative developments, with one industry association advocating for an 'automatic and mandated participation in legislative debates'. Other respondents mentioned that ENISA should provide a review function for security policy.

A few respondents mentioned the importance of ENISA playing an active role in the international arena through cooperation with third countries on network and information security or participation in standard setting bodies. Other respondents mentioned some other specific activities for ENISA such as fighting SPAM, following data retention policy, developing a recommendation on ISP and establishing security levels.

3. **How can effective interaction between the Agency and its stakeholders be enhanced? In its networking activities, to what networks should the Agency give priority to achieve maximum value? How can the Agency capitalise on the wealth of experience of national bodies and communities of stakeholders in the security environment? How could the results of the work of the Agency be best valorised for both the public and the private sectors thus enhancing the visibility of the Agency?**

Highlights

Most respondents indicated that ENISA should enhance the effectiveness of its interaction with stakeholders by establishing good web-based communication tools and by participating more actively but selectively in workshops and conferences, particularly with industry. ENISA needs to consider how to 'promote' itself more effectively and engage with all relevant stakeholders in order to increase its visibility.

The greatest majority of respondents also emphasised the need for ENISA to engage in dialogue with all the various stakeholders, including academia and research, industry, consumer associations, EU bodies and organisations in the Member States. Some respondents highlighted that ENISA should target SMEs in order to develop its credibility with the wider public. One regulatory body considered that, on the contrary, ENISA should focus on multiplier organisations. Many respondents highlighted the importance of the cooperation with industry, with one respondent suggesting the creation of an 'industry envoy' to assist the Executive Director to liaise with businesses.

Many respondents, including most industry associations and companies highlighted the need for ENISA to undertake greater and more proactive communication, notably by using the ICTs to make ENISA s activities known (use of Web 2.0 features, security mailing lists etc). Some respondents believed that the web should be the place to turn to for information requests and for specialized downloads for dissemination and results of events should be made available for download on the website and published in expert journals and magazines so that its deliverables are given appropriate publicity and marketing. Many respondents also suggested the creation of virtual forums that bring together government, industry, academia and experts to exchange information on particular subjects such as the 'Knowledge Transfer Networks' in the UK or CEDEFOP's 'European Training Village'.

Many respondents recommended that ENISA organises more its own events to extend knowledge to users and other stakeholders and that its staff participates more actively in technical workshops to exchange information with industry and promote best practices. Having a stand at important industry conferences was also proposed.

Several respondents proposed to extend the PSG to public administration and academia or leverage better the PSG membership already by using industry associations to disseminate ENISA's results and engage in further dialogue with their member companies. One respondent believed that the interaction between the different stakeholders and ENISA's PSG and working groups should also be improved and that the working groups should be given more support. Another respondent believed that ENISA could set up working groups to deal

with specific security problems. Alternatively, one PSG member could 'champion' a particular activity with the purpose of linking ENISA with its industry.

Many respondents indicated that ENISA is not sufficiently known to the security community and its activities lack sufficient impact and recognition. There is a need for ENISA to valorise and promote itself better, one Member State suggesting that a marketing plan be undertaken. Alternatively, some industry associations suggested the implementation of a professional public communication plan. Several respondents supported the idea to appoint an 'ENISA ambassador' in order to raise the visibility of ENISA, but one respondent did question what benefits such a position would bring and how it may affect the relationship with the Board and with the Executive Director.

A few respondents mentioned the need for closer relations with the EU institutions and policy making and highlighted location as a main drawback for effective interaction and visibility, therefore proposing the opening of a satellite office in Brussels.

A few respondents considered cooperation with CERTs as an important network that ENISA should be actively working with by exchange of information on security threats, participating in technical workshops or combining PSG/MB meetings with visits to security authorities of the host country.

4. **Without changing the current objectives and scope of the Agency, which additional activities may help the Agency to become more effective, deliver significant added value to Member States and stakeholders and, last but not least, ensure a higher impact?**

Highlights

Several respondents suggested that ENISA should not undertake additional activities. Some specific activities were nevertheless proposed by other respondents. What was mentioned by many respondents was that ENISA would be more effective and have higher impact if it focused on increasing its visibility by playing a leading strategic role and on increasing cooperation with multiplier organisations.

The majority of respondents emphasised that in order for ENISA to be more effective it should play a more strategic role and increase its cooperation with stakeholders for 'multiplier effects' including industry, Member State representatives, vendors and user organisations. Most responding Member States considered that ENISA should have no additional tasks. One Member State suggested that ENISA should improve coordination and standardisation of bridge security notifications.

Many respondents, including most of the individual respondents, noted that ENISA could become more effective if it were to host and participate more actively in different NIS events and engage more in cooperation with CERTS and in the Member States in general. According to several respondents, included one Member State, ENISA should promote coordination of alert systems and early warming system.

Several respondents mentioned that ENISA could be more involved in research activities by cooperating with research institutes, trying to influence research through recommendations on FP initiatives, participation in the European Research Area, ensuring a sufficient framework for cutting-edge information security research in Europe and hosting expert visits and exchange.

Some respondents including many industry associations, however, proposed additional activities such as acting as a 'center of review' for new technologies, providing a 'lessons-learned' service on cyber-attacks and incidents and act as a 'reporting point' to help develop best practice or the collection and review of standardisation processes. One Member State suggested that ENISA should promote collaboration and coordination of certification systems and security standards. Some other specific activities mentioned were to work on identity management, to establish minimum security requirements, to address the software security issue, to define activities with multi-thematic programmes, to establish better linkage between its Work Programme and EU legislation and to promote 'proximity' by increasing computer presence.

5. **Would it be useful and feasible to foresee extended objectives and activities, either more operational or regulatory oriented, for the Agency? What kind of tasks would add significant European value for the Member States or stakeholders? How should in this case the objectives and scope be changed?**

Highlights

A broad majority of respondents agreed that extended objectives, be it operational or regulatory, should not be foreseen for ENISA. A few respondents suggested some areas in which ENISA could develop operational activities.

A large majority of respondents, including most responses from Member States, argued against any extension of objectives and activities, whether more operational or regulatory oriented.

