



EUROPEAN UNION

THE EUROPEAN PARLIAMENT

THE COUNCIL

Brussels, 23 April 2013
(OR. en)

2010/0275 (COD)

PE-CONS 4/13

TELECOM 27
MI 112
DATAPROTECT 17
JAI 120
CAB 8
INST 82
CODEC 357
OC 76

LEGISLATIVE ACTS AND OTHER INSTRUMENTS

Subject: REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE
COUNCIL concerning the European Union Agency for Network and
Information Security (ENISA) and repealing Regulation (EC) No 460/2004
COMMON GUIDELINES
Consultation deadline for Croatia: 10.5.2013

**REGULATION (EU) No .../2013
OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL**

of...

**concerning the European Union Agency for Network and Information Security (ENISA)
and repealing Regulation (EC) No 460/2004**

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

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

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee¹,

Acting in accordance with the ordinary legislative procedure,²

¹ OJ C 107, 6.4.2011, p. 58.

² Position of the European Parliament of 16 April 2013 (not yet published in the Official Journal) and decision of the Council of ...

Whereas:

- (1) Electronic communications, infrastructure and services are essential factors, both directly and indirectly, in economic and societal development. They play a vital role for society and have in themselves become ubiquitous utilities in the same way as electricity or water supplies, and also constitute vital factors in the delivery of electricity, water and other critical services. Communications networks function as social and innovation catalysts, multiplying the impact of technology and shaping consumer behaviours, business models, industries, as well as citizenship and political participation. Their disruption has the potential to cause considerable physical, social and 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, availability and confidentiality, faces continuously expanding challenges which relate inter alia to the individual components of the communications infrastructure and the software controlling those components, the infrastructure overall and the services provided through that infrastructure. This is of increasing concern to society not least because of the possibility of problems due to system complexity, malfunctions, systemic failures, accidents, mistakes and attacks that may have consequences for the electronic and physical infrastructure which delivers services critical to the well-being of European citizens.

- (2) The threat landscape is continuously changing and security incidents can undermine the trust that users have in technology, networks and services, thereby affecting their ability to exploit the full potential of the internal market and widespread use of information and communications technologies (ICT).
- (3) Regular assessment of the state of network and information security in the Union, based on reliable Union data, as well as systematic forecast of future developments, challenges and threats, both at Union and global level, is therefore important for policy makers, industry and users.
- (4) By Decision 2004/97/EC, Euratom¹, adopted at the meeting of the European Council on 13 December 2003, the representatives of the Member States 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. Following that Decision, the Greek Government determined that ENISA should have its seat in Heraklion, Crete.
- (5) On 1 April 2005, a Headquarters Agreement ("Seat Agreement") was concluded between the Agency and the host Member State.

¹ Decision 2004/97/EC, Euratom taken by common agreement between the Representatives of the Member States, meeting at Head of State or Government level, of 13 December 2003 on the location of the seats of certain offices and agencies of the European Union (OJ L 29, 3.2.2004, p. 15).

- (6) The Agency's host Member State should ensure the best possible conditions for the smooth and efficient operation of the Agency. It is imperative for the proper and efficient performance of its tasks, for staff recruitment and retention and to enhance the efficiency of networking activities that the Agency be based in an appropriate location, among other things providing appropriate transport connections and facilities for spouses and children accompanying members of staff of the Agency. The necessary arrangements should be laid down in an agreement between the Agency and the host Member State concluded after obtaining the approval of the Management Board of the Agency.
- (7) In order to improve the operational efficiency of the Agency, the Agency has established a branch office in the metropolitan area of Athens, which should be maintained with the agreement and support of the host Member State, and where the operational staff of the Agency should be located. Staff primarily engaged in the administration of the Agency (including the Executive Director), finance, desk research and analysis, IT and facilities management, human resources, training, and communications and public affairs, should be based in Heraklion.
- (8) The Agency has the right to determine its own organisation in order to ensure the proper and efficient performance of its tasks, while respecting the provisions on the seat and Athens branch office laid down in this Regulation. In particular, in order to carry out tasks involving interaction with key stakeholders such as the Union institutions, the Agency should make the necessary practical arrangements to enhance such operational efficiency.

