

EN

EN

EN



EUROPEAN COMMISSION

Brussels, 30.9.2010
COM(2010) 520 final

2010/0274 (COD)

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**

EXPLANATORY MEMORANDUM

1. BACKGROUND

The European Network and Information Security Agency (hereinafter ENISA) was set up in March 2004 for an initial period of five years by Regulation (EC) No 460/2004¹, with the main goal of *'ensuring a high and effective level of network and information security within the [Union], [...] 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'*. Regulation (EC) No 1007/2008² extended ENISA's mandate until March 2012.

The extension of ENISA's mandate in 2008 also launched a debate on the general direction of European efforts towards network and information security (NIS), to which the Commission contributed by launching a public consultation on the possible objectives for a strengthened NIS policy at Union level. The public consultation ran from November 2008 to January 2009 and gathered nearly 600 contributions³.

On 30 March 2009, the Commission adopted a Communication on Critical Information Infrastructure Protection⁴ (CIIP) focusing on the protection of Europe from cyber attacks and cyber disruptions by enhancing preparedness, security and resilience, with an Action Plan calling on ENISA to play a role, mainly in support to Member States. The Action Plan was broadly endorsed in the discussion at the Ministerial Conference on Critical Information Infrastructure Protection (CIIP) held in Tallinn, Estonia, on 27 and 28 April 2009⁵. The European Union Presidency's Conference Conclusions stress the importance of *'leveraging the operational support'* of ENISA; they state that ENISA *'provides a valuable instrument for bolstering Union-wide cooperative efforts in this field'* and point to the need to rethink and reformulate the Agency's mandate *'to better focus on EU priority and needs; to attain a more flexible response capability; to develop skills and competences; and to bolster the Agency operational efficiency and overall impact'* in order to render the Agency *'a permanent asset for each Member State and the European Union at large'*.

After discussion at the Telecom Council of 11 June 2009, where Member States expressed support for extending the ENISA's mandate and increasing its resources in the light of the importance of NIS and the evolving challenges in the area, the debate was brought to a conclusion under the Swedish Presidency of the Union. The Council Resolution of 18

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 (OJ L 77, 13.3.2004, p. 1).

² Regulation (EC) No 1007/2008 of the European Parliament and of the Council of 24 September 2008 amending 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 as regards its duration (OJ L 293, 31.10.2008, p. 1).

³ The summary report of the results of the Public Consultation 'Towards a Strengthened Network and Information Security Policy in Europe' is appended as Annex 11 to the Impact Assessment accompanying this proposal.

⁴ COM(2009) 149, 30.3.2009.

⁵ 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.

December 2009 on a collaborative European approach to NIS⁶ recognises the role and potential of ENISA and the need to ‘*further develop ENISA in an efficient body*’. It also stresses the need to modernise and reinforce the Agency to support the Commission and the Member States in bridging the gap between technology and policy, serving as the Union centre of expertise in NIS matters.

2. GENERAL CONTEXT

Information and communication technologies (ICTs) have become the backbone of the European economy and society as a whole. ICTs are vulnerable to threats which no longer follow national boundaries and which have changed 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. At the same time, challenges related to NIS evolve quickly. Networks and information systems must be effectively protected against all kinds of disruptions and failures, including man-made attacks.

Policies on Network and Information Security (NIS) play a central role in the Digital Agenda for Europe⁷ (DAE), a flagship initiative under the EU 2020 Strategy, to exploit and advance the potential of ICTs and to translate this potential into sustainable growth and innovation. Encouraging the take-up of ICTs and boosting trust and confidence in the information society are key priorities of the DAE. To this end, reform of ENISA is needed to enable the Union, the Member States and stakeholders to develop a high degree of capability and preparedness to prevent, detect and better respond to NIS problems.

3. REASONS FOR ACTION

Along with this proposal, the Commission is proposing a Regulation on ENISA that would replace Regulation (EC) No 460/2004; it thoroughly revises the provisions governing the Agency and establishes the Agency for a period of five years. However, the Commission is aware that the legislative procedure in the European Parliament and in the Council for that proposal may require extensive time for debate, and there is a risk of a legal vacuum if the new mandate of the Agency is not adopted before the expiry of the current mandate.