However, a few respondents made concrete suggestions for extended objectives and activities:

With regards to the regulatory aspects, some respondents, including one Member State, suggested that ENISA should have an enhanced regulatory role; several respondents pointed out to the benefits of self-regulation and private–public partnerships. Many respondents linked ENISA's regulatory activities to either providing input to the Commission during the legislative process or in facilitating cooperation between the Member States and the EU institutions.

A few respondents mentioned some operational tasks that could be considered. A regulatory body proposed ENISA to become more operational based on expert capabilities, although it acknowledged that this may be too demanding on a European level. The regulatory body further suggested extending the tasks to the 'third pillar' of the European Union ("Police and

judicial cooperation in criminal matters"). A Member State suggested taking up technical assistance related to third pillar issues. However, another Member State emphasized that ENISA's objectives and tasks should be limited to first pillar issues. Some industry associations proposed operational tasks related to regulation compliancy assessment (but with the actual tasks being subcontracted) and certifications.

A few respondents suggested some specific policy activities to include developing an EU recommendation on baseline security, contributing to the protection of critical information infrastructures, issuing soft law guidance and developing a manual on how regulation impacts information security.

6. What would be the critical mass and the optimum size of the Agency's staff and budget to allow it to act effectively and allow for an appropriate mix of skills and competences?

Highlights

A majority of respondents considered that the future role and tasks of ENISA should be clarified in order to establish the ideal size of ENISA's staff and budget. However, many of the respondents identified the need for the ratio between administrative and operational staff to be revised so as to enhance the impact of ENISA on network security.

The majority of respondents considered that the future role and tasks of ENISA should be clarified before decisions on the optimum size and budget could be taken. Those respondents that did give figures proposed an increase in staff ranging from minimum 50 to 100 persons, as was suggested in the report of the external panel of experts. A majority of the responding Member States argued in favour of having a 'business case' elaborated before a decision on an increase in the current size of ENISA would be made. One Member State proposed to either increase the technical staff or reduce the tasks.

At the same time, many respondents acknowledged that the balance between the administrative and technical staff of ENISA is far from ideal and favoured an increase in technical staff to enhance the impact of ENISA on European network and information security.

Several responses highlighted the need for ENISA to have resources to allow it to strengthen the relations with Member States by detaching or hosting experts. One proposal was the establishment of an in-house experts group to work with stakeholders. Other suggestions included subcontracting of specific tasks, undertaking projects in partnership with the private sector so that resources could be shared and focusing recruitment on technical expertise were also suggested.

A few respondents touched upon the budget issue to suggest that any increase in staff and tasks of ENISA would make a respective increase in the budget necessary.

7. **How could the issues related to the networking and staff retention capabilities as a result of the location of ENISA that have been identified by the external panel of experts be best addressed?**

Highlights
A majority of respondents considered the location as problematic, and a variety of approaches were suggested to overcome the issues identified by the panel of experts report related to enhancing networking capabilities and staff retention. Several respondents advocated the establishment of a satellite office in Brussels. Several others suggested an increased use of ICTs and engaging staff on short-contracts.

The large majority of respondents see the location as problematic for the effectiveness of the Agency, particularly because of travelling and networking difficulties. Relocation of the agency was suggested as a first option by several respondents, either within Greece (Athens) or another more central European country. Many others, however, appreciated political realities and propose a variety of solutions. A few respondents replied that the location in itself was not an issue.

Many respondents including industry associations and companies and some public bodies advocated the establishment of a satellite office in Brussels, a move generally considered to have a positive impact both in terms of enhancing the networking capabilities of ENISA as well as widen the possibilities for high-skilled recruitment.

Several companies and individual respondents focused on how to make ENISA's operation more effective and counteract the challenges posed by its remoteness. There has been wide support expressed both by industry associations, companies and individual respondents for greater use of ICT particularly for video-conferencing and for the use of 'virtual communities' to enhance communication and networking capabilities.

Some contributions to include industry associations and some individual respondents recommended establishing representatives in Member States in order to ensure higher local presence. Alternatively, a change of ENISA model into a new network centric model was proposed by an industry association.

With regards to staff issues, most respondents from academia, companies and some individuals expressed the view that human resources management should allow more attractive conditions and remote working possibilities such as non-permanent arrangements for staff, temporary transfer possibilities, teleworking, short-term visits and traineeships.

LIST OF CONTRIBUTIONS RECEIVED

Member states (4)
-Ministry of science, technology and innovation (Denmark)
-Ministry of transport and communications (Finland)
-Ministry of Enterprise, Energy and Communications (Sweden)
-Ministry of Communications (Italy)

Public bodies (3)
-National regulatory authority FICORA (Finland)
-Research network operators and/or CSIRTS:
  -NIIF CSIRT (Hungary)
  -JNT association trading as Janet (UK)

Consumer association (1)
-Telecom e V (Germany)

Industry associations (6)
-CSIA (Belgium)
-EICTA (Belgium)
-ETNO (Belgium)
-Eurochambres (Belgium)
-Eurosmart (Belgium)
-BSA (Belgium)

Private companies (6)
-BT (UK)
-Magyar Telecom (Hungary)
-Procedimientos-Uno (Spain)
-Telefonica (Spain)
-RSA –EMC (USA)
-Symantec (UK, USA based company)

Private citizens (11):
-Alain De Greve
-Dieter Zoubek
-en Ferran cabrer i Vilagut
-Evangelos Markatos
-J.P. Velders
-Maarten Van Horenbeeck
-Martin Camilleri
-Miguel A. Amutio
-Minna Romppanen, MoF/State IT-unit
-Peter Peters
-Sachar Paulus

Fifteen respondents requested not to publish their names.

ANNEX 11: Public Consultation "Towards a strengthened Network and Information Security policy in Europe" – Summary of contributions

EUROPEAN COMMISSION
Information Society and Media Directorate-General

PUBLIC CONSULTATION

"TOWARDS A STRENGTHENED NETWORK AND INFORMATION SECURITY POLICY IN EUROPE"

SUMMARY REPORT OF THE CONTRIBUTIONS

POLICY CONTEXT

The European Network and Information Security Agency was established in 2004[122] for a period of five years, as a means of contributing to 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. In June 2007, the Commission issued a Communication on the evaluation of ENISA,[123] which included an appraisal of an evaluation conducted by an external group of experts.[124] The evaluation report identified a number of problems, but also indicated positive aspects of the Agency's achievements in the light of the limited means at its disposal.

