COUNCIL OF THE EUROPEAN UNION

Brussels, 1 October 2010

14358/10

Interinstitutional File: 2010/0275 (COD)

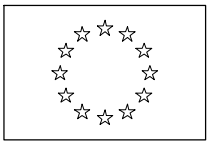
TELECOM 99
MI 346
DATAPROTECT 70
JAI 794
CAB 16
INST 361
CODEC 943

PROPOSAL

from:	Commission
dated:	1 October 2010
Subject:	Proposal for a Regulation of the European Parliament and of the Council concerning the European Network and Information Security Agency (ENISA)

Delegations will find attached a proposal from the Commission, submitted under a covering letter from Mr Jordi AYET PUIGARNAU to Mr Pierre de BOISSIEU, Secretary-General of the Council of the European Union.

Encl.: COM(2010) 521 final



EUROPEAN COMMISSION

Brussels, 30.9.2010
COM(2010) 521 final

2010/0275 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

Concerning the European Network and Information Security Agency (ENISA)

{SEC(2010) 1126}
{SEC(2010) 1127}

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

1.1. Policy context

The European Network and Information Security Agency (ENISA) was established in March 2004 for an initial period of five years by Regulation (EC) No 460/2004[1], 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 1007/2008[2] 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. This public consultation ran from November 2008 to January 2009 and gathered nearly 600 contributions[3].

On 30 March 2009, the Commission adopted a Communication on Critical Information Infrastructure Protection[4] (CIIP) focusing on protecting 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 2009[5]. 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 priorities and needs; to attain a more flexible response capability; to develop skills and competences; and to bolster the Agency's 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 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

---

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.

conclusion under the Swedish Presidency of the Union. The Council Resolution of 18 December 2009 on a collaborative European approach to NIS[6] recognises the role and potential of ENISA and the need to '*further develop ENISA into 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's centre of expertise in NIS matters.

1.2. 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 infrastructure, 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 Europe[7] (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.

ENISA was initially created to ensure a high and effective level of network and information security within the Union. The experience gained with the Agency and the challenges and threats have underlined the need to modernise its mandate to make it better fit needs of the European Union stemming from:

- the fragmentation of national approaches to tackling the evolving challenges;
- the lack of collaborative models in the implementation of NIS policies;
- the insufficient level of preparedness also due to the limited European early warning and response capability;
- the lack of reliable European data and limited knowledge about evolving problems;
- the low level of awareness of NIS risks and challenges;
- the challenge of integrating NIS aspects in policies to fight cybercrime more effectively.

1.3. The policy objectives

The general objective of the proposed regulation is to enable the Union, Member States and stakeholders to develop a high degree of capability and preparedness to prevent, detect and better respond to NIS problems. This will help to build trust, which underpins the

---

6 Council Resolution of 18 December 2009 on a collaborative approach to Network and Information Security (OJ C 321, 29.12.2009, p. 1), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:321:0001:0004:EN:PDF.

7 COM(2010) 245, 19.5.2010.

development of the Information Society, to improve the competitiveness of European businesses and to ensure that the Internal Market functions effectively.

1.4. Existing provisions in the area of the proposal

This proposal complements regulatory and non-regulatory policy initiatives on Network and Information Security taken at Union level to enhance the security and resilience of ICTs:

- The Action Plan launched by the CIIP Communication addressed the establishment of both:

  (1) A European Forum for Member States (EFMS) aimed at fostering discussion and exchange regarding good policy practices with the aim of sharing policy objectives and priorities on security and resilience of ICT infrastructure, also directly benefiting from the work and the support provided by the Agency.

  (2) A European Public-Private Partnership for Resilience (EP3R), which is the flexible Europe-wide governance framework for resilience of ICT infrastructure, which operates by fostering the cooperation between the public and the private sector on security and resilience objectives, baseline requirements, good policy practices and measures.

- The Stockholm Programme, adopted by the European Council on 11 December 2009, promotes policies ensuring network security and allowing faster reaction in the event of cyber attacks in the Union.

- These initiatives contribute to giving effect to the Digital Agenda for Europe. Policies on NIS play a central role in that part of the strategy that focuses on boosting trust and security in the information society. They also support the Commission's support measures and policy on the protection of privacy (notably 'privacy by design') and personal data (review of the framework), the CPC network, identity management, and the Safer Internet Programme.

1.5. Developments in current NIS policy related to the proposal

Several of the ongoing developments in NIS policy, notably those announced in the Digital Agenda for Europe, benefit from the support and expertise of ENISA. These include:

- Strengthening NIS policy cooperation by intensifying activities in the **European Forum of Member States (EFMS)**, that will, with the direct support of ENISA, help:

  – define ways to establish an effective European network through cross-border cooperation between national/governmental Computer Emergency Response Teams (CERTs);

  – identify long-term objectives and priorities for pan-European large scale exercises on NIS incidents;

  – leverage minimum requirements in public procurement to boost security and resilience in public systems and networks;

  – identify economic and regulatory incentives for security and resilience;

– evaluate the state of NIS health in Europe.

- Strengthening cooperation and partnering between the public and the private sector, by supporting the **European Public-Private Partnership for Resilience (EP3R)**. ENISA plays a growing role in the facilitation of EP3R meetings and activities. The next steps of EP3R will include:

  – Discussing innovative measures and instruments to improve security and resilience, such as:

  (1) baseline security and resilience requirements, particularly in public procurement for ICT products or services, to provide a level playing field while ensuring an appropriate level of preparedness and prevention;

  (2) exploring issues of economic operators' liability, for instance when they put in place minimum security requirements;

  (3) economic incentives for the development and uptake of risk management practices, security processes and products;

  (4) risk assessment and management schemes to assess and manage major incidents on a common basis of understanding;

  (5) cooperation between the private and the public sector in the event of large-scale incidents;

  (6) organising a **Business Summit** on economic barriers and drivers for security and resilience.

- Putting the security requirements of the regulatory package on electronic communications into practice, for which ENISA's expertise and assistance is required:

  – to support the Member States and the Commission, taking into account the views of the private sector as appropriate, in laying down a framework of rules and procedures to implement the security breach notification provisions (laid down in Article 13(a) of the revised Framework Directive).

  – to set up a yearly Forum for NIS national competent bodies/National Regulatory Authorities and the private sector stakeholders to discuss lessons learnt and exchange good practices on the application of regulatory measures for NIS.

- Facilitating **EU-wide cyber security preparedness exercises** with the support of the Commission and the contribution of ENISA, with a view to extending such exercises at a later stage at international level.

- **Establishing a CERT (Computer Emergency Response Team) for the EU institutions**. Key Action 6 of the Digital Agenda for Europe is that the Commission will present 'measures aimed at a reinforced and high level Network and Information Security Policy, including […] measures allowing faster reactions in the event of cyber attacks, including a

CERT for the EU institutions'[8]. This will require the Commission and the other Union institutions to analyse, and set up a Computer Emergency Response Team for which ENISA can provide technical support and expertise.

- Mobilising and supporting the Member States in completing and where necessary in setting up **national/governmental CERTs in order to establish a well-functioning network of CERTs covering all of Europe**. This activity will also be instrumental in further developing a European Information Sharing and Alert System (EISAS) for citizens and SMEs to be built with national resources and capabilities by the end of 2012.

- **Raising awareness** of NIS challenges, which will include:

  – the Commission working with ENISA to draft guidance on promoting NIS standards, good practices and a risk management culture. The first sample of guidance will be produced.

  – ENISA organising, in cooperation with the Member States, the '**European month of network and information security for all,**' featuring national/European Cyber Security Competitions.

1.6. Consistency with other policies and objectives of the Union

The proposal is consistent with existing policies and objectives of the European Union and fully in line with the objective of contributing to the smooth functioning of the internal market through enhancing preparedness and responsiveness to the challenges of Network and Information Security.

2. RESULTS OF CONSULTATIONS AND IMPACT ASSESSMENT

2.1. Consultation of interested parties

This policy initiative is the result of a wide discussion carried out following an inclusive approach and respecting the principles of participation, openness, accountability, effectiveness and coherence. The broad process that took place included an evaluation of the Agency in 2006/2007 followed by Recommendations by the Management Board of ENISA, two public consultations (in 2007 and in 2008-2009) and a number of workshops on NIS-related matters.