- (9) In 2004 the European Parliament and the Council adopted Regulation (EC) No 460/2004¹ establishing ENISA 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 Regulation (EC) No 1007/2008² extending the mandate of the Agency until March 2012. Regulation (EC) No 580/2011³ extends the mandate of the Agency until 13 September 2013.
- (10) The Agency should succeed ENISA as established by Regulation (EC) 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 further develop the current practical arrangements in order to ensure the smooth and efficient operation of the Agency, including its Athens branch office, and facilitate the recruitment and retention of highly qualified staff.

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 establishing the European Network and Information Security Agency as regards its duration (OJ L 293, 31.10.2008, p. 1).

³ Regulation (EU) No 580/2011 of the European Parliament and of the Council of 8 June 2011 amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration (OJ L 165, 24.6.2011, p. 3).

- (11) Since ENISA 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. This Regulation aims to strengthen the Agency to successfully contribute to the efforts of the Union institutions and the Member States to develop a European capacity to cope with network and information security challenges.
- (12) 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 Union institutions and the Member States. The heterogeneous application of those requirements can lead to inefficiencies and can create obstacles to the internal market. This makes a centre of expertise at Union level necessary, providing guidance, advice and assistance on issues related to network and information security, which may be relied upon by the Union institutions and the Member States. The Agency can respond to those needs by developing and maintaining a high level of expertise and assisting the Union institutions, the Member States, and the business community in order to help them meet the legal and regulatory requirements of network and information security and to determine and address network and information security issues, thereby contributing to the proper functioning of the internal market.

- (13) The Agency should carry out the tasks conferred on it by legal acts of the Union in the field of electronic communications and, in general, contribute to an enhanced level of security of electronic communications as well as of privacy and personal data protection by, among other things, providing expertise and advice, and promoting the exchange of best practices, and offering policy suggestions.
- (14) 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)¹ requires that providers of public electronic communications networks or publicly available electronic communications services take appropriate measures to safeguard the integrity and security thereof, and introduces an obligation for the national regulatory authorities, where appropriate, to inform, inter alia, the Agency about any security breach or integrity loss that has had a significant impact on the operation of networks or services and to submit to the Commission and to the Agency an annual summary report on the notifications received and the action taken.
- Directive 2002/21/EC further calls on the Agency, by providing opinions, to contribute to the harmonisation of appropriate technical and organisational security measures.

¹ OJ L 108, 24.4.2002, p. 33.

- (15) 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)¹ 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 that the confidentiality of the communications and related traffic data be maintained. 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 data² 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.

¹ OJ L 201, 31.7.2002, p. 37.

² OJ L 281, 23.11.1995, p. 31.

- (16) The Agency should contribute to a high level of network and information security, to better protection of privacy and personal data, and to the development and promotion of a culture of network and information security for the benefit of citizens, consumers, businesses and public sector organisations in the Union, thus contributing to the proper functioning of the internal market. In order to achieve this, the necessary budgetary funds should be allocated to the Agency.
- (17) Given the increasing significance of electronic networks and communications, which now constitute the backbone of the European economy, and the actual size of the digital economy, the financial and human resources allocated to the Agency should be increased to reflect its enhanced role and tasks, and its critical position in defending the European digital ecosystem.
- (18) The Agency should operate as a point of reference establishing trust and 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 its tasks. The Agency should build on national and Union efforts and therefore carry out its tasks in full cooperation with the Union institutions, bodies, offices and agencies and the Member States, and be open to contacts with industry and other relevant stakeholders. In addition, the Agency should build on input from and cooperation with the private sector, which plays an important role in securing electronic communications, infrastructures and services.

- (19) 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 Commission and, where appropriate, with relevant stakeholders, the state of network and information security in the Union. The Agency should ensure coordination and collaboration with the Union institutions, bodies, offices and agencies and Member States, and enhance cooperation between stakeholders in Europe, in particular by involving in its activities competent national and Union bodies and high-level private sector experts in relevant areas, in particular providers of electronic communications networks and services, network equipment manufacturers and software vendors, taking into account that network and information systems comprise combinations of hardware, software and services. The Agency should provide assistance to the Union institutions and to 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.
- (20) Network and information security strategies made public by a Union institution, body, office or agency or a Member State should be provided to the Agency for its information and to avoid duplication of effort. The Agency should analyse the strategies and promote their presentation in a format that facilitates comparability. It should make the strategies and its analyses available to the public through electronic means.