The Commission therefore proposes this Regulation extending the current mandate of the Agency for 18 months to allow sufficient time for discussion.

⁶ Council Resolution of 18 December 2009 on a collaborative approach to Network and Information Security (OJ C 321, 29.12.2009, p. 1).

⁷ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:321:0001:0004:EN:PDF>. COM(2010) 245, 19.5.2010.

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

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

Having regard to the opinion of the European Economic and Social Committee⁸,

Having regard to the opinion of the Committee of the Regions⁹,

After transmission of the proposal to the national Parliaments,

Acting in accordance with the ordinary legislative procedure,

Whereas:

- (1) In 2004, the European Parliament and the Council adopted Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency¹⁰ (hereinafter referred to as ‘the Agency’).
- (2) In 2008, the European Parliament and the Council adopted Regulation (EC) No 1007/2008 amending Regulation (EC) No 460/2004 as regards the duration of the Agency¹¹.
- (3) From November 2008, a public debate was held on the general direction of the European efforts towards an increased network and information security, including the Agency. In line with the Commission’s Better Regulation strategy, and as a contribution to this debate, the Commission launched a public consultation on objectives for a strengthened network and information security policy at Union level,

⁸ OJ C , , p. .

⁹ OJ C , , p. .

¹⁰ 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).

¹¹ Regulation (EC) No 1007/2008 of the European Parliament and of the Council of 24 September 2008 amending 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 as regards its duration (OJ L 293, 31.10.2008, p. 1).

which ran from November 2008 to January 2009. In December 2009, the debate resulted in a Council Resolution of 18 December 2009 on a collaborative approach to Network and Information Security¹².

- (4) Taking account of the results of the public debate, it is envisaged to replace Regulation (EC) No 460/2004.
- (5) A legislative procedure to reform ENISA may require extensive time for debate and since the mandate of the Agency will expire on 13 March 2012, it is necessary to adopt an extension which will both enable sufficient discussion in the European Parliament and in the Council and ensure consistency and continuity
- (6) The duration of the Agency should therefore be extended until 13 September 2013,

HAVE ADOPTED THIS REGULATION:

Article 1

Regulation (EC) No 460/2004 is amended as follows:

Article 27 is replaced by the following:

‘Article 27 — Duration

The Agency shall be established from 14 March 2004 for a period of nine years and six months.’

Article 2 *Entry into force*

This Regulation shall enter into force on the day following that of its publication in the *Official Journal of the European Union*.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at [...],[...]

For the European Parliament
The President

For the Council
The President

¹² Council Resolution of 18 December 2009 on a collaborative approach to Network and Information Security (OJ C 321, 29.12.2009, p. 1).

LEGISLATIVE FINANCIAL STATEMENT FOR PROPOSALS

1. FRAMEWORK OF THE PROPOSAL/INITIATIVE

1.1. Title of the proposal/initiative

Proposal for a Regulation of the European Parliament and of the Council amending 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.

1.2. Policy area(s) concerned in the ABM/ABB structure¹³

Information society and media
Regulatory framework for the Digital Agenda

1.3. Nature of the proposal/initiative

- The proposal/initiative relates to **a new action**
- The proposal/initiative relates to **a new action following a pilot project/preparatory action**¹⁴
- The proposal/initiative relates to **the extension of an existing action**
- The proposal/initiative relates to **an action redirected towards a new action**

1.4. Objectives

1.4.1. *The Commission's multiannual strategic objective(s) targeted by the proposal/initiative*

Improving resilience in European e-communication networks

The Agency will continue working on resilience issues by e.g. conducting surveys of the resilience obligations, requirements and good practices in use¹⁵, plus analysis of further methods and procedures for improving resilience. Additional pilot projects will be undertaken to assess the validity of the requirements, methods and practices. The Agency will contribute to enhancing the security and resilience of critical communication information infrastructures and to the building of the Pan European PPP on Resilience (EP3R) and the pan European Forum of Member States (EFMS).

