EUROPEAN COMMISSION

Brussels, 30.9.2010
SEC(2010) 1127

COMMISSION STAFF WORKING DOCUMENT

SUMMARY OF THE 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) 1126}

SUMMARY OF THE IMPACT ASSESSMENT

1. SCOPE AND CONTEXT

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 necessary policy instrument to deal with NIS challenges, should best be shaped to support Member State bodies and the Commission in achieving NIS policy objectives, when the mandate of the European Network and Information Security Agency (ENISA) expires in March 2012.

1.2. Context

In today's world, society and economy rely critically on the proper functioning of information and communication technologies (ICTs). It is therefore of paramount importance to ensure both that the systems are stable and that users trust them. The increasing number of threats, attacks and malware used against systems could put at risk the proper functioning of basic network and information infrastructure. Given that these systems and networks are transnational, a European answer to the challenge of network and information security (NIS) is needed.

To address these issues, the European Network and Information Security Agency (ENISA) was set up in 2004[1] for a period of five years to '*ensure 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'*.

Since then, NIS challenges have been constantly changing in line with technological and market developments. Therefore, well before the expiry of the ENISA Regulation in March 2009, the Commission started a process of determining with relevant stakeholders what policy proposals would best serve the EU's NIS objectives from 2009 onwards. Following a 2007 mid-term evaluation[2] of ENISA and a public consultation[3], on 24 September 2008 the Council and the European Parliament adopted a Regulation extending ENISA's mandate, as it stood, by three years, to 13 March 2012[4]. In the recitals to this 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***'.

---

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 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, 1.6.2007, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007DC0285:EN:NOT.

3 The consultation ran from 13 June to 7 September 2007.

4 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, 31.10.2008).

The Commission facilitated the discussion by launching a further EU-wide public consultation, in November 2008, on the possible objectives of a strengthened NIS policy and the means of achieving those objectives[5]. The Commission also held a workshop with experts in NIS from the competent bodies in the Member States, in December 2008, on the instruments and mechanisms of a strengthened EU policy on NIS. In addition, in March 2009, the Commission adopted a Communication on Critical Information Infrastructure Protection (CIIP)[6] which sets out a key role for ENISA in supporting the EU to enhance security, resilience and preparedness. This approach was endorsed in the Ministerial Conference on CIIP held in Tallinn on 27 and 28 April 2009, one of the conclusions of which was that '***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*'.

On 18 December 2009, the Council adopted a Resolution on '*a collaborative approach European approach to network and information security*'[7] that stressed that '***ENISA, under a revised mandate, should serve as the EU's centre of expertise in EU related Network and Information Security matters***'.

In the Commission's Europe 2020 Strategy for smart, sustainable and inclusive growth[8], one of the flagship initiatives advancing Europe 2020 is the European Digital Agenda, in which NIS plays a central role. The **objective of this policy initiative for trust and security in the European Digital Agenda is to enable the EU, the Member States and stakeholders to develop a high level of capability and preparedness to prevent, detect and better respond to NIS problems.** This will contribute to increasing trust and security in Europe's Digital Single Market and improve the competitiveness of European businesses.

2. PROBLEM DEFINITION

2.1. What is the problem?

The following problem drivers have been identified which make stakeholders vulnerable to NIS threats and NIS incidents. 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 changing technology and market conditions around NIS.

- **The diversity and fragmentation of national approaches.** NIS problems are not constrained by national boundaries and therefore cannot be effectively addressed at national level only. At the same time, the problem is dealt with in many different ways by public authorities in different Member States. The multiple security requirements in

5 From 7 November 2008 through 9 January 2009, report available at http://ec.europa.eu/information_society/policy/nis/nis_public_consultation/index_en.htm.

6 Communication from the Commission to the European Parliament and the Council on Critical Information Infrastructure Protection - COM(2009)149, 30.3.2009.

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

8 COM(2010) 2020.

different Member States imposes a cost burden on businesses which operate EU-wide, leading to fragmentation and a lack of competitiveness in the European internal market.