The first public consultation was launched in connection with the Commission Communication on the mid-term evaluation of ENISA. It focused on the Agency's future, ran from 13 June to 7 September 2007 and gathered a total of 44 online contributions plus two more submitted in writing. The responses came from a variety of stakeholders and interested parties, including Member States' ministries, regulatory bodies, industry and consumer associations, academic institutions, companies, and individual citizens.

---

[8] Council Resolution of 18 December 2009 on a collaborative European approach to Network and Information Security also provided that: *'The Council […] recognises […] the importance of exploring the strategic effects, risks and prospects for establishing CERTs for the EU institutions and considering the possible future role of ENISA in this matter'.*

The responses highlighted a number of interesting issues concerning the evolution of the threat scenario; the need to clarify and build more flexibility into the Regulation to allow ENISA to adapt to the challenges; the importance of ensuring effective interaction with stakeholders; and the opportunity for a limited increase in its resources.

The second public consultation, which ran from 7 November 2008 to 9 January 2009, aimed to identify the priority objectives for a strengthened NIS policy at European level and the means of achieving those objectives. Nearly 600 contributions were received from Member State authorities, academic/research institutions, industry associations, private companies and other stakeholders, such as data protection organisations and consultancies, and private citizens.

A large majority of the respondents[9] supported extending the Agency's mandate and advocated an enlarged role in coordination of NIS activities at the European level and an increase in its resources. Key priorities were the need for a more coordinated approach to cyber threats across Europe, transnational cooperation to respond to large-scale cyber attacks, building trust and improved information exchange among stakeholders.

An impact assessment on the proposal was carried out, starting in September 2009, based on a preparatory study carried out by an external contractor. A wide variety of stakeholders and experts were involved. The contributors included Member State NIS bodies, national regulatory authorities, telecommunications operators and internet service providers and related sector associations, consumers associations, ICT manufacturers, Computer Emergency Response Teams (CERTs), academics, and corporate users. An Inter-Service Steering Group, composed of the relevant Commission Directorates-General, was set up to support the impact assessment process.

2.2. Impact assessment

Keeping an Agency was identified as an appropriate solution for attaining European policy objectives[10]. Following a pre-screening process, five policy options were selected for further analysis:

- Option 1 — No policy;
- Option 2 — Carry on as before, i.e., with a similar mandate and the same level of resources;
- Option 3 — Expand the tasks of ENISA, adding law enforcement and privacy protection authorities as fully fledged stakeholders;
- Option 4 — Add fighting cyber attacks and response to cyber incidents to its tasks;
- Option 5 — Add supporting law enforcement and judicial authorities in fighting cybercrime to its tasks.

Following a comparative cost-benefit analysis, option 3 was identified as the most cost-effective and efficient way of achieving the policy objectives.

---

9 See Annex XI of the Impact Assessment

10 See Annex IV of the Impact Assessment.

Option 3 envisages an expansion of ENISA's role, to focus on:

- building and maintaining a liaison network between stakeholders and a knowledge network to ensure that ENISA is comprehensively informed of the European NIS landscape;
- being the 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 Union CIIP & Resilience policy (exercises, EP3R, European Information Sharing and Alert System, etc.);
- setting up an Union framework for the collection of NIS data, including developing methods and practices for legal reporting and sharing;
- studying 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 cybercrime law enforcement and judicial cooperation.

3. LEGAL ELEMENTS OF THE PROPOSAL

3.1. Summary of the proposed action

The proposed Regulation aims to strengthen and modernise the European Network and Information Security Agency (ENISA), and to establish a new mandate for a period of five years.

The proposal includes some key changes as compared to the original Regulation:

(1) **More flexibility, adaptability and capability to focus**. The tasks are updated and re-formulated broadly, in order to provide more scope for Agency activities; they are sufficiently precise to depict the means by which the objectives are to be achieved. This better focuses the Agency's mission, improves its capability to achieve its objectives and strengthens its tasks to support the implementation of Union policy.

(2) **Better alignment of the Agency to the Union's policy and regulatory process**. The European institutions and bodies may refer to the Agency for assistance and advice. This is in line with political and regulatory developments: the Council has started addressing the Agency directly in Resolutions, and the EP and the Council have assigned network and information security-related tasks to the Agency in the regulatory framework on electronic communications.

(3) **Interface with the fight against cybercrime**. In the achievement of its objectives, the Agency takes account of the fight against cybercrime. Law enforcement and privacy protection authorities become fully fledged stakeholders of the Agency, notably in the Permanent Stakeholders Group.

(4) **Strengthened governance structure**. The proposal enhances the supervisory role of the Agency's Management Board, in which the Member States and the Commission are represented. For example, the Management Board is able to issue general

directions on staff matters, previously the sole responsibility of the Executive Director. It may also establish working bodies to assist it in carrying out its tasks, including monitoring the implementation of its decisions.

(5) **Streamlining Procedures**. Procedures that have proved to be unnecessarily burdensome are simplified. Examples: (a) simplified procedure for Management Board internal rules, (b) the opinion on the ENISA Work programme is provided by Commission services rather than via a Commission Decision. The Management Board is also given adequate resources in case it needs to take executive decisions and implement them (e.g., if a staff member lodges a complaint against the Executive Director or the Board itself).

(6) **Gradual increase of resources**. In order to meet the reinforced European priorities and the expanding challenges, without prejudice to the Commission's proposal for the next multi-annual financial framework, a gradual increase of the financial and human resources of the Agency are gradually to be increased between 2012 and 2016 is anticipated. Based on the Commission's proposal for the regulation laying down the multiannual financial framework post-2013 and taking into account the conclusions of the impact assessment, the Commission will present an amended Legislative Financial Statement.

(7) **Option of extending the term of office of the Executive Director**. The Management Board may extend the term of office of the Executive Director for three years.

3.2. Legal basis

This proposal is based on Article 114 of the Treaty on the Functioning of the European Union[11] (TFEU).

In accordance with the European Court of Justice judgment[12], before the entry into force of the Lisbon Treaty, **Article 95 of the EC Treaty** was to be considered the appropriate legal basis for the creation of a body for the purpose of ensuring a high and effective level of NIS within the Union. By using the expression 'measures for the approximation' in Article 95 the authors of the Treaty intended to confer on the Union legislature a discretion to choose the appropriate measures for achieving the desired result. 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[13]** describes — almost identically — the internal market responsibility. For the reasons set out above, it will continue to be the applicable legal basis for adopting measures to improve NIS. The Internal Market responsibility is now a shared competence between the Union and the Member States (Article 4(2)(a) TFEU). This means that the Union and the Member States may adopt (binding) measures and that the Member States will act if the Union has not exercised its competence or has decided not to act anymore (Article 2(2) TFEU).

Measures under the Internal Market responsibility will require the ordinary legislative

---

11 OJ C 115, 9.5.2008, p. 94.

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

13 Cf. supra.

procedure (Articles 289 and 294 of the TFEU), which is similar[14] to the former co-decision procedure (Article 251 of the EC Treaty).

With the Lisbon treaty, the former distinction between the pillars has disappeared. Preventing and combating crime has become a shared competence of the Union. This has created an opportunity for ENISA to play a role as a platform on NIS aspects of the fight against cybercrime and to exchange views and best practices with cyber defence, law enforcement and privacy protection authorities.

3.3. Subsidiarity principle

The proposal complies with the subsidiarity principle: NIS policy requires a collaborative approach and the objectives of the proposal cannot be achieved by the Member States individually.

A complete non-intervention strategy by the Union in national NIS policies would leave the task up to the Member States, disregarding the clear interdependence between existing information systems. A measure ensuring 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 arise does therefore respect the subsidiarity principle. Furthermore, European action would improve the effectiveness of existing national policies and thus add value.

In addition, setting up a concerted and collaborative NIS policy will have a beneficial impact on the protection of fundamental rights, and specifically the right to the protection of personal data and privacy. The need to protect data is currently crucial given the fact that European citizens are increasingly entrusting their data to complex information systems, either out of choice or 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.

3.4. Proportionality principle

This proposal complies with the proportionality principle since it does not go beyond what is necessary in order to achieve its objective.

3.5. Choice of instruments

Proposed instrument: a regulation, which is directly applicable in all Member States.

4. BUDGETARY IMPLICATION

The proposal will impact on the Union budget.