Since the ENISA Regulation would have expired on 13 March 2009, the Commission, in order to ensure continuity, proposed an interim measure to extend its duration.[125] In September 2008, the European Parliament and the Council adopted a Regulation extending the mandate of ENISA 'à l'identique' until 14 March 2012.[126] The Parliament and the Council also called for "further discussion on the future of ENISA and on the general direction of the European efforts towards an increased network and information security."[127]

On 30 March 2009, the Commission adopted a Communication on Critical Information Infrastructure Protection, entitled "Protecting Europe from large scale cyber attacks and disruptions: enhancing preparedness, security and resilience." The general objective of this policy initiative is to enhance the level of awareness and preparedness across the EU and to

[122] Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 established the European Network and Information Security Agency (ENISA), OJ L 077 of 13 March 2004.

[123] Communication from the Commission to the European Parliament and the Council on the evaluation of the European Network and Information Security Agency (ENISA)**,**COM/2007/285.

[124] http://ec.europa.eu/dgs/information_society/evaluation/studies/s2006_enisa/docs/final_report.pdf

[125] Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration, COM(2007) 861.

[126] 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.

[127] See Recital 5.

ensure security and resilience of Critical Information Infrastructures as the frontline of defence against cyber attacks and disruptions.

Given the changing landscape of security challenges, the possible policy priorities and objectives to deal with these evolving challenges, as well as the instruments and mechanisms needed for a strengthened network and information security policy at EU level have to be re-defined. In September, last year, Commissioner Viviane Reding called on the European Parliament and the Council to open 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.[128]
In order to facilitate the debate on the future of network and information security (NIS), the Commission services organised this on-line public consultation on the future of network and information security.

CONTRIBUTIONS TO THE CONSULTATION

The public consultation was launched on 7 November 2008 and ran through 9 January 2009. It was available on-line at the 'Europa' website (ec.europa.eu) of the European Commission.

We received 596 contributions to the public consultation: 12 from government and public bodies, 4 from industry associations, 29 from individual companies, 4 from academic institutions, 7 from other organisations, and 540 from individual citizens.

Over three quarters of all contributions received were from individual citizens with addresses in Crete and elsewhere in Greece that replied only to the question of an Agency as a policy instrument (question 8). Most of these replies gave exactly the same formulation in favour of an indefinite mandate for ENISA and an increase of its resources.

SUMMARY OF THE CONTRIBUTIONS

1. **Electronic networks and services constitute the nervous system of our society and the economy, and recent large scale cross-border cyber attacks, for example in Estonia, have highlighted our dependence on them. In this context, what are the major challenges for network and information security to be considered at the national, EU and international level, in particular with regard to resilience of electronic communication networks and information infrastructures?**

Highlights

The threat landscape has been continuously evolving and challenges have changed in nature and increased in complexity. Attacks have become more targeted and more difficult to detect. Cyber attacks, in particular, have become more organised and sophisticated. They are either conducted to achieve financial gains or are

[128] Intervention during the Plenary Session of European Parliament on 2 September 2008.

politically motivated.

Increased use of networks, emerging technologies, and the need to improve the level of security of hardware and software pose further challenges. In addition, the globalisation of threats and the global interdependencies have magnified a need for enhanced international cooperation and coordination.

A security framework needs to face the challenge of properly addressing personal data protection issues and civil liberties, especially with the emerging dominance of mobility in inter-personal communication and data handling.

A further challenge will be the development of common, internationally applicable security standards and regulations.

The majority of respondents, including three Member States, a government agency, four private companies and two industry associations, stated that **cyber-threats are a major challenge that would need to be addressed.** In general, it was recognised that attackers have become more sophisticated and their attacks more targeted and more difficult to detect. It was generally acknowledged that cyber attacks are either politically or financially motivated, the latter organised by criminal gangs, involving identity theft, phishing attacks, spam as well as the dissemination and use of botnets and other malicious codes or unsolicited software.

A number of respondents, including a Member State and an industry association, expressed the view that a security **framework would have to face the challenge of properly addressing personal data protection issues and civil liberties, especially with the emerging dominance of mobility in inter-personal communication and data handling.** The need **to uphold and enforce the rule of law** on the net was considered necessary by an academic institution, so that the state could regain its "**digital sovereignty.**" The latter point was also shared by a Member State.

Many respondents, most of which are private companies and an industry association, pointed out that the major challenge **would be the development of common, internationally applicable security standards and regulations**. The cross border **interdependence** of networks today invariably **involved links to insecure networks abroad**. A majority of respondents, including a national regulator and a government agency as well as three private companies, also acknowledged that **threats to network security had become a global** issue and justified the need for enhanced EU and international cooperation and coordination to **harmonise security legislation and standards, to facilitate the exchange of information, and to conduct joint exercises.**

Several respondents noted the following **challenges at technical level**: **security problems arising from the use of emerging technologies and ubiquitous ICTs, the need to improve the level of security in software and in hardware, a lack of minimum standards, the protection of the physical infrastructure such as deep sea cables.** Several respondents highlighted that as networks were continuously becoming more **complex and interconnected**, security risks were becoming increasingly difficult to identify.

A sizable amount of respondents, including a government agency and an industry association, noted that in the competitive telecoms market economic considerations would take precedent over security concerns when designing, producing and implementing new hard- and software. Also, **new security challenges are arising from the continued convergence of technologies, from networking, and from information sharing among users.** At the same time the respondents expressed concern about the rising costs that an increase in security would entail.

A few respondents, including a Member State body, commented on **the lack of skilled personnel** in the respective entities, as well as a lack of expertise and research in the security field in general. It was also felt by some respondents, amongst others two Member State bodies, that there was a lack of understanding of the implications of NIS and that there was a **low security awareness** of end-users, including small and medium enterprises (SMEs), despite the fact that they were increasingly relying on computer technology and internet applications which were continuously evolving. This reliance includes access to eGovernment services.