- **Limited European early warning and response capability.** The current, national early warning and incident handling systems differ significantly across Member States, while no EU system exists. There is a need for EU policy instruments identifying NIS risks and vulnerabilities, setting out appropriate response mechanisms, and ensuring that these response mechanisms are known and applied by the stakeholders.

- **A 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 incidents, which makes it difficult for policy makers to adopt adequate policy measures and for businesses to make decisions on investing in security.

- **Alack of awareness of NIS risks and challenges.** Responsibility for ensuring NIS lies with individual stakeholders; however, their responsibilities are not always clearly defined and communicated. On the one hand, consumers often underestimate NIS risks and ignore their personal responsibility for securing their ICT systems. On the other hand, businesses often mainly see the costs of NIS and not the potential savings it entails.

- **The international dimension of network and information security problems.** Threats to NIS and any subsequent incidents are international by nature, so EU actions may be less effective if NIS problems are not also adequately addressed internationally. We need to develop an EU strategy and reference point for NIS to put the EU in a better position internationally.

- **The need for models of collaboration to ensure adequate policy implementation.** Adequate implementation of NIS policies requires collaborative models at EU level. Stakeholders need guidance in identifying NIS threats and developing good practices in implementing existing NIS policies.

- **The need for more efficient action against cyber crime.** NIS efforts have been predominantly organised under the former first pillar, i.e. matters discussed among the institutions. However, with the entry into force of the Lisbon Treaty, it is necessary to take into account a broader task package for an NIS agency, also covering 'second and third pillar' areas, i.e. matters that were formerly decided by the Council alone.

2.2. Who is most affected by the problem?

NIS incidents could have a very large impact on a variety of stakeholders, comprising large and small businesses, public authorities and administrations and individual citizens. In other words, everyone is concerned with and responsible for NIS.

There is little or no objective quantitative information available about the exact number of NIS incidents and/or their respective economic impacts. One indication is given by the IDC EMEA market study[9], which stated that 28% of the EU-27 households had suffered from

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

problems with spam or viruses in the last 12 months. On average, approximately 7% of business users experienced a security incident in the last year.

3. RATIONALE FOR EU ACTION, EU VALUE ADDED AND SUBSIDIARITY

The interdependence of networks and information systems makes it extremely difficult, if not impossible, for individual actors to correctly judge the global economic and societal impact of their measures to protect against NIS incidents. Different national policies and practices disrupt the internal market because of both the negative externalities of NIS incidents (inadequate policies affect markets in other Member States), and the positive externalities of good NIS practices (good practice in one Member State improves NIS as a whole, thus creating a clear societal good). Therefore, EU policy intervention is justified as it would provide real added value to the functioning of the internal market. Such added value was also recognised in Regulation (EC) No 460/2004 establishing ENISA, which provides that the competences of ENISA aim to contribute to the smooth functioning of the internal market.

Furthermore, EU intervention in NIS policy is justified by the *subsidiarity principle*. As noted in the CIIP Communication, an EU strategy of complete non-intervention in national NIS policies is rather akin to asking each Member State to only guard its own backyard, regardless of the interdependence of information systems. An appropriate degree of coordination between the Member States to ensure that the cross-border implications of NIS risks can be well managed is therefore consistent with the subsidiarity principle. Furthermore, EU action would improve the effectiveness of any existing national policies.

EU citizens are increasingly entrusting their data to complex information systems (e.g. cloud computing). Therefore, concerted and collaborative NIS policy action can have a strong beneficial impact on effective *protection of fundamental rights*, and specifically the right to the *protection of personal data and privacy*. For this reason too, further EU policy action seems amply justified.

4. POLICY OBJECTIVES

This impact assessment examines the extent to which 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 is to enable the EU, the Member States and stakeholders to develop a high degree of capability and preparedness to prevent, detect and better respond to NIS problems. This will contribute to increasing trust and security in Europe's Digital Single Market and improve the competitiveness of European businesses.