Developing and maintaining cooperation between Member States

ENISA should continue building on its efforts to identify Europe-wide security competence circles on topics like awareness-raising and incident response, cooperation on interoperability

¹³ ABM: Activity-Based Management – ABB: Activity-Based Budgeting.

¹⁴ As referred to in Article 49(6)(a) or (b) of the Financial Regulation.

¹⁵ Such surveys will build on those conducted by ENISA in 2006 and 2007 on the security measures implemented by the e-communication operators.

of pan-European eID¹⁶ and maintenance of a platform supporting European NIS good practice brokerage¹⁷. Further cooperation between Member States should be achieved with the aim of improving the capabilities of all Member States and increasing the overall levels of coherence and interoperability.

Identifying emerging risks for creating trust and confidence

The Agency will continue working on establishing a framework that will enable decision makers to better understand and assess emerging risks, arising from new technologies and new application, through a practice of systematic data collection, processing, dissemination and feedback.

Building information confidence with micro-enterprises

The digital information age is continuing to open up numerous opportunities for businesses, especially for micro-enterprises. However, further development and user adoption of ICT still suffer from vulnerabilities. The goal is to gather and assess micro-enterprises' needs and expectations in this field. ENISA will pursue this goal through fostering and piloting models for cross-border cooperation between multipliers and associations in the area of NIS capacity building aimed at micro enterprises; elaboration on certification schemes targeted at micro enterprises and development of compliance frameworks for non-experts; generation and piloting of good practice for business continuity; elaboration on compliance issues that will allow SMEs and micro-enterprises to express their security objectives and formulate road maps to achieve them.

1.4.2. Specific objective(s) and ABM/ABB activity(ies) concerned

Specific objective

To increase network and information security (NIS), to develop a culture of network and information security for the benefits of citizens, consumers, businesses and public sector organisations and identify policy challenges that are raised by future networks and the Internet

ABM/ABB activity(ies) concerned

Electronic communications policy and Network Security

¹⁶ This support will follow up the work conducted by ENISA in 2006 and 2007 on a common language to improve eID interoperability.

¹⁷ This platform is a follow-up to the work conducted in 2007 to define a roadmap on establishment of European NIS good practice brokerage.

1.4.3. *Expected result(s) and impact*

Achieve a high level of network and information security within the Union and a culture of network and information security for the benefit of citizens, consumers, businesses and public sector organisations in the European Union, thereby contributing to the smooth functioning of the internal market.

1.4.4. *Indicators of results and impact*

See 1.4.1 above

1.5. Grounds for the proposal/initiative

1.5.1. *Requirement(s) to be met in the short or long term*

ENISA was initially created in 2004 for dealing with the threats to and possible subsequent breaches of NIS. Since then the challenges related to Network Information Security have evolved with technology and market developments and have been the subject of further reflection and debate, allowing 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. In particular, the Presidency conclusions from the Ministerial conference on CIIP in Tallinn stated that “the new and long lasting challenges ahead require a thorough rethinking and reformulation of the Agency’s (ENISA’s) mandate in order to better focus on Union 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”.

Along with this proposal, the Commission is proposing a Regulation concerning ENISA that would replace Regulation (EC) No 460/2004, foresees a thorough revision of the provisions governing the Agency and establishes the Agency for a 5-year duration. However, the Commission is aware that the legislative procedure in the European Parliament and in the Council for that proposal may require extensive time for debate, and there would be a risk of a legal vacuum if the new mandate of the Agency is not adopted before the expiry of the current mandate.

The Commission therefore proposes this Regulation extending of the current mandate of the Agency for 18 months to allow for sufficient time for discussion.

1.5.2. *Added value of EU involvement*

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. These differences can constitute a major obstacle to the implementation of appropriate Union-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 European Union level and lead to fragmentation and lack of competitiveness in the European internal market.

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.

1.5.3. Lessons learned from similar experiences in the past

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 report¹⁸ 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.

See also 1.5.1 above

1.5.4. Coherence and possible synergy with other relevant instruments

The future of ENISA has been part of the general debate on NIS and other policy initiatives that focus on the future of NIS.