Since the tasks to be included in the new mandate for ENISA are laid down, it is anticipated that the Agency will be given the resources required to carry out its activities satisfactorily. The evaluation of the Agency, the extensive consultation process with stakeholders at all levels and the impact assessment show general agreement that the size of the Agency is below

[14] The ordinary legislative procedure differs in particular in terms of majority requirements in Council and EP.

its critical mass and that an increase in resources is required. The consequences and effects of an increase in the staff and budget of the Agency are analysed in the Impact Assessment accompanying the proposal.

EU funding after 2013 will be examined in the context of a Commission-wide debate on all proposals for the post-2013 period.

5. ADDITIONAL REMARKS

5.1. Duration

The Regulation shall cover a period of five years.

5.2. Review clause

The Regulation provides for an evaluation of the Agency, covering the period since the previous evaluation in 2007. It will assess the Agency's effectiveness in achieving its objectives as set out in the Regulation, whether it is still an effective instrument and whether the duration of the Agency should be further extended. Based on the findings, the Management Board will make recommendations to the Commission regarding changes to this Regulation, the Agency and its working practices. To enable the Commission to draft any proposal for an extension of the mandate in good time, the evaluation will have to be done by the end of the second year of the mandate provided by the Regulation.

5.3. Interim measure

The Commission is aware that the legislative procedure in the European Parliament and in the Council may require extensive time for debate on the proposal, and there is a risk of a legal vacuum if the new mandate of the Agency is not adopted in due time before the expiry of the current mandate. The Commission is therefore proposing, along with this proposal, a Regulation extending the current mandate of the Agency for 18 months to allow sufficient time for debate and due process.

2010/0275 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

Concerning the European Network and Information Security Agency (ENISA)

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 Committee[15],

Having regard to the opinion of the Committee of the Regions[16],

After transmission of the proposal to the national Parliaments,

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) Electronic communications, infrastructure and services are an essential factor in economic and societal development. They play a vital role for society and have become ubiquitous utilities in the same way that electricity or water supplies are. Their disruption has the potential to cause considerable economic damage, underlining the importance of measures to increase protection and resilience aimed at ensuring continuity of critical services. The security of electronic communications, infrastructure and services, in particular their integrity and availability, faces continuously expanding challenges. This is of increasing concern to society not least because of the possibility of problems due to system complexity, accidents, mistakes and attacks that may have consequences for the physical infrastructure which delivers services critical to the well-being of European citizens.

(2) The threat landscape is continuously changing and security incidents can endanger user confidence. While severe disruptions of electronic communications, infrastructure and services can have a major economic and social impact, everyday security breaches, problems and nuisances also risk eroding public confidence in technology, networks and services.

(3) Regular assessment of the state of network and information security in Europe, based on reliable European data, is therefore important for policy makers, industry and users.

---

15 OJ C , , p. .

16 OJ C , , p. .

(4) The representatives of the Member States, meeting in the European Council on 13 December 2003, decided that the European Network and Information Security Agency (ENISA), that was to be established on the basis of the proposal submitted by the Commission, would have its seat in a town in Greece to be determined by the Greek Government.

(5) In 2004 the European Parliament and the Council adopted a Regulation (EC) No 460/2004[17] establishing the European Network and Information Security Agency with the purpose of contributing to the goals of ensuring a high level of network and information security within the Union and developing a culture of network and information security for the benefit of citizens, consumers, enterprises and public administrations. In 2008, the European Parliament and the Council adopted a Regulation (EC) No 1007/2008[18] extending the mandate of the Agency until March 2012.

(6) Since the Agency was set up, the challenges of network and information security have changed with technology, market and socio-economic developments and have been the subject of further reflection and debate. In response to the changing challenges, the Union has updated its priorities for network and information security policy in a number of documents, including the 2006 Commission Communication *A strategy for a Secure Information Society — Dialogue, partnership and empowerment*[19], the Council Resolution of 2007 on a Strategy for a Secure Information Society in Europe[20], the 2009 Communication *Critical Information Infrastructure Protection – 'Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience'*[21], the Presidency Conclusions of the Ministerial Conference on Critical Information Infrastructure Protection (CIIP), the Council Resolution of 2009 on a collaborative European approach to Network and Information Security[22]. The need has been recognised to modernise and strengthen the Agency to successfully contribute to the efforts of the European institutions and the Member States to develop a European capacity to cope with network and information security challenges. More recently, the Commission adopted the Digital Agenda for Europe[23], as a flagship initiative under the Europe 2020 Strategy. This comprehensive agenda aims at exploiting and advancing the potential of ICT in order to translate this potential into sustainable growth and innovation. Boosting trust and confidence in the information society is one of the key objectives of this comprehensive agenda, which announced a number of actions to be taken by the Commission in this area, including the present proposal.

(7) Internal market measures in the field of security of electronic communications, and, more generally, network and information security require different forms of technical and organisational applications by the Member States and the Commission.. The heterogeneous application of these requirements can lead to inefficiencies and can

---

17 OJ L 77, 13.3.2004, p. 1.
18 OJ L 293, 31.10.2008, p. 1
19 COM(2006) 251, 31.5.2006.
20 Council Resolution of 22 March 2007 on a Strategy for a Secure Information Society in Europe (OJ C 68, 24.3.2007, p. 1).
21 COM(2009) 149, 30.3.2009.
22 Council Resolution of 18 December 2009 on a collaborative approach to Network and Information Security (OJ C 321, 29.12.2009, p. 1).
23 COM(2010)245, 19.5.2010

create obstacles to the internal market. This calls for a centre of expertise at European level providing guidance, advice, and when called upon, assistance on issues related to network and information security, which may be relied upon by the Member States and the European institutions. The Agency can respond to these needs by developing and maintaining a high level of expertise and assisting the Member States, the Commission and as a consequence the business community in order to help them to meet the legal and regulatory requirements of network and information security, thereby contributing to the smooth functioning of the internal market.

(8) The Agency should carry out the tasks conferred on it by present Union legislation in the field of electronic communications and, in general, contribute to an enhanced level of security of electronic communications by, among other things, providing expertise and advice, and promoting the exchange of good practices.

(9) Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive)[24] further requires that providers of public electronic communications networks or publicly available electronic communications services take appropriate measures to safeguard their integrity and security and introduces security breach and integrity loss notification requirements. Where appropriate, the Agency is also to be notified by the national regulatory authorities, which must also submit to the Commission and the Agency an annual summary report on the notifications received and the action taken. Directive 2002/21/EC further calls on the Agency to contribute to the harmonisation of appropriate technical and organisational security measures by providing opinions.

(10) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)[25] requires a provider of a publicly available electronic communications service to take appropriate technical and organisational measures to safeguard the security of its services and also requires confidentiality of the communications and related traffic data. Directive 2002/58/EC introduces personal data breach information and notification requirements for electronic communication services providers. It also requires the Commission to consult the Agency on any technical implementing measures to be adopted concerning the circumstances or format of and procedures applicable to information and notification requirements. 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[26] requires Member States to provide that the controller must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network and against all other unlawful forms of processing.

---

[24] OJ L 108, 24.4.2002, p. 33.
[25] OJ L 201, 31.7.2002, p. 37.
[26] OJ L 281, 23.11.1995, p. 31.

(11) The Agency should contribute to a high level of network and information security within the Union and to the development of a culture of network and information security for the benefit of citizens, consumers, businesses and public sector organisations in the European Union, thus contributing to the smooth functioning of the internal market.

(12) A set of tasks should indicate how the Agency is to accomplish its objectives while allowing flexibility in its operations. The tasks carried out by the Agency should include the collection of appropriate information and data needed to carry out analyses of the risks to the security and resilience of electronic communications, infrastructure and services and to assess, in cooperation with Member States, the state of network and information security in Europe. The Agency should ensure coordination with Member States and enhance cooperation between stakeholders in Europe, in particular by involving in its activities competent national bodies and private sector experts in the area of network and information security. The Agency should provide assistance to the Commission and the Member States in their dialogue with industry to address security-related problems in hardware and software products, thereby contributing to a collaborative approach to network and information security.

(13) The Agency should operate as a point of reference and establishing confidence by virtue of its independence, the quality of the advice it delivers and the information it disseminates, the transparency of its procedures and methods of operation, and its diligence in carrying out the tasks assigned to it. The Agency should build on national and Union efforts and therefore carry out its tasks in full cooperation with the Member States and be open to contacts with industry and other relevant stakeholders. In addition, the Agency should build on the input from and cooperation with the private sector, which play an important role in securing electronic communications, infrastructures and services.