- (21) The Agency should assist the Commission by means of advice, opinions and analyses on all the Union matters related to policy development in the area of network and information security, including Critical Information Infrastructure Protection and resilience. The Agency should also assist the Union institutions, bodies, offices and agencies and where relevant, the Member States, at their request, in their efforts to develop network and information security policy and capability.
- (22) The Agency should take full account of the ongoing research, development, and technological assessment activities, in particular those carried out by the various Union research initiatives to advise the Union institutions, bodies, offices and agencies and where relevant, the Member States, at their request, on research needs in the area of network and information security.
- (23) The Agency should assist the Union institutions, bodies, offices and agencies as well as the Member States in their efforts to build and enhance cross-border capability and preparedness to prevent, detect 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 Commission and other Union institutions, bodies, offices and agencies and the Member States. To this end, the Agency should support the Member States in their continuous efforts to improve their response capability and to organise and run European exercises on security incidents and, at the request of a Member State, national exercises.

- (24) 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, with statistical bodies and others, collect relevant information. Furthermore, the Agency should assist the Union institutions, bodies, offices and agencies and the Member States and in their efforts to collect, analyse and disseminate network and information security data. The collection of appropriate statistical information and data needed to carry out analyses of the risks to the security and resilience of electronic communications, infrastructure and services should take place on the basis of the information provided by the Member States and the Agency's insight to the Union institutions' ICT infrastructures in accordance with Union provisions and national provisions in compliance with Union law. On the basis of that information, the Agency should maintain awareness of the latest state of network and information security and related trends in the Union for the benefit of Union institutions, bodies, offices and agencies and the Member States.
- (25) In performing its tasks, the Agency should facilitate cooperation between the Union and the Member States to improve awareness of the state of network and information security in the Union.

- (26) The Agency should facilitate cooperation among the Member States' competent independent regulatory authorities, in particular supporting the development, promotion and exchange of best practices and standards for education programmes and awareness-raising schemes. Increased information exchange between Member States will facilitate such action. The Agency should contribute towards raising the awareness of individual users of electronic communications, infrastructure and services, including by assisting Member States, where they have chosen to use the public interest information platform provided for in Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive)¹, to produce relevant public interest information regarding network and information security, and also by assisting in the development of such information to be included with the supply of new devices intended for use on public communications networks. The Agency should also support cooperation between stakeholders at Union level, partly by promoting information sharing, awareness-raising campaigns and education and training programmes.
- (27) The Agency should, inter alia, assist the relevant Union institutions, bodies, offices and agencies and the Member States in public education campaigns to end users, aiming at promoting safer individual online behaviour and raising awareness of potential threats in cyberspace, including cybercrimes such as phishing attacks, botnets, financial and banking fraud, as well as promoting basic authentication and data protection advice.

¹ OJ L 108, 24.4.2002, p. 51.

- (28) To ensure that it fully achieves its objectives, the Agency should liaise with relevant bodies, including those dealing with cybercrime such as Europol, and privacy protection authorities to exchange know-how and best practices and provide advice on network and information security aspects that might have an impact on their work. The Agency should aim to achieve synergies between the efforts of those bodies and its own efforts to promote advanced network and information security. Representatives of national and Union law enforcement and privacy protection authorities should be eligible to be represented in the Agency's Permanent Stakeholders Group. In liaising with law enforcement bodies regarding network and information security aspects that might have an impact on their work, the Agency should respect existing channels of information and established networks.
- (29) The Commission has launched a European Public-Private Partnership for Resilience as a flexible Union-wide cooperation platform for resilience of ICT infrastructure, in which the Agency should play a facilitating role, bringing together stakeholders to discuss public policy priorities, economic and market dimensions of challenges and measures for the resilience of ICT.
- (30) In order to promote network and information security and its visibility, the Agency should facilitate cooperation among the Member States' competent public bodies, in particular by supporting the development and exchange of best practices and awareness-raising schemes and by enhancing their outreach activities. The Agency should also support cooperation between stakeholders and the Union institutions, partly by promoting information sharing and awareness-raising activities.