This objective is broken down into seven **specific objectives**:

(1) **Coherence of regulatory approaches** — provide guidance and advice to the Commission and the Member States on updating and developing a holistic normative framework in the field of NIS;

(2) **Prevention, detection and response** — improve preparedness by contributing to a European early warning and incident response capability, pan-European contingency plans and exercises;

(3) **Support for policy making** — provide assistance and deliver advice to the Commission and the Member States;

(4) **Empowerment of 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 SMEs as well as developing a culture of NIS awareness;

(5) **Making Europe a viable player in the international context** — achieve a high level of 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;

(6) **Collaborative implementation** — facilitate collaboration in implementing NIS policies;

(7) **Fighting cyber crime** — develop an effective response to NIS aspects of cyber crime through cooperation with (former) second and third pillar authorities, e.g. with Europol.

5. POSSIBLE ORGANISATIONAL FORMATS AND POLICY OPITONS

A number of possible organisational formats to implement the above policy options are examined in the Impact Assessment (Chapter 4 and Annex 4), 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) direct incorporation into a Commission service.

Comparing these different organisational formats, the Agency format seems best suited as the policy instrument of choice because of its advantages regarding: (1) legal certainty of the organisational structure as well as on substance, (2) its suitability for the specific concerns of a sector as sensitive as NIS (body of external expertise, coordination of relationship with stakeholders, involvement/commitment of Member States) and (3) acceptance of and the reputation of ENISA in the NIS community.

Hence, the following policy options were developed and assessed in detail for the organisational format of an Agency.

Policy option 1: No policy

Under the option 'No policy', it is assumed that ENISA would stop existing after March 2012 and that no other EU institution would take over all or part of ENISA's current activities.

Closing down ENISA would mean all the investment made so far, for example in setting up an organisation that is capable of attracting highly specialised people, in building up experience, and in creating networks with and between stakeholders and with international institutions, would be withdrawn at a moment when the existing Agency has reached cruising speed.

The complex nature of the NIS problem across Europe calls for a modernised and strengthened Agency, not for closing the existing one down. This is confirmed by the explicit role given to ENISA, for example in the reformed regulatory framework for electronic

communications[10], and the general support expressed by stakeholders for a more important role for a European NIS Agency.

Policy option 2: Continuation à l'identique

Option 2 represents the 'business as usual' scenario, i.e. continuation of the same policy instrument in an identical form and with the same resources. Among stakeholders, there is a general consensus that ENISA has matured into a credible point of reference for NIS issues and developed into a centre of excellence in its domain.

Given the current staffing and budgetary restrictions, the Agency will be able to have an impact only on a very limited number of NIS issues. However, this contrasts with the overall expectations of stakeholders. Not giving the Agency the possibility to further evolve and live up to such increasing expectations could ultimately lead to a crisis of credibility.

Policy option 3: Expanding the functions currently defined for ENISA and adding law enforcement and privacy protection agencies as fully fledged stakeholders

Under this option the role of a NIS Agency would be expanded, focusing on:

- Building and maintaining a liaison network between stakeholders and a knowledge network;
- 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 the EU CIIP & resilience policy (e.g. exercises, EP3R[11], European Information Sharing and Alert System, etc.);
- Setting up an EU framework for the collection of NIS data, including developing 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);
- Performing non-operational tasks related to NIS aspects of law enforcement and judicial cooperation.

The Agency would dispose of all resources necessary to perform its activities in a satisfactory in-depth way, i.e. allowing for a real impact. With more resources available, ENISA 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 constantly evolving NIS environment.

Policy option 4: Adding operational functions in fighting cyber attacks and response to cyber incidents

In addition to the activities set out under option 3, the Agency would have operational functions such as taking a more active role in EU CIIP, for example in incident prevention

---

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

[11] European Public Private Partnership for Resilience, see COM(2009) 149.

and response, specifically by acting as an EU NIS Computer Emergency Response Team (CERT) and by coordinating national CERTs as an EU NIS Storm Centre, including both day-to-day management activities and handling emergency services.

This option would require a substantial increase in the Agency's budget and human resources, which raises concerns about its absorption capacity and effective use of the budget in relation to the benefits to be attained.

Policy option 5: Adding operational functions in supporting law enforcement and judicial authorities in fighting cybercrime

In addition to the activities listed in option 4, this option would include functions for the Agency relating to:

- Providing support on procedural law (cf. Convention on Cybercrime): e.g. collection of traffic data, interception of content data, monitoring flows in case of denial-of-service attacks;
- Being a centre of expertise for criminal investigation including NIS aspects.