2. Given the importance of electronic networks and services for society and the economy, what should be the three key priorities for policy to address the evolving challenges to network and information security at the EU and the international level?

Highlights

The establishment of public-private partnerships is a necessary and helpful way to disseminate information, to share best practices and can act as a forum for cooperation to reach common standards within the EU and beyond. The creation of a baseline standard on security should be considered, with involvement of hardware and software producers. Given the international nature of the network connections, extending and aligning the activities in international fora is of high importance.

Data protection is a key priority to be addressed. Data retention policies as well as on line criminal activities, reaching from spam to identity theft, expose users to abuse.

When working on regulation, we should use 'principle' rather than 'rule-based' legislation and regulation.

A very high proportion of respondents, in particular some private companies, two NGOs and many citizens, identified data protection issues as being on of the major challenges which needed to be addressed. Some of these respondents suggested in this context that legislation would be introduced and proposed that a body is set up to target entities engaged in criminal activities on the web to re-establish trust in the security in the networks with users. An NGO also suggested reviewing requirements for data retention for law enforcement or consumer protection to **minimise the unnecessary and avoidable risks to data protection.**

A large proportion of respondents, including two Member States and two industry associations, saw developing legislation as another priority in order to achieve network security. A regulator pointed out that this should best be done **by using principle -,** rather than rule-based legislation and regulation.

Two Member States and a government agency as well as five private companies and an industry association suggested that the development of public-private partnerships would be a priority to exchange best practices, to discuss and facilitate NIS, and to help develop resilient, sustainable and secure infrastructure and services, thereby **creating a knowledgeable and proactive NIS community throughout the EU and beyond.**

A certain amount of respondents, a Member State, a private company and an industry association, also suggested that a common security baseline standard or a minimum framework of common capabilities would be developed. **A citizen even suggested a European Code of Good Security Practices.** These discussions would also need to include the producers of software and hardware. A certification of people, processes and products in the field of security should be considered. In general, more funding for research projects on security issues should be made available by the EU, a Member State and an academic institution suggested.

A number of respondents, involving two Member States, a government agency and three companies, considered **awareness raising of users to be a necessity in order to enhance network security.** One service provider explicitly mentioned child protection issues.

Some respondents, including a regulatory body, suggested that it **would be of high importance to extend and align the activities currently pursued in different international fora** due to the international nature of the network connections.

On a more **technical side**, the following suggestions were made: promoting "**secure-by-design**" infrastructures; by developing **metric and observation mechanisms** for assessing and proving security and dependability of complex systems; to implement **electronic signature** allowing secure but anonymous navigation of the internet; **enhancing identity management** technologies; the development of **intelligent context reasoning** components for the purpose of security and identification; the **establishment of Next-Generation-Networks;** use of open-source standards; create a repository about incidents and their resolution; **CERTs across the EU**.

Some respondents, including a private company, suggested that in addition to regulation, **financial incentives** are a helpful component to promote security issues. **This could include assisting Member States who need financial and technical support to reach an EU wide security standard.**

A large number of individual citizens expressed the need for access to networks, irrespective of personal income or remoteness of location, as well as access to technical support possibilities. Ensuring the availability of networks was also frequently mentioned.

3. **Member States have a key role and overall responsibility in guaranteeing the security and continuity of critical services for citizens and businesses. In this context, what should be the focus of future EU policy in order to**
   a. **enhance cooperation at the EU level between national competent bodies; and**
   b. **achieve a holistic, all-encompassing approach to network and information security;**
   c. **reinforce the synergy between measures focusing on prevention and resilience ("first pillar") and measures supporting judicial and law enforcement cooperation ("third pillar")?**

Highlights

Cooperation at EU level
The exchange of information between the competent bodies of the Member States should be facilitated. Relationships of mutual trust and public-private partnerships should be built. An EU-wide early warning mechanism should be established.

Holistic approach
Member States should identify the potential threats, strengths and weaknesses of their critical infrastructures. ENISA can act as a platform for information exchange and increased cooperation between organisations fighting spam. There is a continuing need for training, awareness rising of all stakeholders, and (funding of) research on security issues. It is necessary to find a trade-off between security and cost for businesses. We need to work towards clearer, harmonised rules and a reduction of the compliance burden.

Synergies
Synergy between pillar one and pillar three activities is essential. Cyber analysis capabilities should be available for law enforcement purposes.

Future EU policy to enhance cooperation at EU level

Many respondents, including two Member State bodies, stated a need to facilitate the exchange of information between the competent bodies of the different Member States, as well as international bodies, **to achieve a minimum functional capability** within the EU. A Member State suggested that in this case ENISA could act as focal point of communication. One private company stated that ENISA should be the only EU entity involved in this respect.

Several respondents, including an industry association, were of the opinion that a European Public-Private Dialogue and **Cooperation and voluntary measures were the appropriate means to achieve a minimum functional capability within the EU.** One industry association in particular pointed out that it was necessary to build up **mutual understanding amongst the stakeholders involved, as mistrust and misunderstanding were hampering cooperation.** A private company suggested that the Member States are hesitant to let go of an area which ties in with national security and which they formerly controlled.

An industry association and a private company suggested that the cooperation could be enhanced by establishing an **institutional early warning system at European and Member State level that would jointly** allow the handling of serious threats, be they local or global.

Future EU policy to achieve a holistic approach to network and information security

A large number of respondents, including three private companies and an industry association, were of the opinion that training and awareness raising measures amongst all stakeholders were necessary. A private company remarked in particular that the business sector needs to be involved to clarifying its rights and obligations.

Two Member States, a private company and an academic institution, felt that there is a need for increased professionalism and research in information security. This should include, according to a private company and an industry association, the development of new technologies to help build a proactive framework for advancing cyber security.