¹⁸ See http://ec.europa.eu/dgs/information_society/evaluation/studies/s2006_enisa/docs/final_report.pdf

1.6. Duration and financial impact

Proposal/initiative of **limited duration**

- Proposal/initiative in effect from 14/03/2012 to 13/09/2013
- Financial impact from 2012 to 2013

Proposal/initiative of **unlimited duration**

- Implementation with a start-up period from YYYY to YYYY,
- followed by full-scale operation.

1.7. Management mode(s) envisaged¹⁹

Centralised direct management by the Commission

Centralised indirect management with the delegation of implementation tasks to:

- executive agencies
- bodies set up by the Communities²⁰
- national public-sector bodies/bodies with public-service mission
- persons entrusted with the implementation of specific actions pursuant to Title V of the Treaty on European Union and identified in the relevant basic act within the meaning of Article 49 of the Financial Regulation

Shared management with the Member States

Decentralised management with third countries

Joint management with international organisations (*to be specified*)

¹⁹ Details of management modes and references to the Financial Regulation may be found on the BudgWeb site: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html
²⁰ As referred to in Article 185 of the Financial Regulation.

2. MANAGEMENT MEASURES

2.1. Monitoring and reporting rules

The Executive Director is responsible for the effective monitoring and evaluation of the performance of the Agency against its objectives and reports annually to the Management Board.

The Executive Director drafts a general report covering all the activities of the Agency in the previous year which, in particular, compares the results achieved with the objectives of the annual work programme. Following adoption by the Management Board, this report is forwarded to the European Parliament, the Council, the Commission, the Court of Auditors, the European Economic and Social Committee and the Committee of the Regions and published.

2.2. Management and control system

2.2.1. Risk(s) identified

Since ENISA was established in 2004, it has been subject to external and internal evaluations.

In accordance with Article 25 of the ENISA Regulation, the first step in this process was independent evaluation of ENISA by a panel of external experts in 2006/2007. The report by the panel of external experts²¹ confirmed that the original policy reasons for establishing ENISA and its original goals are still valid and was also instrumental in raising some of the issues that need to be tackled.

In March 2007 the Commission reported on the evaluation to the Management Board which subsequently made its own recommendations on the future of the Agency and on changes to the ENISA Regulation²².

In June, 2007 the Commission submitted its own appraisal of the results of the external evaluation and the recommendations of the Management Board in a Communication to the European Parliament and the Council.²³ The Communication stated that a choice needs to be made between 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. The Communication also launched a public consultation on the matter, soliciting input from European stakeholders with a list of questions to guide further discussions²⁴.

²¹ http://ec.europa.eu/dgs/information_society/evaluation/studies/index_en.htm.

²² As provided for in Article 25 of the ENISA Regulation. The full text of the document adopted by the ENISA Management Board, which also contains the Board's considerations, is available at the following website: http://enisa.europa.eu/pages/03_02.htm.

²³ 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>.

²⁴ <http://ec.europa.eu/yourvoice/ipm/forms/dispatch?form=EnisaFuture&lang=en>.

In 2009, the Commission launched an impact assessment to examine the possible options for the future of ENISA. This impact assessment accompanies the proposal for a Regulation concerning ENISA that would replace Regulation (EC) No 460/2004.

2.2.2. *Control method(s) envisaged*

See 2.2.1

2.3. Measures to prevent fraud and irregularities

Payments for any service or studies requested are checked by the Agency's staff prior to payment, taking into account any contractual obligations, economic principles and good financial or management practice. Anti-fraud provisions (supervision, reporting requirements, etc.) will be included in all agreements and contracts concluded between the Agency and recipients of any payments.

