



COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 1.6.2007
COM(2007) 285 final

**COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN
PARLIAMENT AND THE COUNCIL**

On the evaluation of the European Network and Information Security Agency (ENISA)

INVITATION TO COMMENT ON THIS COMMUNICATION

The European Commission would like to invite all interested parties to comment on the issues addressed in this Communication, and in particular the questions listed in section 7.2, by filling out an on-line survey. The possibility to fill out the survey will be open for eight weeks. A link to the survey can be found at the following website:

<http://ec.europa.eu/yourvoice/ipm/forms/dispatch?form=EnisaFuture&lang=en>

A report summarising the comments received and a list of organisations or people that have filled out the survey will be published on the web. Anonymous comments will not be considered.

The Commission reserves the right not to include comments it receives in the summary (e.g., because the comments contain offensive language). The summary will be available in due time via a link at the website mentioned above.

**COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN
PARLIAMENT AND THE COUNCIL**

On the evaluation of the European Network and Information Security Agency (ENISA)

TABLE OF CONTENTS

1.	Introduction	4
2.	ENISA: the history	4
3.	The Evaluation of ENISA: process and objectives	5
3.1.	The process.....	6
3.2.	The objectives of the external evaluation.....	6
4.	Findings and recommendations of the external evaluation.....	6
4.1.	Key findings of the Evaluation Panel.....	6
4.2.	Recommendations of the Evaluation Panel.....	8
5.	Appraisal of the results of the external evaluation.....	8
6.	Recommendations of the ENISA Management Board	9
7.	The way forward	10
7.1.	Further consultation and analysis.....	10
7.2.	Questions to guide further discussions.....	10
8.	Conclusion.....	11

1. INTRODUCTION

Communications networks and information systems have become an essential factor in economic and societal development. The security and resilience of communication networks and information systems is of increasing concern to society. The Commission i2010 strategy “A European Information Society for growth and employment”¹ reiterated the importance of network and information security for the creation of a single European information space. More recently, the Communication “A strategy for a Secure Information Society – Dialogue, partnership and empowerment”² reviewed the current state of threats to the Information Society and presented an updated policy strategy, highlighting the positive impact of technological diversity on security and the importance of openness and interoperability.

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.³ 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.”

This Communication presents 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.⁴ It also makes an appraisal of the evaluation report and launches a public consultation. The full text of the evaluation report⁵ and the document containing the recommendations of the Management Board⁶ are being forwarded to the European Parliament and the Council.⁷ The evaluation of ENISA is part of the practice of the Commission to systematically evaluate in a cycle of ex ante, intermediate and ex post, all Community activities.

2. ENISA: THE HISTORY

In its proposal for a Regulation of the European Parliament and the Council to establish ENISA,⁸ the Commission acknowledged that network and information security “*had become a major policy concern.*” Against this background ENISA was established in March 2004. The formal structure of the Agency includes a Management Board (comprising of Member State, Commission and stakeholder representatives), an Executive Director and a Permanent Stakeholder’s Group, which is constituted to offer advice and engage in liaison in connection

¹ http://europa.eu.int/information_society/eeurope/i2010/index_en.htm

² COM(2006) 251, 31.5.2006

³ 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”)

⁴ See Article 25 of the ENISA Regulation

⁵ Available at: http://ec.europa.eu/dgs/information_society/evaluation/studies/index_en.htm

⁶ Available at: http://enisa.europa.eu/pages/03_02.htm

⁷ In accordance with Article 25(3) of the ENISA Regulation.

⁸ COM(2003) 63, 11.2.2003

with the Agency work programme. The legal basis for the ENISA Regulation is Article 95 of the Treaty establishing the European Community. This legal basis was confirmed by the European Court of Justice (ECJ) following an action brought by the United Kingdom, in which the ECJ confirmed that the Regulation was rightly based on Article 95.⁹

The first act under the ENISA Regulation was the establishment of the Management Board which, on 14 September 2004, nominated the Executive Director (from a shortlist proposed by the Commission). Following an initial period in Brussels during the start-up phase, on the 1st September 2005, the Agency moved to Heraklion, and the staff took up their duties there. The seat had been decided by the Greek Government further to the Decision taken at the European Council meeting on 12-13 December 2003 to locate the Agency in Greece.

The tasks conferred on the Agency include the collection of appropriate information with a view to carrying out an analysis of current and emerging risks, in particular those which are likely to have an impact on the resilience of electronic communications networks and on the authenticity, integrity and confidentiality of those communications. The Agency is also called upon to develop ‘common methodologies’ to prevent security issues, contribute to raising awareness, promote exchanges of ‘current best practices’ and ‘methods of alert’ and risk assessment and management activities. The Agency is also entrusted with enhancing cooperation between those involved in the area of network and information security, providing assistance to the Commission and the Member States in their dialogue with industry to address security-related problems in hardware and software products and contributing to Community efforts to cooperate with third States and, where appropriate, with international organisations to promote a common global approach to network and information security issues, thereby contributing to the development of a culture of network and information security.¹⁰

The Council of the European Union, in its Resolution of 11-12 December 2006 on a Strategy for a Secure Information Society in Europe, reiterated the importance of these tasks by calling upon “*ENISA to continue working in close cooperation with the Member States, the Commission and other relevant stakeholders, in order to fulfil those tasks and objectives that are defined in the Regulation of the Agency and to assist the Commission and the Member States in their effort to meet the requirements of network and information security, thus contributing to the implementation and further development of the new Strategy for a Secure Information Society in Europe as set out in this Resolution.*”¹¹ Since its establishment, ENISA has carried out activities and produced deliverables as defined in the Work programmes for 2005 and 2006.¹²

3. THE EVALUATION OF ENISA: PROCESS AND OBJECTIVES

In Article 25 the ENISA Regulation mandates evaluation of the Agency by the Commission before March 2007. To this end, the Commission “*shall undertake the evaluation, notably to determine whether the duration of the Agency should be extended beyond the period specified in Article 27*” (that is, five years). Furthermore, “*the evaluation shall assess the impact of the*

⁹ Judgment of 2 May 2006 in Case C-217/04

¹⁰ As reiterated in the judgment of the ECJ, sections 56 and 57

¹¹ Document 15900/06 (Presse 343), 2772nd Council Meeting, Transport, Telecommunications and Energy, Brussels, 11-12 December 2006, p. 14.