- (31) In order to enhance an advanced level of network and information security in the Union, the Agency should promote cooperation and the exchange of information and best practices between relevant organisations, such as Computer Security Incident Response Teams (CSIRTs) and Computer Emergency Response Teams (CERTs).
- (32) A Union system of properly functioning CERTs should constitute a cornerstone of the Union's network and information security infrastructure. The Agency should support Member State CERTs and the Union CERT in the operation of a network of CERTs, including the members of the European Governmental CERTs Group. In order to assist in ensuring that each of the CERTs has sufficiently advanced capabilities and that those capabilities correspond as far as possible to the capabilities of the most developed CERTs, the Agency should promote the establishment and operation of a peer-review system. Furthermore, the Agency should promote and support cooperation between the relevant CERTs in the event of incidents, attacks on or disruptions of networks or infrastructure managed or protected by the CERTs and involving or potentially involving at least two CERTs.

- (33) Efficient network and information 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 regarding how to apply them efficiently. Promoting and developing best practices 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 the Union. To this end, the Agency should support cooperation between stakeholders at Union level, facilitating their efforts relating to the establishment and take-up of European and international standards for risk management and for measurable security of electronic products, systems, networks and services which, together with software, comprise the network and information systems.
- (34) Where appropriate and useful for fulfilling its objectives and tasks, the Agency should share experience and general information with Union institutions, bodies, offices and agencies dealing with network and information security. The Agency should contribute to identifying research priorities, at Union level, in the areas of network resilience and network and information security, and should convey knowledge of industry needs to relevant research institutions.

- (35) The Agency should encourage Member States and service providers to raise their general security standards so that all internet users take the necessary steps to ensure their own personal cyber security.
- (36) Network and information security problems are global issues. There is a need for closer international cooperation to improve security standards, including the definition of common norms of behaviour and codes of conduct, and information sharing, promoting swifter international collaboration in response to, as well as a common global approach to, network and information security issues. To that end, the Agency should support further Union involvement and cooperation with third countries and international organisations by providing, where appropriate, the necessary expertise and analysis to the relevant Union institutions, bodies, offices and agencies.

- (37) The Agency should operate in accordance with the principle of subsidiarity, ensuring an appropriate degree of coordination between the Member States on matters relating to network and information security and improving the effectiveness of national policies, thus adding value to them and in accordance with the principle of proportionality, not going beyond what is necessary in order to achieve the objectives set out by this Regulation. The exercise of the Agency's tasks should reinforce, but not interfere with, the competences, nor should it pre-empt, impede or overlap with the relevant powers and tasks, of the national regulatory authorities as set out in the Directives relating to electronic communications networks and services, as well as those of the Body of European Regulators for Electronic Communications (BEREC) established by Regulation (EC) No 1211/2009¹ and the Communications Committee referred to in Directive 2002/21/EC, of the European standardisation bodies, the national standardisation bodies and the Standing Committee as set out in Directive 98/34/EC² and the independent supervisory authorities of the Member States as set out in Directive 95/46/EC.
- (38) It is necessary to implement certain principles regarding the governance of the Agency in order to comply with the Joint Statement and Common Approach agreed upon in July 2012 by the Inter-Institutional Working Group on EU decentralised agencies, the purpose of which statement and approach is to streamline the activities of agencies and improve their performance.

¹ Regulation (EC) No 1211/2009 of the European Parliament and of the Council of 25 November 2009 establishing the Body of European Regulators for Electronic Communications (BEREC) and the Office (OJ L 337, 18.12.2009, p. 1).

² 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 (OJ L 204, 21.7.1998, p. 37).

- (39) The Joint Statement and Common Approach should also be reflected, as appropriate, in the Agency's Work Programmes, evaluations of the Agency, and the Agency's reporting and administrative practice.
- (40) In order for the Agency to function properly, the Commission and the Member States should ensure that persons to be appointed to the Management Board have appropriate professional expertise. The Commission and the Member States should also make efforts to limit the turnover of their respective Representatives on the Management Board, in order to ensure continuity in its work.
- (41) It is essential that the Agency establish and maintain a reputation for impartiality, integrity and high professional standards. Accordingly, the Management Board should adopt comprehensive rules covering the entire Agency for the prevention and management of conflicts of interest.
- (42) Given the unique circumstances of the Agency and the difficult challenges facing it, the organisational structure of the Agency should be simplified and strengthened to ensure greater efficiency and effectiveness. Therefore, among other things, an Executive Board should be established in order to enable the Management Board to focus on issues of strategic importance.
- (43) The Management Board should appoint an Accounting Officer in accordance with rules adopted under Regulation (EU, Euratom) No 966/2012¹ (the 'Financial Regulation').