3. ESTIMATED FINANCIAL IMPACT OF THE PROPOSAL/INITIATIVE

3.1. Heading(s) of the multiannual financial framework and expenditure budget line(s) affected

- Existing expenditure budget lines

Heading of multiannual financial framework	Budget line	Type of expenditure	Contribution			
	Number / Description	DA/NDA ⁽²⁵⁾	from EFTA ²⁶ countries	from candidate countries ²⁷	from third countries	within the meaning of Article 18(1)(aa) of the Financial Regulation
1.a Competitiveness for growth and employment	09 02 03 01 European Network and Information Security Agency – Subsidy under Titles 1 and 2	DA	YES	NO	NO	NO
	09 02 03 02 European Network and Information Security Agency – Subsidy under Title 3	DA	YES	NO	NO	NO
5 Administrative expenditure	09 01 01 Expenditure related to staff in active employment of Information society and media policy area	NDA	NO	NO	NO	NO
	09 01 02 11 Other management expenditure	NDA	NO	NO	NO	NO

²⁵ DA= Differentiated appropriations / DNA= Non-Differentiated Appropriations

²⁶ EFTA: European Free Trade Association.

²⁷ Candidate countries and, where applicable, potential candidate countries from the Western Balkans.

3.2. Estimated impact on expenditure

3.2.1. Summary of estimated impact on expenditure

EUR million (to 3 decimal places)

Heading of multiannual financial framework:	1.a	Competitiveness for growth and employment
--	-----	---

ENISA			14 Mar- 31 Dec 2012	1 Jan- 13 Sep 2013	TOTAL
Operational appropriations					
09 02 03 02 European Network and Information Security Agency – Subsidy under Title 3	Commitments	(1)	2,073	1,734	3,807
	Payments	(2)	2,073	1,734	3,807
Administrative appropriations					
09 02 03 01 European Network and Information Security Agency – Subsidy under Titles 1 and 2		(3)	4,600	4,291	8,891
TOTAL appropriations under Heading 1a	Commitments	=1 +3	6,673	6,025	12,698
	Payments	=2+3	6,673	6,025	12,698

• TOTAL operational appropriations	Commitments	(4)	2,073	1,734	3,807
	Payments	(5)	2,073	1,734	3,807
• TOTAL appropriations of an administrative nature financed from the envelop of specific programs		(6)	4,600	4,291	8,891

TOTAL appropriations under HEADING 1.a Competitiveness for growth and employment of the multiannual financial framework	Commitments	=4+ 6	6,673	6,025	12,698
	Payments	=5+ 6	6,673	6,025	12,698

EUR million (to 3 decimal places)

Heading of multiannual financial framework:	5	Administrative expenditure
--	---	----------------------------

	14 Mar-31 Dec 2012	1 Jan-13 Sep 2013	Total
Human resources	0,342	0,299	0,641
Other administrative expenditure	0,008	0,007	0,015
TOTAL DG INFSO	0,350	0,306	0,656
Appropriations			

TOTAL appropriations under HEADING 5 of the multiannual financial framework	(Total commitments = total payments)	0,350	0,306	0,656
--	--------------------------------------	-------	-------	--------------

		14 Mar-31 Dec 2012	1 Jan-13 Sep 2013	Total
TOTAL appropriations under HEADINGS 1 to 5 of the multiannual financial framework	Commitments	7,023	6,331	13,354
	Payment	7,023	6,331	13,354

3.2.2. *Estimated impact on operational appropriations*

- The proposal/initiative does not require the use of operational appropriations
- The proposal/initiative requires the use of operational appropriations, as explained below:

Commitment appropriations in EUR million (to 3 decimal places)

Indicate objectives and outputs	14 March - 31 December 2012	1 January – 13 September 2013	TOTAL
↓			
Improving resilience in European e-communication networks	0,237	0,198	0,435
Developing and maintaining cooperation between Member	0,237	0,198	0,435
Identifying emerging risks for creating trust and confidence	0,169	0,141	0,310
Building information confidence with micro-enterprises	0,087	0,072	0,159
Management of horizontal activities	1,344	1,124	2,468
TOTAL COST	2,073	1,734	3,807

3.2.3. Estimated impact on appropriations of an administrative nature²⁸

3.2.3.1. Summary

- The proposal/initiative does not require the use of administrative appropriations
- The proposal/initiative requires the use of administrative appropriations, as explained below:

a) Administrative expenditure under Heading 5 of the multiannual financial framework

EUR million (to 3 decimal places)

HEADING 5 of the multiannual financial framework	14 Mar-31 Dec 2012	1 Jan-13 Sep 2013	TOTAL
---	--------------------	-------------------	--------------

Human resources	0,342	0,299	0,641
Other administrative expenditure	0,008	0,007	0,015

TOTAL	0,350	0,306	0,656
--------------	-------	-------	--------------

b) Administrative expenditure related to ENISA – covered under the Budget line "09.020301 European Network and Information Security: Titles 1 – Staff and Title 2 – Functioning of the Agency".