(14) The Commission has launched a European Public-Private Partnership for Resilience as a flexible Europe-wide governance framework for resilience of ICT infrastructure, in which the Agency should play a facilitating role, bringing together public and private sector stakeholders to discuss public policy priorities, economic and market dimensions of challenges and measures for resilience of ICT infrastructure and to identify stakeholders' responsibility.

(15) The Agency should provide advice to the Commission by means of opinions and technical and socio-economic analyses, at the request of the Commission or on its own initiative, to assist with policy development in the area of network and information security. The Agency should also assist, at their request, Member States and European institutions and bodies in their efforts to develop network and information security policy and capability.

(16) The Agency should assist the Member States and the European institutions in their efforts to build and enhance cross-border capability and preparedness to prevent, detect, mitigate and respond to network and information security problems and incidents; in this regard, the Agency should facilitate cooperation among the Member States and between the Member States and the Commission. To this end, the Agency should play an active role in supporting Member States in their continuous efforts to improve their response capability and to organise and run national and European exercises on security incidents.

(17) Directive 95/46/EC governs the processing of personal data carried out pursuant to this Regulation.

(18) To understand better the challenges in the network and information security field, the Agency needs to analyse current and emerging risks. For that purpose the Agency should, in cooperation with Member States and, as appropriate, statistical bodies, collect relevant information. Furthermore, the Agency should assist the Member States and the European institutions and bodies in their efforts to collect, analyse and disseminate network and information security data.

(19) In carrying out monitoring activities in the Union, the Agency should facilitate cooperation between the Union and the Member States on assessing the state of network and information security in Europe and contribute to assessment activities in cooperation with the Member States.

(20) The Agency should facilitate cooperation among the Member States' competent public bodies, in particular supporting the development and exchange of good practices and standards for education programmes and awareness-raising schemes. Increased information exchange between Member States will facilitate such action. The Agency should also support cooperation between public and private stakeholders at the Union level, partly by promoting information sharing, awareness-raising campaigns and education and training programmes.

(21) Efficient security policies should be based on well-developed risk assessment methods, both in the public and private sector. Risk assessment methods and procedures are used at different levels with no common practice on their efficient application. The promotion and development of best practice for risk assessment and for interoperable risk management solutions in public and private sector organisations will increase the security level of networks and information systems in Europe. To this end, the Agency should support cooperation between public and private stakeholders at Union level, facilitating their efforts relating to the development and take-up of standards for risk management and for measurable security of electronic products, systems, networks and services.

(22) The work of the Agency should utilise ongoing research, development and technological assessment activities, in particular those carried out by the different European Union research initiatives.

(23) Where appropriate and useful for fulfilling its scope, objectives and tasks, the Agency should share experience and general information with bodies and agencies created under European Union law and dealing with network and information security.

(24) In liaising with law enforcement bodies on the security aspects of cybercrime, the Agency respects existing channels of information and established networks such as the points of contact mentioned in the proposed Directive of the European Parliament and the Council on attacks against information systems, repealing Framework Decision 2005/222/JHA, or the Europol Heads of High Tech Crime Units Task Force.

(25) To ensure full achievement of its objectives, the Agency should liaise with law enforcement bodies and privacy protection authorities to highlight and properly address the network and information security aspects of fighting cybercrime.

Representatives of these authorities should become fully fledged stakeholders of the Agency and should be represented in the Agency's Permanent Stakeholders Group.

(26) Network and information security problems are global issues. There is a need for closer international cooperation to improve security standards, improve information exchange, and promote a common global approach to network and information security issues. To this end, the Agency should support cooperation with third countries and international organisations in cooperation, where appropriate, with the EEAS.

(27) The exercise of the Agency's tasks should not interfere with the competencies nor pre-empt, impede or overlap with the relevant powers and tasks of: the national regulatory authorities as set out in the Directives relating to the electronic communications networks and services, as well as on the Body of European Regulators for Electronic Communications (BEREC) established by Regulation 1211/2009 [27] of the European Parliament and the Council and the Communications Committee referred to in Directive 2002/21/EC, the European standardisation bodies, the national standardisation bodies and the Standing Committee as set out in Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society Services[28] and the supervisory authorities of the Member States relating to the protection of individuals with the regard to the processing of personal data and on the free movement of such data.

(28) In order to ensure that the Agency is effective, the Member States and the Commission should be represented on a Management Board, which should define the general direction of the Agency's operations and ensure that it carries out its tasks in accordance with this Regulation. The Management Board should be entrusted with the necessary powers to establish the budget, verify its execution, adopt the appropriate financial rules, establish transparent working procedures for decision making by the Agency, adopt the Agency's work programme, adopt its own rules of procedure and the Agency's internal rules of operation, and appoint and decide on the extension or termination of the mandate of the Executive Director. The Management Board should be able to set up working bodies to assist it with its tasks; such bodies could for example draft its decisions or monitor their implementation.

(29) The smooth functioning of the Agency requires its Executive Director to be appointed on the grounds of merit and documented administrative and managerial skills, as well as competence and experience relevant for network and information security, and that he/she performs his/her duties with complete independence as to the organisation of the internal functioning of the Agency. To this end, the Executive Director should prepare a proposal for the Agency's work programme, after prior consultation with the Commission services, and take all necessary steps to ensure the proper execution of the work programme of the Agency. He should prepare a draft general report each year to be submitted to the Management Board, should draw up a draft statement of estimates of revenue and expenditure for the Agency, and should implement the budget.

---

27 OJ L 337, 18.12.2009, p.1.

28 OJ L 204, 21.7.1998, p. 37.

(30) The Executive Director should have the option of setting up ad hoc Working Groups to address specific matters, in particular of a scientific or technical, or a legal or socio-economic nature. In setting up the ad hoc Working Groups the Executive Director should seek input from and draw on the relevant external expertise needed to enable the Agency to have access to the most up-to-date information available on security challenges posed by the developing information society. The Agency should ensure that the ad hoc Working Groups' membership is selected according to the highest standards of expertise, taking due account of a representative balance, as appropriate according to the specific issues, between the public administrations of the Member States, the private sector, including industry, the users, and academic experts in network and information security. The Agency may, as necessary, invite individual experts recognised as competent in the relevant field to participate in the Working Groups' proceedings, on a case-by-case basis. Their expenses should be met by the Agency in accordance with its internal rules and in accordance with the existing Financial Regulations.

(31) The Agency should have a Permanent Stakeholders' Group as an advisory body, to ensure regular dialogue with the private sector, consumers' organisations and other relevant stakeholders. The Permanent Stakeholders' Group, set up by the Management Board on a proposal by the Executive Director, should focus on issues relevant to all stakeholders and bring them to the attention of the Agency. The Executive Director may, where appropriate and according to the agenda of the meetings, invite representatives of the European Parliament and other relevant bodies to take part in meetings of the Group.

(32) The Agency shall operate according to, respectively, (i) the principle of subsidiarity, ensuring an appropriate degree of coordination between the Member States on NIS-related matters and improving the effectiveness of national policies, thus adding value to them and (ii) the principle of proportionality, not going beyond what is necessary in order to achieve the objectives set out by this Regulation.

(33) The Agency should apply the relevant Union legislation concerning public access to documents as set out in Regulation (EC) No 1049/2001 of the European Parliament and of the Council[29] and the protection of individuals with regard to the processing of personal data as set out in Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data[30].

(34) Within its scope, in its objectives and in the fulfilment of its tasks, the Agency should comply in particular with the provisions applicable to the European institutions, and with national legislation regarding the treatment of sensitive documents. The Management Board should have the power to take a decision allowing the Agency to handle classified information.

---

29 Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (OJ L 145, 31.5.2001, p. 43).

30 Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1).

(35) In order to guarantee the full autonomy and independence of the Agency, it is considered necessary to grant it an autonomous budget whose revenue comes primarily from a contribution from the Union and contributions from third countries participating in the Agency's work. The host Member State, or any other Member State, should be allowed to make voluntary contributions to the revenue of the Agency. The Union's budgetary procedure remains applicable as far as any subsidies chargeable to the general budget of the European Union are concerned. Moreover, the Court of Auditors should undertake the auditing of accounts.

(36) The Agency should succeed ENISA as established by Regulation No 460/2004. Within the framework of the decision of the Representatives of the Member States, meeting in the European Council of 13 December 2003, the host Member State should maintain and develop the current practical arrangements in order to ensure the smooth and efficient operation of the Agency, having regard in particular to the Agency's cooperation with and assistance to the Commission, the Member States and their competent bodies, other Union institutions and bodies, and public and private stakeholders from throughout Europe.