Further, a private company and an industry association felt that it should be ensured that Member States have identified the potential threats as well as the strengths and weaknesses of their critical infrastructures. An industry association suggested the creation of an **EU organisation mandated with developing resilience policies and coordinating responses to attacks on information infrastructures.** A Member State believed that ENISA could act as a platform for information exchange and increased cooperation between organisations fighting spam. It was also remarked by a Member State, a private company and an industry association, among other, that there is a need to **harmonise the different policies governing security and continuity of service issues.** A citizen believed that a code of good practices should be drafted to which the service providers in Europe were forced to adhere to.

Other respondents, including an industry association, added that a trade-off between security and cost needed to be found. In this context clearer rules and a reduction of the compliance burden for business are considered helpful. One service provider pointed out that, given the fragmentation and inhomogeneous approach to critical national infrastructure protection across the EU, a **common reporting procedure for operators that are engaged in different Member States would be welcomed.**

A private company and an industry association suggested to develop **a "common capabilities framework" (i.e. public-private partnerships), would contribute to improving the operational resilience.**

On a more technical and programmatic level, respondents made the following suggestions: to define a level of assurance (STORK project); align legislative issues related to the use of national ID tokens and related identity attributes across Europe; **create a framework for security labels or certification levels of products and services to ensure better transparency of the usage of the network;** support of the ITU-T Recommendation X.1250, Capabilities for enhanced global **identity management**, trust and interoperability; compliance with common international security standards such as ISO/IEC 27001; develop traceability means of information to avoid criminal usage of the network; establish "Secure-by-Design Infrastructures Framework;" defining minimal set of standards to use and effectiveness of metrics; creating a specific program "European Network and Infrastructure Information and

Security Assurance Partnership;" the burden of security precautions should not be on the end user; decentralisation of security, counter-attack and telecom infrastructures.

One organisation suggested that instead of addressing network security by using a vertical approach by Member State, a horizontal approach along industry sector lines, such as finance, legal, medical, etc., is more promising, as the industry sectors are affected by the same issues, irrespective of the Member State that they are located in.

A citizen suggested starting an open dialogue with all citizens, promoting the value of e-services and proving that it is possible to improve societal rights via the appropriate use of ICT.

Future EU policy to reinforce synergies between "first" and "third pillar" measures

A large number of respondents, including two Member States, four private companies and two industry associations, see a synergy between pillar one and pillar three in the fight against cyber crime, the protection of intellectual property rights and the protection of information security, in particular on an operational level. Some citizens suggested the creation of an agency that enables the reporting and investigation of cyber crimes. A private company favoured a closer co-ordination of law enforcement agencies across the EU to speed up the judicial process. Further, a private company and an industry association suggested the advancement of cyber analysis capabilities for national and EU response teams to identify and mitigate attacks which could then assist law enforcement officials.

However, one Member State agency remarked that a clear distinction between first and third pillar activities should in principle be maintained, but which would be reassessed on a case by case basis. Related activities should rather be bundled in a common EU strategy, such as post-"i2010."

A small number of respondents, including a Member State and an academic institution, pointed out that work and research should be conducted towards identifying new paradigms that allow the application of different or special jurisdictions in IT related cases. Some citizens also pointed out that the training of judges and lawyers in IT related fields would be beneficial for law enforcement purposes. A Member State made the case to regain the manageability and the control over illegal use of the internet.

A few respondents, from an academic institution, pointed out that also second pillar issues (common foreign and security policy) have an important role to play and that without a common defence policy a real cooperation in security matters, including ICT, will not take place. Available mechanisms under the second pillar should be utilised to set up further cooperation.

On a more technical level, respondents made the following suggestions: standardisation of the conditions for processing information for identification and tracking; better cooperation of law enforcement agencies within the EU and internationally, in line with the Council of Europe, Convention on Cyber Crime, 2001; removing 'data paradises' out of the EU.

4. **The security and resilience of the Internet is a joint responsibility of all stakeholders, including operators, service providers, hardware and software providers, end-users, public bodies and national governments. This responsibility is shared across**

geographical boundaries, in particular when responding to large-scale cyber attacks. In this context, what role should the EU play to strengthen the preparedness of the key stakeholders?

Highlights

There should be closer cooperation amongst the stakeholders concerned, supported by ENISA. We need more common, harmonised standards across the EU. Exchange of good practices, exercises and awareness raising programs are necessary for all stakeholders. We should not forget to address possible physical disruptions, especially between continents, caused by undersea cable cuts, natural disasters or human error.

Many respondents, among other two Member States, an industry association and six private companies, expressed the wish for **closer cooperation amongst all the stakeholders**, utilising ENISA in that regard, to reach a common understanding, generally applicable guidelines, streamlined policies and procedures, generally accepted minimum standards and, ultimately, the creation of a common (capabilities) framework throughout the EU. Likewise, many respondents, including a government agency and two private companies, pointed to the need of CERTs throughout Europe. Another organisation even noted the need for an EU CERT.

A large number of respondents, including four Member States, a government agency and four private companies, felt that the exchange of **good practices, exercises and awareness raising** programs for all stakeholders are necessary. More specifically, an industry association and a service provider called for the introduction of a security certification program for security experts.

A Member State and an industry association also stressed the importance of **addressing possible physical disruptions**, especially between continents, caused by undersea cable cuts, natural disasters or human error. Mitigating such incidents and restoring operations requires trusted and tested response plans.

Another industry association argued that funding is necessary to enable critical infrastructure sectors to improve security where the business case for implementing necessary security measures is inadequate. Likewise, an academic institution argued that the EU should support more studies looking into virtual infrastructures.

On a more technical level, respondents made the following suggestions: to analyse DDOS attacks and what resources the Member States can bring to bear to counter such attacks; engaging in a policy which focuses on the physical and logical protection of interconnection points and the security of the domain name system; to take into account ITU-T References X.805, 1051 and 1121 as well and ISO/IEC 27002 as well as to promote the adoption of common, standards based, auditable technical approach standards when addressing security and resilience of the internet and other ICT networks based on the internet protocol; to offer a framework of trust which, when applied, ensures reasonable security; understanding the internet exchange and the peering contracts as digital EU frontiers which require a

requirements framework for international connections to ultimately regulate the functional properties and the allowed exchanges; a decentralisation of data storage, since large server pools are usually the targets of cyber attacks; to promote the use of open source solutions which are less vulnerable to attacks as commercial products seem to be; to promote the use of a "stripped down" open source solution thereby focusing on a limited set of services, thus limiting the exposure to attacks.