¹ Regulation (EU, Euratom) No 966/2012 of the European Parliament and of the Council of 25 October 2012 on the financial rules applicable to the general budget of the Union and repealing Council Regulation (EC, Euratom) No 1605/2002 (OJ L 298, 26.10.2012, p. 1).

- (44) In order to ensure that the Agency is effective, the Member States and the Commission should be represented on the 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 powers necessary 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, appoint the Executive Director, decide on the extension of the Executive Director's term of office after obtaining the views of the European Parliament, and decide on the termination thereof. The Management Board should set up an Executive Board to assist it with its administrative and budgetary tasks.
- (45) The smooth functioning of the Agency requires that its Executive Director be appointed on grounds of merit and documented administrative and managerial skills, as well as competence and experience relevant for network and information security, and that the duties of the Executive Director be carried out 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, and take all necessary steps to ensure the proper execution of the work programme of the Agency. The Executive Director should prepare an annual report to be submitted to the Management Board, draw up a draft statement of estimates of revenue and expenditure for the Agency, and implement the budget.

- (46) The Executive Director should have the option of setting up ad hoc Working Groups to address specific matters, in particular of a scientific, technical or legal or socio-economic nature. In setting up 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 regarding security challenges posed by the developing information society. The Executive Director should ensure that the ad hoc Working Groups' members are selected according to the highest standards of expertise, taking due account of a representative balance, as appropriate according to the specific issues in question, between the public administrations of the Member States, the Union institutions and the private sector, including industry, users, and academic experts in network and information security. The Executive Director should be able, as appropriate, to 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 rules adopted under the Financial Regulation.
- (47) 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 stakeholders and bring them to the attention of the Agency. The Executive Director should, where appropriate and according to the agenda of the meetings, be able to invite representatives of the European Parliament and other relevant bodies to take part in meetings of the Group.

- (48) Since there is provision for ample representation of stakeholders in the Permanent Stakeholders Group, and that group is to be consulted in particular regarding the draft Work Programme, there is no longer any need to provide for representation of stakeholders in the Management Board.
- (49) The Agency should apply the relevant Union provisions concerning public access to documents as set out in Regulation (EC) No 1049/2001¹ of the European Parliament and of the Council. The information processed by the Agency for purposes relating to its internal functioning as well as the information processed in carrying out its tasks should be subject to 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 data².
- (50) The Agency should comply with the provisions applicable to the Union institutions, and with national legislation regarding the treatment of sensitive documents.

¹ 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).

² OJ L 8, 12.1.2001, p. 1.

- (51) In order to guarantee the full autonomy and independence of the Agency and to enable it to perform additional and new tasks, including unforeseen emergency tasks, the Agency should be granted a sufficient and autonomous budget whose revenue comes primarily from a contribution from the Union and contributions from third countries participating in the Agency's work. The majority of the Agency staff should be directly engaged in the operational implementation of the Agency's mandate. 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 should remain applicable as far as any subsidies chargeable to the general budget of the European Union are concerned. Moreover, the Court of Auditors should audit the Agency's accounts to ensure transparency and accountability.
- (52) In view of the continually changing threat landscape and the evolution of Union policy on network and information security, and in order to align to the multiannual financial framework, the duration of the mandate of the Agency should be set to a limited period of seven years with a possibility of extending the duration.
- (53) The Agency's operations should be evaluated independently. The evaluation should have regard to the Agency's effectiveness in achieving its objectives, its working practices and the relevance of its tasks, in order to determine the continuing validity, or otherwise, of the objectives of the Agency and, based thereon, whether and for what period the duration of its mandate should be further extended.

- (54) If, towards the end of the duration of the mandate of the Agency, the Commission has not introduced a proposal for an extension of the mandate, the Agency and the Commission should take the relevant measures, addressing in particular issues relating to staff contracts and budget arrangements.
- (55) Since the objective of this Regulation, namely to establish a European Union Agency for Network and Information Security 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 and promote a culture of network and information security in society for the benefit of citizens, consumers, enterprises and public sector organisations in the Union, thus contributing to the establishment and proper functioning of the internal market, cannot be sufficiently achieved by the Member States and can therefore be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality, as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.
- (56) Regulation (EC) No 460/2004 should be repealed.
- (57) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 and adopted his opinion on 20 December 2010¹,

HAVE ADOPTED THIS REGULATION:

¹ OJ C 101, 1.4.2011, p. 20.