(37) The Agency should be established for a limited period. Its operations should be evaluated with regard to the effectiveness of achieving the objectives and of its working practices, in order to determine the continuing validity, or otherwise, of the objectives of the Agency and, based on this, whether the duration of its operations should be further extended,

HAVE ADOPTED THIS REGULATION:

SECTION 1 SCOPE, OBJECTIVES AND TASKS

Article 1
Subject matter and Scope

1. This Regulation establishes a European Network and Information Security Agency (hereinafter 'the Agency') for the purpose of contributing to a high level of network and information security within the Union and in order to raise awareness and develop a culture of network and information security in society for the benefit of the citizens, consumers, enterprises and public sector organisations in the Union, thus contributing to the smooth functioning of the internal market.

2. The objectives and the tasks of the Agency shall be without prejudice to the competencies of the Member States regarding network and information security and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the issues relate to State security matters) and the activities of the State in areas of criminal law.

3. For the purposes of this Regulation "*network and information security*" shall mean the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via these networks and systems.

Article 2
Objectives

1. The Agency shall assist the Commission and the Member States to meet the legal and regulatory requirements of network and information security in present and future Union legislation, thus contributing to the smooth functioning of the internal market.

2. The Agency shall enhance the capability and preparedness of the Union and of Member States to prevent, detect and respond to network and information security problems and incidents.

3. The Agency shall develop and maintain a high level of expertise and shall use this expertise to stimulate broad cooperation between public and private-sector actors.

Article 3
Tasks

1. Within the purpose set out in Article 1, the Agency shall perform the following tasks:

(a) Assist the Commission, at its request or on its own initiative, on network and information security policy development by providing it with advice and opinions and with technical and socio-economic analyses, and with preparatory work for developing and updating Union legislation in the field of network and information security;

(b) Facilitate the cooperation among the Member States and between the Member States and the Commission in their efforts with a cross-border dimension to prevent, detect and respond to network and information security incidents;

(c) Assist the Member States and the European institutions and bodies in their efforts to collect, analyse and disseminate network and information security data;

(d) Regularly assess, in cooperation with the Member States and the European institutions, the state of network and information security in Europe;

(e) Support cooperation among competent public bodies in Europe, in particular supporting their efforts to develop and exchange good practices and standards;

(f) Assist the Union and the Member States in promoting the use of risk management and security good practice and standards for electronic products, systems and services;

(g) Support cooperation between public and private stakeholders on the Union level, inter alia, by promoting information sharing and awareness raising, and facilitating their efforts to develop and take up standards for risk management and for the security of electronic products, networks and services;

(h) Facilitate dialogue and exchange of good practice among public and private stakeholders on network and information security, including aspects of the fight against cybercrime; assist the Commission on policy developments that take into account network and information security aspects of the fight against cybercrime;

(i) Assist the Member States and the European institutions and bodies, at their request, in their efforts to develop network and information security detection, analysis and response capability;

(j) Support Union dialogue and cooperation with third countries and international organisations in cooperation where appropriate with the EEAS, to promote international cooperation and a global common approach to network and information security issues;

(k) Carry out tasks conferred on the Agency by Union legislative acts.

SECTION 2 ORGANISATION

Article 4
Bodies of the Agency

The Agency shall comprise:

(a) a Management Board;

(b) an Executive Director and the staff; and

(c) a Permanent Stakeholders' Group.

Article 5
Management Board

1. The Management Board shall define the general direction of the operation of the Agency and ensure that the Agency works in accordance with the rules and principles laid down in this Regulation. It shall also ensure consistency of the Agency's work with activities conducted by the Member States as well as at Union level.

2. The Management Board shall adopt its rules of procedure in agreement with the relevant Commission services.

3. The Management Board shall adopt the Agency's internal rules of operation in agreement with the relevant Commission services. These rules shall be made public.

4. The Management Board shall appoint the Executive Director in accordance with Article 10(2) and may remove the Executive Director. The Management Board shall exercise disciplinary authority over the Executive Director.

5. The Management Board shall adopt the Agency's work programme in accordance with Article 13(3) and the general report on the Agency's activities for the previous year in accordance with Article 14(2).

6. The Management Board shall adopt the financial rules applicable to the Agency. They may not depart from Commission Regulation (EC, Euratom) No 2343/2002 of 19 November 2002 on the framework Financial Regulation for the bodies referred to in Article 185 of Council Regulation (EC, Euratom) No 1605/2002 on the Financial Regulation applicable to the

general budget of the European Communities[31], unless such departure is specifically required for the Agency's operation and the Commission has given its prior consent.

7. The Management Board, in agreement with the Commission, shall adopt appropriate implementing rules, in accordance with Article 110 of the Staff Regulations.

8. The Management Board may set up working bodies composed of its members to assist it in carrying out its tasks, including drafting its decisions and monitoring the implementation thereof.

9. The Management Board may adopt the Multi-Annual Staff Policy Plan, after consulting the Commission services and having duly informed the Budgetary Authority.

Article 6
Composition of the Management Board

1. The Management Board shall be composed of one representative of each Member State, three representatives appointed by the Commission, and three representatives without the right to vote, appointed by the Commission, each of whom represent one of the following groups:

(a) the information and communication technologies industry;

(b) consumer groups;

(c) academic experts in network and information security.

2. Board members and their alternates shall be appointed on the basis of their degree of relevant experience and expertise in the field of network and information security.

3. The term of office of the representatives of the groups referred to in paragraph 1(a), (b) and (c) shall be four years. This term of office may be extended once. If a representative ceases his/her affiliation with the respective interest group, the Commission shall appoint a replacement.

Article 7
Chairperson of the Management Board

The Management Board shall elect its Chairperson and a Deputy Chairperson from among its members for a period of three years, which shall be renewable. The Deputy Chairperson shall ex officio replace the Chairperson if the latter is unable to attend to his or her duties.

Article8
Meetings

1. Meetings of the Management Board shall be convened by its Chairperson.

---

[31] OJ L 357, 31.12.2002, p. 72.

2. The Management Board shall hold an ordinary meeting twice a year. It shall also hold extraordinary meetings at the instance of the Chairperson or at the request of at least a third of its members with the right to vote.

3. The Executive Director shall take part in the meetings of the Management Board, without voting rights.

Article 9
Voting

1. The Management Board shall take its decisions by a majority of its members with the right to vote.

2. A two-thirds majority of all Management Board members with the right to vote is required for the adoption of its rules of procedure, the Agency's internal rules of operation, the budget, the annual work programme, and the appointment, extension of the term of office or removal of the Executive Director.

Article 10
Executive Director

1. The Agency shall be managed by its Executive Director, who shall be independent in the performance of his/her duties.

2. The Executive Director shall be appointed and dismissed by the Management Board. The appointment shall be done from a list of candidates proposed by the Commission for a period of five years, on grounds of merit and documented administrative and managerial skills, as well as specific competence and experience. Before appointment, the candidate selected by the Management Board may be invited to make a statement before the competent committee of the European Parliament and answer questions put by its members.

3. In the course of the nine months preceding the end of this period, the Commission shall undertake an evaluation. In the evaluation, the Commission shall assess in particular:

– the performance of the Executive Director;

– the Agency's duties and requirements in the coming years.

4. The Management Board, acting on a proposal from the Commission, taking into account the evaluation report and only in those cases where it can be justified by the duties and requirements of the Agency, may extend the term of office of the Executive Director for no more than three years.

5. The Management Board shall inform the European Parliament about its intention to extend the Executive Director's term of office. Within a month before the extension of his/her term of office, the Executive Director may be invited to make a statement before the competent committee of the Parliament and answer questions put by its members.

6. If the term of office is not extended, the Executive Director shall remain in office until the appointment of his/her successor.

7. The Executive Director shall be responsible for:

(a) the day-to-day administration of the Agency;

(b) implementing the work programme and the decisions adopted by the Management Board;

(c) ensuring that the Agency performs its activities in accordance with the requirements of those using its services, in particular with regard to the adequacy of the services provided;

(d) all specific staff matters, ensuring compliance with the general directions of the Management Board and with Management Board decisions of a general nature;

(e) developing and maintaining contact with the European institutions and bodies;

(f) developing and maintaining contact with the business community and consumers' organisations to ensure regular dialogue with relevant stakeholders;

(g) other tasks assigned to him/her by this Regulation.