5. **Because of the global nature of the Internet, each and every country has a degree of inter-dependence with other countries, not least when responding to large-scale cyber attacks. How can we support trans-national cooperation in the EU to cope with evolving network and information security challenges?**

Highlights

Trans-national cooperation is important in order to respond to large scale attacks. Cross-border cooperation can be supported by promoting information exchange, dissemination of best practices and building trust among stakeholders. The EU should support the establishment and /or reinforcement of national CERTs.

Most respondents acknowledged that the **EU has a role to play to support trans-national cooperation.** One Member State highlighted the fact that such cooperation is particularly useful in order to enhance the ability to detect the attacks at their source.

Many respondents believed that **exchange of information and of best practices** could be useful for a better understanding of vulnerabilities etc., and should be promoted. One Member State authority argued that there is a case for promoting good practice in developing national capability to identify and protect critical services.

Some respondents representing an industry association and private companies suggested that the Commission, in collaboration with stakeholders, should **define common cyber security best practices** and should **stimulate new technologies** (e.g. that improve awareness and response capabilities) and, in order to do so, should establish a trusted community of experts to facilitate the process in their respective organisations.

Many respondents considered that the Commission should promote the **establishment and/or reinforcement of CERTs** in order to improve the readiness of the EU. At the same time, respondents noted that a CERT organisation might be established at European level to help coordinate the activities of Member States, in particular when responding to large scale attacks which affect several countries. Some respondents mentioned that ENISA could assist in these efforts.

Several respondents highlighted **building trust** as a key aspect of providing support to cross border cooperation. In response to the question on how to support trans-national cooperation in the EU to cope with evolving network and information security challenges, other suggestions include: facilitating and promoting exercises as well as other common

preparedness projects, promoting research and development, promoting awareness raising among stakeholders and encouraging use of standards.

Some respondents considered that the EU should encourage trans-national cooperation using current foras and specifically in international foras such as the UN, OECD etc. Some other respondents noted that the EU should be involved in global cooperation to fight illegal activities against networks and services.

Some specific proposals made by an industry association and a private company referred to: identifying the critical communication nodes and components to enable replication and capacity of alternative routings, establishing levels that allow effective traffic controls in a coordinated way on the operational side and, on the organisational aspects, developing an European security certification programme which would provide harmonised training and recognition of security experts within the EU.

More suggestions: developing continuity plans, facilitating the import/export of commercial security products, facilitating cooperation in the management of risk and studying the interdependencies between networks and services and creating a European data base of security incidents.

6. What instruments are needed at EU level to tackle the challenges and support the policy priorities in the field of network and information security? In particular, what instruments or mechanisms are needed to enhance preparedness to handle large scale cyber disruptions and to ensure high levels of security and resilience of electronic networks and infrastructures?

Highlights

There should be more coordination of responses to cyber threats through ENISA or another EU-level body. In order to achieve a more homogeneous approach to NIS, a set of minimum standards for security should be adopted across Europe. We need more activities aimed at awareness raising in cybersecurity.

The majority of respondents believed that there should be a more coordinated response to cyber threats. Ways to achieve such result are to improve information sharing among Member States, among national CERTs. There should be an EU-level Coordination body (some respondents pointed at ENISA or at the EU institutions) that would issue guidelines and best practices to help find a common methodology to counter cyber threats.

Along the same lines, many respondents identified such a coordination body acting as a centre of excellence where data on NIS could be found and kept updated for Member States and relevant stakeholders, and where research could be carried out, such as in the area of cross-boarder risk assessment, impacts and points of failure.

Three Member State bodies and another significant group of respondents stressed the importance of having a set of minimum security standards at the European level in order to attain a more homogenous approach to NIS both from Member States and private parties.

Some proposed a step further in setting security standards; notably they recommended that hardware and software manufacturers should issue products compliant with security standards, "secure by design," with the advantage of putting into the market resilient devices. However, it was also acknowledged that such an approach could be too burdensome for vendors in economic terms and it could not be done without some financial support.

Several respondents, including three Member State bodies, called for an EU level NIS strategy and a common Action Plan which would help to coordinate Member States' policies in the sector and make them more effective.

Finally, the majority of respondents agreed that there should be more activities aiming at raising awareness in the field of cyber-security, and some respondents called for more R&D in order to improve the technology for the quality and resilience of networks.

7. A strong and effective European incident response capability could be a key element of ensuring fast responses to cyber attacks and speedy recovery from disruptions. Building upon initiatives at national level, what EU instruments or actions could be considered to reinforce incident response capability?

Highlights

European incident response capability should be built through national CERTs. In addition, there is scope for a European incident response capability.

A majority of respondents considered that **existing national structures should be reinforced**: European incident response capability should be built through national CERTs, but that **there is a role to be played by the EU in ensuring and facilitating cooperation** between them. Such a role could include facilitating information sharing and exchange, dissemination of best practice, facilitating and promoting exercise and training in order to improve Member State capabilities and encouraging the establishment of CERTs where needed. Two Member States specifically noted that they do not see the necessity of a common European incident response capability.

However, many respondents, including industry associations and private companies but also one Member State authority considered that a European incident response body would be useful. Some respondents noted that its role should include to coordinate response teams at Member State level, to intervene in the case of serious threats of a trans-border nature (serious cyber attacks) and response and recovery operations at EU level, to provide incident mitigation advice, to provide a framework or criteria for what constitutes incidents of significance or to define security and resilience postures and response actions. Some specific services were suggested by one Member State: to collect monitoring information and to

deliver updates to national incident response capabilities. ENISA was mentioned several times as the right body through which to establish such coordination.

A third option was mentioned by a private citizen which suggested the creation of an EU industry driven cooperation body, whilst one Member State suggested that the EU institutions should create their own body to deal with cyber attacks.

Other suggestions included the creation of a joint NATO-Europol-industry incident response network or generally more coordination with other organisations (such as Eurojust, OLAF etc).