Like option 4, this would require a substantial increase in the Agency's resources and raise similar concerns regarding absorption capacity and effective use of the budget.

6. COMPARISON OF POLICY OPTIONS AND ASSESSMENT OF IMPACTS

Analysis of the possible economic, social and environmental impacts reveals that ***option 1*** would produce negative effects in all respects and the situation would worsen.

Option 2 turns out to be sub-optimal as the Agency would not have the necessary resources to address adequately the challenges of the constantly changing NIS landscape, which could lead to reputational risk and — ultimately — a crisis of credibility.

Under ***option 3,*** a modernised NIS Agency would contribute to:

Reducing the fragmentation of national approaches (problem driver 1), increasing data and knowledge/information-based policy and decision making (problem driver 3) and increasing overall awareness of and the tackling of NIS risks and challenges (problem driver 4) by contributing to:

- more efficient collection of relevant information on risks, threats and vulnerabilities by each individual Member State;
- increased availability of information on current and future NIS challenges and risks;
- higher-quality NIS policy provision in Member States.

Improving European early warning and response capability (problem driver 2) by:

- helping the Commission and Member States to set up pan-European exercises, thereby achieving economies of scale in responding to EU-wide incidents;

- facilitating the functioning of the EP3R, which could ultimately lead to more investment triggered by common policy objectives and EU-wide standards for security and resilience.

Promoting a common global approach to NIS (problem driver 5) by:

- increasing the exchange of information and knowledge with non-EU countries.

Fighting cybercrime more efficiently and effectively (problem driver 7) by:

- being involved in non-operational tasks relating to NIS aspects of law enforcement and judicial cooperation, such as bi-directional exchange of information and training (e.g., in cooperation with the European Police College CEPOL).

Option 4 would produce a greater impact at operational level, in addition to the impacts to be achieved under option 3. By acting as an EU NIS CERT and by coordinating national CERTs, the Agency would contribute to higher economies of scale in responding to EU-wide incidents and lower operational risks for business due to higher levels of security and resilience, for example.

Option 5 would achieve greater effectiveness in fighting cybercrime than options 3 and 4, with the addition of operational functions in supporting law enforcement and judicial authorities.

However, while both options 4 and 5 would have greater positive impacts than option 3, both these options would be politically sensitive for the Member States in relation to their CIIP responsibilities (i.e. a number of Member States would not be in favour of centralised operational functions). In addition, enlarging the mandate as examined under options 4 and 5 may create render the Agency's position ambiguous. Moreover, adding these new and completely different operational tasks to the Agency's mandate may turn out to be very challenging in the short run and there is a significant risk that the agency would not be able to carry out this kind of task properly within a reasonable time-span. Last, but not least, the cost of implementing options 4 and 5 is prohibitively high — the budget required would be four or five times as much as ENISA's current budget .

When comparing the impacts of all five policy options for the organisational format of a modernised NIS Agency, options 1 and 2 have to be discarded because neither would allow the complex NIS problem to be addressed adequately at EU level. Options 3, 4 and 5, on the other hand, would an enable the EU to address future NIS policy options appropriately. Options 4 and 5 seem, for the time being, over-ambitious, both as regards the political sensitivities of the majority of Member States and as regards the budget implications. Hence, ***option 3 appears to be the best option to address the seven NIS problems identified in the most efficient way.***

7. MONITORING AND EVALUATION: HOW ARE THE ACTUAL COSTS AND BENEFITS AND THE ACHIEVEMENT OF THE DESIRED EFFECTS TO BE MEASURED?

This policy initiative would provide for periodic evaluations which would be forwarded by the Commission to the European Parliament and the Council and be made public. These

evaluations would take into account the views of all relevant stakeholders, on the basis of terms of reference agreed with the Management Board of the Agency, and would 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. Following an evaluation, the Management Board of the Agency would issue recommendations to the Commission regarding any appropriate changes to be made to the Regulation. 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 Article 228 of the Treaty.