¹² See <http://enisa.europa.eu/>

Agency on achieving its objectives and tasks, as well as its working practices and envisage, if necessary, the appropriate proposals.”

3.1. The process

In accordance with terms of reference agreed with the ENISA Management Board, the Commission launched an independent evaluation by an external panel of experts as the basis for the evaluation mandated in the ENISA Regulation. The scope of the external evaluation was to provide a formative assessment of the Agency’s working practices, organisation and remit and if appropriate, recommendations for improvements. As specified in the terms of reference, the external evaluation took account of the views of all relevant stakeholders.

3.2. The objectives of the external evaluation

The principal objective of the external evaluation was to assess the impact of the Agency on achieving its objectives and tasks, as well as its working practices. It assessed the potential to impact at national and international levels, together with lessons learnt useful for the work-programme development and the possible re-orientation of the Agency scope. The evaluation also analysed the capacity built by the Agency and the networks built with stakeholders.

The scope of the external evaluation focussed on

- (1) Relevance and utility, including the consistency of the scope, objectives and tasks of the Agency with the needs of stakeholders.
- (2) Efficiency and effectiveness and impact of, among others, use of budget and human resources, distribution of results; use of external expert knowledge pools, and networking. What was the added value of the ENISA activities; how efficient are the systems of management, internal control, budgetary and internal procedures?
- (3) Lessons for the future: input and ideas among key stakeholders on what should be the priority initiatives and tasks for the Agency for the future; how to optimise synergies with other EU level institutions and activities; how to enhance synergies with stakeholders in Member States and industry.

4. FINDINGS AND RECOMMENDATIONS OF THE EXTERNAL EVALUATION

4.1. Key findings of the Evaluation Panel

The evaluation report of the external panel of experts¹³ 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

¹³ The report is available at the following website:
http://ec.europa.eu/dgs/information_society/evaluation/studies/index_en.htm

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
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.¹⁴

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.

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.

¹⁴ It should be recalled that the seat has been established by decisions of the Heads of State and Government and of the Greek Government.

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.¹⁵ 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 formulated recommendations on the future of the Agency and on changes to the ENISA Regulation.¹⁶

Recommendations of the ENISA Management Board:

- (1) The Regulation should be revised to extend the mandate. That mandate should again have a review point.
- (2) The scope of Agency should not be materially changed.
- (3) The Regulation should be revised to combine Articles 2 and 3¹⁷ to set outcome-based key objectives that are realistic and within the scope of the Agency.

¹⁵ COM(2006) 251, 31.5.2006.

¹⁶ 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

¹⁷ On, respectively, Objectives and Tasks.

- (4) 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.
- (5) The governance structure of a Management Board, Executive Director and Permanent Stakeholders' Group should not be changed.
- (6) 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.

7. THE WAY FORWARD

7.1. Further consultation and analysis

At this stage, the Commission considers it appropriate to initiate a public consultation and an impact assessment, including a cost/benefit analysis, on the extension and the future of the Agency, in line with the Commission's Better Regulation strategy.¹⁸ The Commission will inform the European Parliament and the Council of the overall findings and results thereof.

For the purposes of the public consultation and the impact assessment (including the cost/benefit analysis), there are several avenues to be explored. First of all, the choice needs to be made whether to extend the mandate of the Agency or to replace the Agency by another mechanism, such as a permanent forum of stakeholders or a network of security organisations. If the mandate is to be extended, decisions need to be taken on the optimal operational size of the Agency in view of the need to enhance its networking capability and a possible expansion of its tasks.

If the mandate of the Agency is to be extended, its remit would need to be made more precise to support the networks and information security components of the electronic communication regulatory framework being revised under the 2006 review. The goal would be to clarify how the Agency should work with National regulatory bodies, other centres of expertise in the Member States, and the private sector to define requirements and guide their implementations to meet security and integrity challenges related to current and future electronic networks. In doing so, it will be crucial for ENISA to focus on impacts rather than deliverables in order to achieve a maximum added value for the internal market.

7.2. Questions to guide further discussions

To guide further discussions, the Commission has formulated a number of questions.

- (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

¹⁸ See, inter alia, "Better Regulation for Growth and Jobs in the European Union," Communication from the Commission to the Council and the European Parliament, COM(2005)97, 16.3.2005.

European response most needed? Is an Agency still the right instrument or would another mechanism be better suited to deal with these issues?

- (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?
- (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?
- (4) Without changing the current objectives and scope of ENISA, 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?
- (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?
- (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?
- (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?

8. CONCLUSION

The Commission values the findings and analyses of the evaluation report of the external panel of experts and the recommendations of the ENISA Management Board on the future of the Agency and changes to the ENISA Regulation. A public consultation and an impact assessment that will include a cost/benefit analysis will complete the inputs and comments needed to fully and transparently decide on a possible extension of ENISA. The Commission will inform the European Parliament and the Council of the results of the public consultation and the impact assessment as well as further specify its overall evaluation findings, in particular its decision whether or not to introduce a proposal for the extension of the duration of the Agency.