8. Where necessary and within the Agency's objectives and tasks, the Executive Director may set up ad hoc Working Groups composed of experts. The Management Board shall be informed in advance. The procedures regarding in particular the composition, the appointment of the experts by the Executive Director and the operation of the ad hoc Working Groups shall be specified in the Agency's internal rules of operation.

9. The Executive Director shall make administrative support staff and other resources available to the Management Board whenever necessary.

Article 11

Permanent Stakeholders' Group

1. The Management Board shall set up a Permanent Stakeholders' Group on a proposal by the Executive Director, composed of experts representing the relevant stakeholders, such as the information and communication technologies industry, consumer groups, academic experts in network and information security, and law enforcement and privacy protection authorities.

2. Procedures for, in particular, the number, composition, and appointment of the members by the Management Board, proposal by the Executive Director and the operation of the Group shall be specified in the Agency's internal rules of operation and shall be made public.

3. The Group shall be chaired by the Executive Director.

4. The term of office of the Group's members shall be two-and-a-half years. Members of the Management Board may not be members of the Group. Commission staff shall be entitled to be present at the meetings and participate in the work of the Group.

5. The Group shall advise the Agency in the performance of its activities. The Group shall in particular advise the Executive Director on drawing up a proposal for the Agency's work programme, and on ensuring communication with the relevant stakeholders on all issues related to the work programme.

SECTION 3 OPERATION

Article 12
Work Programme

1. The Agency shall carry out its operations in accordance with its work programme, which shall contain all of its planned activities. The work programme shall not prevent the Agency from taking up unforeseen activities that fall within its objectives and tasks and within the limits of its budget. The Executive Director shall inform the Management Board of activities of the Agency that are not provided for in the work programme.

2. The Executive Director shall be responsible for drawing up the Agency's draft work programme after prior consultation with the Commission services. Before 15 March each year the Executive Director shall submit the draft work programme for the following year to the Management Board.

3. Before 30 November each year, the Management Board shall adopt the Agency's work programme for the following year in consultation with the Commission services. The work programme shall include a multi-annual outlook. The Management Board shall ensure that the work programme is consistent with the Agency's objectives and with the Union's legislative and policy priorities in the area of network and information security.

4. The work programme shall be organised in accordance with the Activity-Based Management (ABM) principle. The work programme shall be in line with the statement of estimates of the Agency's revenue and expenditure and the Agency's budget for the same financial year.

5. The Executive Director shall, following adoption by the Management Board, forward the work programme to the European Parliament, the Council, the Commission and the Member States and shall have it published.

Article 13
General report

1. Each year, the Executive Director shall submit to the Management Board a draft general report covering all the activities of the Agency in the previous year.

2. Before 31 March each year, the Management Board shall adopt the general report on the Agency's activities for the previous year.

3. The Executive Director shall, following adoption by the Management Board, transmit the Agency's general report 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 shall have it published.

Article 14

Requests to the Agency

1. Requests for advice and assistance falling within the Agency's objectives and tasks shall be addressed to the Executive Director and accompanied by background information explaining the issue to be addressed. The Executive Director shall inform the Management Board of the requests received, and in due course, of the follow-up given to the requests. If the Agency refuses a request, justification shall be given.

2. Requests referred to in paragraph 1 may be made by:

(a) the European Parliament;

(b) the Council;

(c) the Commission;

(d) any competent body appointed by a Member State, such as a national regulatory authority as defined in Article 2 of Directive 2002/21/EC.

3. The practical arrangements for applying paragraphs 1 and 2, regarding in particular submission, prioritisation, follow up and information of the Management Board on the requests to the Agency, shall be laid down by the Management Board in the Agency's internal rules of operation.

Article 15

Declaration of interest

1. The Executive Director and officials seconded by Member States on a temporary basis shall make a written declaration of commitments and a written declaration indicating the absence of any direct or indirect interest which might be considered prejudicial to their independence.

2. External experts participating in ad hoc Working Groups shall declare at each meeting any interest which might be considered prejudicial to their independence in relation to the items on the agenda and abstain from participating in the discussions on such points.

Article 16

Transparency

1. The Agency shall ensure that it carries out its activities with a high level of transparency and in accordance with Article 13 and 14.

2. The Agency shall ensure that the public and any interested parties are given objective, reliable and easily accessible information, in particular with regard to the results of its work, where appropriate. It shall also make public the declarations of interest made by the Executive Director and by officials seconded by Member States on a temporary basis, together with the declarations of interest made by experts in relation to items on the agendas of meetings of the ad hoc Working Groups.

3. The Management Board, acting on a proposal from the Executive Director, may authorise interested parties to observe the proceedings of some of the Agency's activities.

4. In its internal rules of operation, the Agency shall lay down the practical arrangements for implementing the transparency rules referred to in paragraphs 1 and 2.

Article 17
Confidentiality

1. Without prejudice to Article 14, the Agency shall not divulge to third parties information that it processes or receives for which confidential treatment has been requested.

2. Members of the Management Board, the Executive Director, the members of the Permanent Stakeholders Group, external experts participating in ad hoc Working Groups, and members of the staff of the Agency including officials seconded by Member States on a temporary basis are subject to confidentiality requirements under Article 339 of the Treaty even after their duties have ceased.

3. The Agency shall lay down in its internal rules of operation the practical arrangements for implementing the confidentiality rules referred to in paragraphs 1 and 2.

4. The Management Board may decide to allow the Agency to handle classified information. In that case the Management Board shall, in agreement with the relevant Commission services, adopt internal rules of operation applying the security principles contained in Commission Decision 2001/844/EC, ECSC, Euratom of 29 November 2001 amending its internal rules of procedure[32]. This shall cover, inter alia, provisions for the exchange, processing and storage of classified information.

Article 18
Access to documents

1. Regulation (EC) No 1049/2001 shall apply to documents held by the Agency.

2. The Management Board shall adopt arrangements for implementing Regulation (EC) No 1049/2001 within six months of the establishment of the Agency.

3. Decisions taken by the Agency pursuant to Article 8 of Regulation (EC) No 1049/2001 may form the subject of a complaint to the Ombudsman or of an action before the Court of Justice of the European Union, under Articles 228 and 263 of the Treaty respectively.

SECTION 4 FINANCIAL PROVISIONS

Article 19
Adoption of the budget

1. The revenues of the Agency shall consist of a contribution from the European Union budget, contributions from third countries participating in the work of the Agency as provided for in Article 29, and contributions from Member States.

---

[32] OJ L 317, 3.12.2001, p. 1.

2. The expenditure of the Agency shall include staff, administrative and technical support, infrastructure and operational expenses, and expenses resulting from contracts entered into with third parties.

3. By 1 March each year at the latest, the Executive Director shall draw up a draft statement of estimates of the Agency's revenue and expenditure for the following financial year, and shall forward it to the Management Board, together with a draft establishment plan.

4. Revenue and expenditure shall be in balance.

5. Each year, the Management Board, on the basis of a draft statement of estimates of revenue and expenditure drawn up by the Executive Director, shall produce a statement of estimates of revenue and expenditure for the Agency for the following financial year.

6. This statement of estimates, which shall include a draft establishment plan together with the draft work programme, shall, by 31 March at the latest, be sent by the Management Board to the Commission and the States with which the European Union has concluded agreements in accordance with Article 24.

7. This statement of estimates shall be forwarded by the Commission to the European Parliament and the Council (both hereinafter 'the budgetary authority') together with the draft general budget of the European Union.

8. On the basis of this statement of estimates, the Commission shall enter in the draft general budget of the European Union the estimates it deems necessary for the establishment plan and the amount of the subsidy to be charged to the general budget, which it shall submit to the budgetary authority in accordance with Article 314 of the Treaty.

9. The budgetary authority shall authorise the appropriations for the subsidy to the Agency.

10. The budgetary authority shall adopt the establishment plan for the Agency.

11. Together with the work programme, the Management Board shall adopt the Agency's budget. It shall become final following final adoption of the general budget of the European Union. Where appropriate, the Management Board shall adjust the Agency's budget and work programme in accordance with the general budget of the European Union. The Management Board shall forward it without delay to the Commission and the budgetary authority.