SECTION 1

SCOPE OBJECTIVES AND TASKS

Article 1

Subject matter and Scope

1. This Regulation establishes a European Union Agency for Network and Information Security (ENISA, hereinafter "the Agency") to undertake the tasks assigned to it for the purpose of contributing to a high level of network and information security within the Union and in order to raise awareness of network and information security and to develop and promote a culture, of network and information security in society for the benefit of citizens, consumers, enterprises and public sector organisations in the Union, thus contributing to the establishment and proper functioning of the internal market.
2. The objectives and the tasks of the Agency shall be without prejudice to the competences of the Member States regarding network and information security and in any case to activities concerning public security, defence, national security (including the economic well-being of the state when the issues relate to national security matters) and the activities of the state in areas of criminal law.
3. For the purposes of this Regulation "network and information security" means 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 those networks and systems.

Article 2
Objectives

1. The Agency shall develop and maintain a high level of expertise.
2. The Agency shall assist the Union institutions, bodies, offices and agencies in developing policies in network and information security.
3. The Agency shall assist the Union institutions, bodies, offices and agencies and the Member States in implementing the policies necessary to meet the legal and regulatory requirements of network and information security under existing and future legal acts of the Union, thus contributing to the proper functioning of the internal market.
4. The Agency shall assist the Union and the Member States in enhancing and strengthening their capability and preparedness to prevent, detect and respond to network and information security problems and incidents.
5. The Agency shall use its expertise to stimulate broad cooperation between actors from the public and private sectors.

Article 3

Tasks

1. Within the purpose set out in Article 1, and in order to attain the objectives set out in Article 2, whilst respecting Article 1(2), the Agency shall perform the following tasks:
 - (a) support the development of Union policy and law, by:
 - (i) assisting and advising on all matters relating to Union network and information security policy and law;
 - (ii) providing preparatory work, advice and analyses relating to the development and update of Union network and information security policy and law;
 - (iii) analysing publicly available network and information security strategies and promoting their publication;
 - (b) support capability building by:
 - (i) supporting Member States, at their request, in their efforts to develop and improve the prevention, detection and analysis of and the capability to respond to network and information security problems and incidents, and providing them with the necessary knowledge;

- (ii) promoting and facilitating voluntary cooperation among the Member States and between the Union institutions, bodies, offices and agencies and the Member States in their efforts to prevent, detect and respond to network and information security problems and incidents where these have an impact across borders;
- (iii) assisting the Union institutions, bodies, offices and agencies in their efforts to develop the prevention, detection and analysis of and the capability to respond to network and information security problems and incidents, in particular by supporting the operation of a Computer Emergency Response Team (CERT) for them;
- (iv) supporting the raising of the level of capabilities of national/governmental and Union CERTs, including by promoting dialogue and exchange of information, with a view to ensuring that, with regard to the state of the art, each CERT meets a common set of minimum capabilities and operates according to best practices;
- (v) supporting the organisation and running of Union network and information security exercises, and, at their request, advising Member States on national exercises;

- (vi) assisting the Union institutions, bodies, offices and agencies and the Member States in their efforts to collect, analyse and, in line with Member States' security requirements, disseminate relevant network and information security data; and on the basis of information provided by the Union institutions, bodies, offices and agencies and the Member States in accordance with provisions of Union law and national provisions in compliance with Union law, maintaining the awareness, on the part of the Union institutions, bodies, offices and agencies as well as the Member States of the latest state of network and information security in the Union for their benefit;
 - (vii) supporting the development of a Union early warning mechanism that is complementary to Member States' mechanisms;
 - (viii) offering network and information security training for relevant public bodies, where appropriate in cooperation with stakeholders;
- (c) support voluntary co-operation among competent public bodies, and between stakeholders, including universities and research centres in the Union, and support awareness raising, inter alia, by:
- (i) promoting cooperation between national and governmental CERTs or Computer Security Incident Response Teams (CSIRTs), including the CERT for the Union institutions, bodies, offices and agencies;
 - (ii) promoting the development and sharing of best practices with the aim of attaining an advanced level of network and information security;