EUR million (to 3 decimal places)

	14 Mar-31 Dec 2012	1 Jan-13 Sep 2013	TOTAL
--	--------------------	-------------------	--------------

Human resources - Title 1 – Staff	4,216	3,916	8,132
Other expenditure of an administrative nature – Title 2 – Functioning of the Agency	0,384	0,375	0,759

TOTAL	4,600	4,291	8,891
--------------	--------------	--------------	--------------

²⁸ The Annex to the Legislative Financial Statement is not filled in since it is not applicable to the current proposal.

3.2.3.2. Estimated requirements of human resources

- The proposal/initiative does not require the use of human resources
- The proposal/initiative requires the use of human resources, as explained below:

a) Human resources within the Commission

	14 Mar-31 Dec 2012	1 Jan-13 Sep 2013
Establishment plan posts (officials and temporary agents) (in Full Time Equivalent FTE)		
XX 01 01 01 (Headquarters and Commission's Representation Offices)	3,5	3,5
TOTAL	3,5	3,5

b) Human resources of ENISA

		14 Mar-31 Dec 2012	1 Jan-13 Sep 2013
Establishment plan of ENISA (in Full Time Equivalent FTE)			
Officials or temporary staff	AD	29	29
	AST	15	15
TOTAL officials or temporary staff		44	44
Other staff (in FTE)			
Contract agents		13	13
Seconded national experts (SNE)		5	5
TOTAL other staff		18	18
TOTAL		62	62

Description of tasks to be carried out by the Agency's staff:

<p>Officials and temporary agents</p>	<p>The Agency will continue to:</p> <ul style="list-style-type: none"> – have advisory and coordinating functions, where it gathers and analyses data on information security. Today both public and private organisations with different objectives gather data on IT incidents and other data relevant to information security. There is, however, no central entity at European level that, in a comprehensive manner, can collect and analyse data and provide opinions and advice to support the Union’s policy work on network and information security; – serve as a centre of expertise to which both Member States and European institutions can turn for opinions and advice on technical matters relating to security; – contribute to broad cooperation between different actors in the information security field, e.g. assist in the follow-up activities in support of secure e-business. Such cooperation will be a vital prerequisite for secure functioning of networks and information systems in Europe. Participation and involvement of all stakeholders is necessary; – contribute to a coordinated approach to information security by providing support to Member States, e.g. on promotion of risk assessment and awareness-raising activities; – ensure interoperability of networks and information systems when Member States apply technical requirements that affect security; – identify the relevant standardisation needs and assess existing security standards and certification schemes and promote their widest possible use in support of the European legislation; – support international cooperation in this field which is becoming more and more necessary as network and information security issues are global.
<p>External personnel</p>	<ul style="list-style-type: none"> – See above

3.2.4. *Compatibility with the current multiannual financial framework*

- Proposal/initiative is compatible the current multiannual financial framework.
- Proposal/initiative will entail reprogramming of the relevant heading in the multiannual financial framework.
- Proposal/initiative requires application of the flexibility instrument or revision of the multiannual financial framework²⁹.

3.2.5. *Third-party contributions*

- The proposal/initiative does not provide for co-financing by third parties
- The proposal/initiative provides for the co-financing estimated below (applicable to the lines 09.020301 and 09.020302):

Indicative appropriations in EUR million (to 3 decimal places)

	14 Mar-31 Dec 2012	1 Jan-13 Sep 2013	Total
<i>EFTA</i>	0,160	0,145	0,305

3.3. **Estimated impact on revenue**

- Proposal/initiative has no financial impact on revenue.
- Proposal/initiative has the following financial impact:
 - on own resources
 - on miscellaneous revenue

²⁹ See points 19 and 24 of the Interinstitutional Agreement.