Article 20
Combating fraud

1. In order to combat fraud, corruption and other unlawful activities, Regulation (EC) No 1073/1999 of the European Parliament and of the Council of 25 May 1999 concerning investigations conducted by the European Anti-fraud Office (OLAF)[33] shall apply without restriction.

2. The Agency shall accede to the Interinstitutional Agreement of 25 May 1999 between the European Parliament and the Council of the European Union and the Commission of the European Communities concerning internal investigations by the European Anti-fraud Office

[33] OJ L 136, 31.5.1999, p. 1.

(OLAF)[34] and shall issue, without delay, the relevant provisions applicable to all the employees of the Agency.

Article 21
Implementation of the budget

1. The Executive Director shall implement the Agency's budget.

2. The Commission's internal auditor shall exercise the same powers over the Agency as over Commission departments.

3. By 1 March at the latest following each financial year, the Agency's accounting officer shall send the provisional accounts to the Commission's accounting officer together with a report on the budgetary and financial management for that financial year. The Commission's accounting officer shall consolidate the provisional accounts of the institutions and decentralised bodies in accordance with Article 128 of Council Regulation (EC, Euratom) No 1605/2002 of 25 June 2002 on the Financial Regulation applicable to the general budget of the European Communities[35] (hereinafter 'the general Financial Regulation').

4. No later than 31 March following each financial year, the Commission's accounting officer shall send the Agency's provisional accounts to the Court of Auditors, together with a report on the budgetary and financial management for that financial year. The report on the budgetary and financial management for the financial year shall also be sent to the budgetary authority.

5. On receipt of the Court of Auditor's observations on the Agency's provisional accounts, pursuant to Article 129 of the general Financial Regulation, the Executive Director shall draw up the Agency's final accounts under his/her own responsibility and send them to the Management Board for an opinion.

6. The Management Board shall deliver an opinion on the Agency's final accounts.

7. The Executive Director shall, no later than 1 July following each financial year, transmit the final accounts to the European Parliament, the Council, the Commission and the Court of Auditors, together with the Management Board's opinion.

8. The Executive Director shall publish the final accounts.

9. The Executive Director shall send the Court of Auditors a reply to its observations by 30 September at the latest. He/she shall also send this reply to the Management Board.

10. The Executive Director shall submit to the European Parliament, at the latter's request, all the information necessary for the smooth application of the discharge procedure for the financial year in question, as laid down in Article 146(3) of the general Financial Regulation.

11. The European Parliament, acting on a recommendation from the Council, shall, before 30 April of year N+2, give a discharge to the Executive Director in respect of the implementation of the budget for the year N.

---

[34] OJ L 136, 31.5.1999, p. 15.
[35] OJ L 248, 16.9.2002, p. 1.

SECTION 5 GENERAL PROVISIONS

Article 22
Legal status

1. The Agency shall be a body of the Union. It shall have legal personality.

2. In each of the Member States the Agency shall enjoy the most extensive legal capacity accorded to legal persons under their laws. It may in particular, acquire and dispose of movable and immovable property and be a party to legal proceedings.

3. The Agency shall be represented by its Executive Director.

Article 23
Staff

1. The rules and regulations applicable to officials and other staff of the European Union shall apply to the staff of the Agency, including its Executive Director.

2. In respect of the Executive Director, the Management Board shall exercise the powers conferred on the appointing authority by the Staff Regulations and on the authority entitled to conclude contracts by the Conditions of Employment.

3. In respect of the staff of the Agency, the Executive Director shall exercise the powers conferred on the appointing authority by the Staff Regulations and on the authority entitled to conclude contracts by the Conditions of Employment.

4. The Agency may employ national experts from Member States on secondment. The Agency shall lay down in its internal rules of operation the practical arrangements for implementing this.

Article 24
Privileges and immunities

The Protocol on the Privileges and Immunities of the European Communities shall apply to the Agency and its staff.

Article 25
Liability

1. The contractual liability of the Agency shall be governed by the law applicable to the contract in question.

The Court of Justice of the European Union shall have jurisdiction to give judgment pursuant to any arbitration clause contained in a contract concluded by the Agency.

2. In the case of non-contractual liability, the Agency shall, in accordance with the general principles common to the laws of the Member States, make good any damage caused by it or its servants in the performance of their duties.

The Court of Justice shall have jurisdiction in any dispute relating to compensation for such damage.

3. The personal liability of its servants towards the Agency shall be governed by the relevant conditions applying to the staff of the Agency.

Article 26
Languages

1. The provisions laid down in Regulation No 1 of 15 April 1958 determining the languages to be used in the European Economic Community[36] shall apply to the Agency. The Member States and the other bodies appointed by them may address the Agency and receive a reply in the European Union language of their choice.

2. The translation services required for the functioning of the Agency shall be provided by the Translation Centre for the Bodies of the European Union.

Article 27
Protection of personal data

When processing data relating to individuals, the Agency shall be subject to the provisions of Regulation (EC) No 45/2001.

Article 28
Participation of third countries

1. The Agency shall be open to the participation of third countries which have concluded agreements with the European Union by virtue of which they have adopted and applied Union legislation in the field covered by this Regulation.

2. Arrangements shall be made under the relevant provisions of those agreements, specifying in particular the nature, extent and manner in which these countries will participate in the Agency's work, including provisions relating to participation in the initiatives undertaken by the Agency, financial contributions and staff.

[36] OJ 17, 6.10.1958, p. 385/58. Regulation as last amended by the 1994 Act of Accession.

SECTION 6 FINAL PROVISIONS

Article 29
Review clause

1. Within three years from the date of establishment referred to in Article 34, the Commission, taking into account the views of all relevant stakeholders, shall carry out an evaluation on the basis of terms of reference agreed with the Management Board. The evaluation shall assess the impact and the effectiveness of the Agency in achieving the objectives set out in Article 2, and the effectiveness of the Agency's working practices. The Commission shall undertake the evaluation notably in order to determine whether an Agency is still an effective instrument and whether the duration of the Agency should be further extended beyond the period specified in Article 34.

2. The evaluation findings shall be forwarded by the Commission to the European Parliament and the Council and shall be made public.

3. The Management Board shall receive the evaluation and issue recommendations regarding changes to this Regulation, the Agency and its working practices to the Commission. The Management Board and the Executive Director shall take the results of the evaluation into consideration in the Agency's multi-annual planning.

Article 30
Cooperation of the host Member State

The Agency's host Member State shall ensure the best possible conditions for the smooth and efficient operation of the Agency.

Article 31
Administrative control

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

Article 32
Repeal and succession

1. Regulation (EC) No 460/2004 is repealed.

References to Regulation (EC) No 460/2004 and to ENISA shall be construed as references to this Regulation and to the Agency.

2. The Agency succeeds the Agency that was established by Regulation (EC) No 460/2004 as regards all ownership, agreements, legal obligations, employment contracts, financial commitments and liabilities.

Article 33
Duration

The Agency shall be established from […] for a period of five years.

Article 34
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*, and shall apply with effect from 14 March 2012 or from the day following that of its publication, whichever comes later.

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

Done at […],

For the European Parliament	*For the Council*
The President	*The President*

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 Concerning the European Network and Information Security Agency (ENISA)

1.2. Policy area(s) concerned in the ABM/ABB structure[37]

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**[38]

☑ 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

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.

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

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 Union, 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 Union, etc.

Empowering stakeholders – develop a culture of security and risk management by stimulating information sharing and broad cooperation between actors from the public and

[37] ABM: Activity-Based Management – ABB: Activity-Based Budgeting.

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

private sector, also for the direct benefit of citizens and developing a culture of NIS awareness.

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).

Towards collaborative implementation – facilitate collaboration in implementing NIS policies.

Fighting cybercrime – integrate NIS aspects of the fight against cybercrime in discussions and exchange of good practice among public and private stakeholders, in particular through cooperation with (past) 2nd and 3rd pillar authorities, e.g., with Europol.

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

Specific objective No

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

1.4.3. Expected result(s) and impact

The initiative is expected to bring the following economic impacts:

- increased availability of information on current and future challenges and risks for security and resilience

- non-duplication of efforts in collecting relevant information on risks, threats and vulnerabilities by each individual Member State

- increased level of informedness of policy makers when making decisions

- increased quality of NIS policy provisions in Member States due to dissemination of best practices

- economies of scale in responding to incidents at EU level

- more investments triggered by common policy objectives and standards for security and resilience at EU level

- lower operational risks for business due to higher level of security and resilience

- more coherent measures to fight cyber-crime.