8. Given the evolving network and information security challenges, is an Agency still the right instrument to "enhance the capability of the Community, the Member States and, as a consequence, the business community to prevent, address and respond to network and information security problems"? If yes, what should be the mandate and the size of such an Agency to successfully meet this objective? If no, what are the alternatives that should be considered?

Highlights

ENISA is perceived by most respondents as being the right instrument. Other respondents have no preference for an agency as policy instrument or consider ENISA not the right instrument and propose alternatives.

The Agency should focus in particular on its facilitating and advisory roles, and should act as a centre of excellence.

The substantial number of replies **only to this question** reflected strong Greek support for ENISA (which includes the majority of contributions of private citizens, many Greek companies and even several contributions from private citizens that were submitted by Greeks from other EU and non-EU countries).

Therefore, to the question of whether an Agency is still the right instrument to enhance the capability of the Community, Member States and business community to prevent, address and respond to network and information security problems, a vast majority of respondents, notably of Greek origin, replied positively. Among these, many argued that ENISA should have an **indefinite mandate and increased resources**.

The contribution from ENISA itself supported the recommendations proposed in the IDC evaluation report[129] which foresaw: an increase in the Agency's size and resources and that the Regulation of the Agency should be revised, to reflect the Agency's strategic role and to clear ambiguities about its profile as a centre of expertise and advice.

A small number of respondents nevertheless thought that ENISA would not be the right instrument. Alternatives proposed include a joint incident response operation, or a steering committee of representatives of national bodies with decision powers for common policies, or a global agency (considered better than a regional one). A private company proposed the set up of a separate organisation to deal with resilience policy.

A few respondents, including three Member States, noted not to be particularly attached to the agency format as such, but that the emphasis should be put on the competences and efficiency of the instrument chosen.

As regards the mandate, a majority of respondents considered that ENISA's **advisory and facilitator roles** as well as being a **centre of excellence and expertise** and collecting best practices, should be maintained.

In addition, some respondents could foresee a role for ENISA in the **coordination of responses to large scale attacks**, and two Member States were against operational activities.

Some respondents mentioned that ENISA could be more involved in the development of security standards. Other suggestions included: improving connections between policies and R &D and technical standards and cooperation with services of other regions.

One Member State authority foresaw an important role to be played by ENISA in two areas: fighting SPAM and improving cyber-security (e.g. facilitating information sharing, building bridges between cyber security and cybercrime, advisory role on relevant regulations, and drafting best practice).

As regards the question on size, a majority of respondents in favour of the Agency also asked for an increase in its size and resources. Some respondents commented that the size should be established depending on the activities and projects that will have to be undertaken. A few respondents also mentioned the imbalance between the administrative and technical staff.

A few respondents, including one Member State authority, mentioned that the agency should be stationed in a location easier to reach.

9. Given the shared responsibility of stakeholders for Internet security and resilience, what are the most appropriate instruments to foster international dialogue and cooperation? In particular, what instruments are required to nurture cross-border public-private partnerships to ensure the good functioning of today's electronic networks and infrastructures?

Highlights

Public-private partnerships are key elements to promote dialogue among stakeholders. In this context, some believe that existing instruments are sufficient, while others argue the need for a debate to identify the responsibilities of each stakeholder. Building trust and identifying the right stakeholders are important

elements in establishing effective public-private partnerships.

A majority of respondents considered that **public-private partnerships** are key to promote dialogue among stakeholders and many respondents, including two Member States authorities, said that existing foras are sufficient (no need for a further instrument was foreseen).

Another block of respondents thought that current instruments are not enough, one Member State arguing that more analysis was needed in order to determine the right means, whilst another Member State authority and other respondents considered that there is the need to create a specific exchange platform. Several private companies advocated the idea to organise an international conference in order to launch a comprehensive debate to identify each stakeholder's responsibility. The need to create a common framework in which these various roles would be clarified was also mentioned.

Several respondents, including two Member States authorities, considered that **building trust** was a very necessary ingredient, and, to this aim, highlighted the **importance of identifying the right stakeholders** to be engaged.

Some respondents from industry associations and private companies also thought that clarity of purpose, focus on outcomes and broader engagement (stronger links to international organisations, undertaking dialogue with corresponding bodies in the US, China, Russia and other regions) are important elements in order to foster effective international dialogue and cooperation. Some respondents noted that ENISA could play an active role in coordinating international dialogue and cooperation.

Some respondents considered the need to provide solutions for the co-financing/ financing by Member States of projects, whilst others highlighted the need to develop financial incentives in order to involve the private sector more.

Some other proposals included elaborating international recommendations (e.g. data protection) and setting up an international convention in which the participants concede to the UN a mandate to globally address the main issues related to network and information security.

ANNEX 12: FINDINGS AND RECOMMENDATIONS OF THE EVALUATION OF THE EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY (COM (2007) 285 FINAL)

Part 4 and 5 of COM(2007)285 final

4. Findings and recommendations of the external evaluation

4.1. Key findings of the Evaluation Panel

The evaluation report of the external panel of experts[130] confirms the validity of the original policy rationale behind the creation of ENISA and its original goals. All the main stakeholders share this idea. Furthermore, the Agency's activities are in line with its work programme, and its achievements are adequate or even good so far.

However, the Agency's activities appear insufficient to achieve the high level of impacts and value added hoped for, and its visibility is below expectations. There are a number of problems that affect the ability of the Agency to perform at its best: they concern its organisational structure, the skills mix and the size of its operational staff, the remote location, and the lack of focus on impacts rather than on deliverables. Many of these problems have roots in the ambiguities or the choices of the original Regulation, and the chances for a successful future for ENISA depend on a renewed political agreement among the Member States, built on the lessons learned and the achievement of the first phase of the Agency.

It should be emphasised that the evaluation has been carried out after the Agency had only been operational for a year. The potential contribution of the Agency for the functioning of the internal market is appreciated by the stakeholders and expected to grow, especially concerning the reduction of the duplication of activities in the NIS field between the MS and the Commission and the harmonisation of policy and regulations.

According to the opinion of most stakeholders, closing the Agency when the mandate expires in 2009 would represent a significant missed opportunity for Europe, and would have negative consequences for network and information security and the smooth functioning of the internal market. On the other hand, they also believe that change is needed in the Agency's strategic direction and structure.

'SWOT' table from the Evaluation Report of the external panel of experts, p. 72	
STRENGTHS	**WEAKNESSES**
• Member States and Commission Mandate • Good start in building relationships • Staff competence	• Lack of vision, focus and flexibility • Uneasy relationship between Management Board and Agency • Location problem for recruitment and networking • Lack of critical mass of the operational staff • Early phase of learning curve

[130] The report is available at the following website: http://ec.europa.eu/dgs/information_society/evaluation/studies/index_en.htm

OPPORTUNITIES	THREATS
• Increasing importance of security in the EU • Unique position to respond to security coordination needs • Global alliances look for EU counterpart • Launching new projects with high relevance in the security field • Becoming a reference point for all the MS	• If effectiveness is not improved, rapid weakening and loss of reputation • High turnover is weakening the staff • Contradictory expectations from MS and between MS and stakeholders • Misperception of role and goals by external stakeholders

4.2. Recommendations of the Evaluation Panel

In addition to the findings and the analysis of the data collected, the report of the evaluation panel contains some recommendations on the future of ENISA after 2009 briefly summarised in the following:

- The mandate of the Agency should be extended after 2009, maintaining its original main objectives and policy rationale, but taking into account the current experience.

- The Regulation of the Agency should be revised, to reflect ENISA's original strategic role and to clear ambiguities about its profile. The Regulation should not define in detail the operational tasks of the Agency to allow for flexibility in adapting to the evolution of the security environment.

- The Agency's size and resources should be increased (up to 100 persons approximately) in order to reach the necessary critical mass.

- The role of the Management Board should be revised in order to improve the governance of ENISA.

- The appointment of a high-profile figure, well recognised in the NIS environment, who could act as an ambassador, could help increase ENISA's visibility.

- The Panel also makes recommendations regarding the location of the Agency in Heraklion.[131]

Finally, the evaluation panel recommends a number of short terms actions to improve the performance of ENISA. The Commission has invited the Management Board and the Executive Director of ENISA to duly consider these short-term recommendations and to take the necessary steps.

[131] It should be recalled that the seat has been established by decisions of the Heads of State and Government and of the Greek Government.

5. Appraisal of the results of the external evaluation

The evaluation of the external panel of experts has produced many valuable findings on specific aspects that are critical for both the good functioning of ENISA and its impact on the situation of network and information security, in particular its internal market dimension. The Commission largely agrees with these findings that, altogether, highlight the validity of the original policy rationale and goals but underline also how the current size of the Agency and the organisation of its work do not appear to be adequate for its future challenges.

There is a valuable lesson to be learnt, as a number of important difficulties encountered by ENISA seem to be of a structural nature stemming from ambiguity in the interpretation of its Regulation and the suboptimal level of human resources available to the Agency. The misalignment between the interpretation of the Regulation by the Agency staff and by the Management Board may have additional causes that hinge on the lack of a shared vision of ENISA among the Member States. The evaluation report is, in this respect, very clear and highlights the diverse needs of Member States concerning network and information security. The enlargement to 25 countries on 1 May 2004 (and to 27 on 1 January 2007) has exposed ENISA and its operation to higher expectations and demands than those that had been anticipated when the agency was established.

The advent and convergence of more sophisticated and advanced communication and wireless technologies together with the fast evolving nature of threats have also contributed to transform the environment in which ENISA operates. The potential impact of these developments on the network and information security challenges for the EU has been highlighted by the Commission in its Communication on a strategy for a secure Information Society.[132] It is important to take these developments in due consideration when reflecting on the future of ENISA and deciding how the EU member States and stakeholders should cooperate to cope with new challenges for network and information security.

A key finding of the evaluation report is the importance for ENISA to enhance contacts and working relations with stakeholders and Member States centres of expertise. In particular, the lack of regular and effective networking activities with the existing European scientific, technical and industrial communities and sectors is considered as a main impediment for ENISA to position itself in this area and exercise its role as defined in its Regulation. According to the report of the external panel of experts, the current location is, in this regard, not helping ENISA as it makes it more difficult to establish regular and continuous working contacts with scientific, technical and industrial communities and sectors as well as to attract and keep key domain experts who may have the profile and personality to establish these contacts. Similar arguments hold for what concerns the working relations and contacts with Member States laboratories and/or technical centres.

6. Recommendations of the ENISA Management Board

At the meetings of the ENISA Management Board on 26 January 2007 in Brussels and 22-23 March 2007 in Heraklion, the Commission reported on the evaluation and the Management Board discussed the report of the external experts. On 23 March, the Management Board

---

132 COM(2006) 251, 31.5.2006.

formulated recommendations on the future of the Agency and on changes to the ENISA Regulation.[133]

Recommendations of the ENISA Management Board:

The Regulation should be revised to extend the mandate. That mandate should again have a review point.

1. The scope of Agency should not be materially changed.

2. The Regulation should be revised to combine Articles 2 and 3[134] to set outcome-based key objectives that are realistic and within the scope of the Agency.

3. The Agency should maintain the capability to respond to specific requests for advice and assistance but the nature of these requests and the process for receiving and considering them should be more clearly stated in the Regulation.

4. The governance structure of a Management Board, Executive Director and Permanent Stakeholders' Group should not be changed.

5. The Executive Director should be required to appoint – in consultation with the Management Board - a stakeholder to chair the Permanent Stakeholders' Group. In addition to its role in relation to the Work Programme, the Group should be more clearly tasked to contribute to the two way flow of ideas between the Agency (both Board and Executive Director) and the stakeholder community as well as encouraging the commitment of resource by the stakeholder community in support of the Agency's aims.

[133] As foreseen in article 25 of the ENISA Regulation. The full text of the document adopted by the ENISA Management Board, which also contains the Boards considerations, is available at the following website: http://enisa.europa.eu/pages/03_02.htm

[134] On, respectively, Objectives and Tasks.