The initiative is expected to create the following social impacts:

- higher trust of users in Information Society services and systems;

- increased trust in the functioning of the EU Internal market by achieving higher levels of consumer protection;

- increased exchange of information and knowledge with non-EU countries;

- better safeguarding of EU fundamental human rights through ensuring equal levels of protection of EU citizens' personal data and privacy.

The expected environmental impacts are minimal:

- 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.

1.4.4. Indicators of results and impact

The monitoring indicators per objective are as follows:

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

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.

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

See Points *1.5.1 and 1.5.2.*

1.5.4. Coherence and possible synergy with other relevant instruments

This initiative is fully coherent with the general debate on NIS and other policy initiatives that focus on the future of NIS. It is one of the main components of the Digital Agenda for Europe, the latter being a flagship initiative of the Europe 2020 strategy.

1.6. Duration and financial impact

☑ Proposal/initiative of **limited duration**

– ☑ The starting point of the 5-year extension will be 14/03/2012 or the day when the new Regulation enters into force, whichever comes later.

– ☑ Financial impact from 2012 to 2017

☐ 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) envisaged[39]

☐ **Centralised direct management** by the Commission

☑ **Centralised indirect management** with the delegation of implementation tasks to:

– ☐ executive agencies

– ☑ bodies set up by the Communities[40]

– ☐ 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)***

---

[39] 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

[40] 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 experts[41] 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 Regulation[42].

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[43]. 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 discussions[44].

---

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

42 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.

43 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.

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

2.2.2. Control method(s) envisaged

See point 2.1 and point 2.2.1, above

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 (45)	from EFTA[46] countries	from candidate countries[47]	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

* The estimated financial impact of the proposal for the period going beyond the current financial programming period 2007-2013 is not covered by the present Legislative Financial Statement. Based on the Commission's proposal for the regulation laying down the multiannual financial framework post-2013 and taking into account the conclusions of the impact assessment, the Commission will present an amended Legislative Financial Statement.

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

46 EFTA: European Free Trade Association.

47 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			1 Jan-13 Mar 2012	14 Mar-31 Dec 2012	2013	2014	2015	2016	1 Jan-13 Mar 2017	**TOTAL 14 Mar 2012 – 13 Mar 2017**
Operational appropriations										
09 02 03 02 European Network and Information Security Agency – Subsidy under Title 3	Commitments	(1)	0,454	1,976	2,470	--	--	--	--	--
	Payments	(2)	0,454	1,976	2,470	--	--	--	--	--
Administrative appropriations										
09 02 03 01 European Network and Information Security Agency – Subsidy under Titles 1 and 2		(3)	1,293	4,697	6,120	--	--	--	--	--
TOTAL appropriations under HEADING 1a	Commitments	=1 +3	1,747	6,673	8,590	--	--	--	--	--
	Payments	=2+3	1,747	6,673	8,590	--	--	--	--	--

TOTAL operational	Commitments	(4)	0,454	1,976	2,470	--	--	--	--	--

appropriations	Payments	(5)	0,454	1,976	2,470	--	--	--	--	--
TOTAL appropriations of an administrative nature financed from the envelop of specific programs		(6)	1,293	4,697	6,120	--	--	--	--	--
TOTAL appropriations under HEADING 1.a of the multiannual framework programme	Commitments	=4+ 6	1,747	6,673	8,590	--	--	--	--	--
	Payments	=5+ 6	1,747	6,673	8,590	--	--	--	--	--

EUR million (to 3 decimal places)

Heading of multiannual financial framework:	5	Administrative expenditure

		1 Jan-13 Mar 2012	14 Mar-31 Dec 2012	2013	2014	2015	2016	1 Jan-13 Mar 2017	Total
Human resources		0,085	0,342	0,427	--	--	--	--	--
Other administrative expenditure		0,002	0,013	0,015	--	--	--	--	--
TOTAL DG INFSO	Appropriations	0,087	0,355	0,442	--	--	--	--	--

TOTAL appropriations under HEADING 5 of the multiannual financial framework	(Total commitments = total payments)	0,087	0,355	0,442	--	--	--	--	--

		1 Jan-13 Mar 2012	14 Mar-31 Dec 2012	2013	2014	2015	2016	1 Jan-13 Mar 2017	Total
TOTAL appropriations under HEADINGS 1 to 5 of the multiannual financial framework	Commitments	1,834	7,028	9,032	--	--	--	--	--
	Payment	1,834	7,028	9,032	--	--	--	--	--

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 ⇩	1 Jan-13 Mar 2012	14 Mar-31 Dec 2012	2013	2014	2015	2016	1 Jan-13 Mar 2017	**TOTAL 14 Mar 2012 – 13 Mar 2017**
Coherence of regulatory approaches	0,114	0,494	0,620	--	--	--	--	--
Prevention, detection and response	0,114	0,494	0,620	--	--	--	--	--
Knowledge enhancement for policy makers	0,068	0,297	0,370	--	--	--	--	--
Empowering stakeholders	0,050	0,218	0,270	--	--	--	--	--
Sheltering Europe from international threats	0,023	0,099	0,120	--	--	--	--	--
Towards collaborative implementation	0,064	0,276	0,340	--	--	--	--	--
Fighting cyber crime	0,023	0,098	0,120	--	--	--	--	--
TOTAL COST	0,454	1,976	2,460	--	--	--	--	--

3.2.3. Estimated impact on appropriations of an administrative nature[48]

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	1 Jan-13 Mar 2012	14 Mar-31 Dec 2012	2013	2014	2015	2016	1 Jan-13 Mar 2017	**Total 14 Mar 2012 – 13 Mar 2017**
Human resources	0,085	0,342	0,427	--	--	--	--	--
Other administrative expenditure	0,002	0,013	0,015	--	--	--	--	--
TOTAL	0,087	0,355	0,442	--	--	--	--	--

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)

	1 Jan-13 Mar 2012	14 Mar-31 Dec 2012	2013	2014	2015	2016	1 Jan-13 Mar 2017	**Total 14 Mar 2012 – 13 Mar 2017**
Human resources - Title 1 – Staff	1,153	4,329	5,607	--	--	--	--	--
Other expenditure of an administrative nature – Title 2 – Functioning of the Agency	0,140	0,368	0,513	--	--	--	--	--
TOTAL	**1,293**	**4,697**	**6,120**	--	--	--	--	--

[48] 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

Each year the establishment plan of the Agency shall be explained and justified in a document called Staff Policy Plan which shall be submitted to the Budgetary Authority.

– ☐ 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

	1 Jan-13 Mar 2012	14 Mar-31 Dec 2012	2013	2014	2015	2016	1 Jan-13 Mar 2017
Establishment plan posts (officials and temporary agents)							
XX 01 01 01 (Headquarters and Commission's Representation Offices)	3,5	3,5	3,5	--	--	--	--
TOTAL	**3,5**	**3,5**	**3,5**	--	--	--	--

b) Human resources of ENISA

		1 Jan-13 Mar 2012	14 Mar-31 Dec 2012	2013	2014	2015	2016	1 Jan-13 Mar 2017
Establishment plan of ENISA (in Full Time Equivalent FTE)								
Officials or temporary staff	AD	29	31	31	--	--	--	--
	AST	15	16	16	--	--	--	--
TOTAL officials or temporary staff		44	47	47	--	--	--	--
Other staff (in FTE)								
Contract agents		13	14	14	--	--	--	--
Seconded national experts (SNE)		5	5	5	--	--	--	--
Total other staff		18	19	19	--	--	--	--
TOTAL		**62**	**66**	**66**	--	--	--	--

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

Officials and temporary agents	The Agency will continue to:

	– 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.
External personnel	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 framework[49].

EU funding after 2013 will be examined in the context of a Commission-wide debate on all proposals for the post-2013 period. This means that once the Commission has made its proposal for the next multi-annual financial framework, the Commission will present an amended legislative financial statement taking into account the conclusions of the impact assessment.

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:

Indicative appropriations in EUR million (to 3 decimal places)

	1 Jan-13 Mar 2012	14 Mar-31 Dec 2012	2013	2014	2015	2016	1 Jan-13 Mar 2017	**Total 14 Mar 2012 – 13 Mar 2017**
EFTA	0,042	0,160	0,206	--	--	--	--	--

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

[49] See points 19 and 24 of the Interinstitutional Agreement.