- (iii) facilitating dialogue and efforts to develop and exchange best practices;
 - (iv) promoting best practices in information sharing and awareness raising;
 - (v) supporting the Union institutions, bodies, offices and agencies and, at their request, the Member States and their relevant bodies in organising awareness raising, including at the level of individual users, and other outreach activities to increase network and information security and its visibility by providing best practices and guidelines;
- (d) support research and development and standardisation, by:
- (i) facilitating the establishment and take-up of European and international standards for risk management and for the security of electronic products, networks and services;
 - (ii) advising the Union and the Member States on research needs in the area of network and information security with a view to enabling effective responses to current and emerging network and information security risks and threats, including with respect to new and emerging information and communications technologies, and to using risk-prevention technologies effectively;
- (e) cooperate with Union institutions, bodies, offices and agencies, including those dealing with cybercrime and the protection of privacy and personal data, with a view to addressing issues of common concern, including by:
- (i) exchanging know-how and best practices;

- (ii) providing advice on relevant network and information security aspects in order to develop synergies;
 - (f) contribute to the Union's efforts to cooperate with third countries and international organisations to promote international cooperation on network and information security issues, including by:
 - (i) being engaged, where appropriate, as an observer and in the organisation of international exercises, and analysing and reporting on the outcome of such exercises;
 - (ii) facilitating exchange of best practices of relevant organisations;
 - (iii) providing the Union institutions with expertise.
2. Union institutions, bodies, offices and agencies and Member State bodies may request advice from the Agency in the event of breach of security or loss of integrity with a significant impact on the operation of networks and services.
 3. The Agency shall carry out tasks conferred on it by legal acts of the Union.
 4. The Agency shall express independently its own conclusions, guidance and advice on matters within the scope and objectives of this Regulation.

SECTION 2 ORGANISATION

Article 4

Composition of the Agency

1. The Agency shall comprise:
 - (a) a Management Board;
 - (b) an Executive Director and staff; and
 - (c) a Permanent Stakeholders' Group.

2. In order to contribute to enhancing effectiveness and efficiency of the operation of the Agency, the Management Board shall establish an Executive Board.

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 the Agency's annual and multiannual work programme.
3. The Management Board shall adopt an annual report on the Agency's activities and send it, by 1 July of the following year, to the European Parliament, the Council, the Commission and the Court of Auditors. The annual report shall include the accounts and describe how the Agency has met its performance indicators. The annual report shall be made public.
4. The Management Board shall adopt an anti-fraud strategy that is proportionate to the fraud risks having regard to a cost-benefit analysis of the measures to be implemented.
5. The Management Board shall ensure adequate follow-up to the findings and recommendations resulting from investigations of the European Anti-fraud Office (OLAF) and the various internal or external audit reports and evaluations.
6. The Management Board shall adopt rules for the prevention and management of conflicts of interest.
7. The Management Board shall exercise, with respect to the staff of the Agency, the powers conferred by the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Union (hereinafter referred to as the "Staff Regulations" and the "Conditions of Employment of Other Servants"), laid down in Regulation (EEC, Euratom, ECSC) No 259/68¹ on the Appointing Authority and on the Authority Empowered to Conclude Contract of Employment, respectively.

¹ OJ L 56, 4.3.1968, p. 1.

The Management Board shall adopt, in accordance with the procedure under Article 110 of the Staff Regulations, a decision based on Article 2(1) of the Staff Regulations and on Article 6 of the Conditions of Employment of Other Servants delegating the relevant Appointing Authority powers to the Executive Director. The Executive Director may sub-delegate those powers.

Where exceptional circumstances so require, the Management Board may revoke the delegation of the powers of the Appointing Authority to the Executive Director and those sub-delegated by the Executive Director. In such a case, the Management Board may delegate them, for a limited period to one of its members or to a staff member other than the Executive Director.

8. The Management board shall adopt appropriate rules implementing the Staff Regulations and the Conditions of Employment of Other Servants in accordance with the procedure provided for in Article 110 of the Staff Regulations.
9. The Management Board shall appoint the Executive Director and may extend his term of office or remove him from office in accordance with Article 24 of this Regulation.
10. The Management Board shall adopt the rules of procedure for itself and for the Executive Board after consulting the Commission. The rules of procedure shall provide for expedited decisions through either written procedure or by remote conferencing.

11. The Management Board shall adopt the Agency's internal rules of operation after consulting the Commission services. Those rules shall be made public.
12. 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 Communities¹, unless such departure is specifically required for the Agency's operation and the Commission has given its prior consent.
13. The Management Board shall adopt a Multiannual Staff Policy Plan, after consulting the Commission services and having duly informed the European Parliament and the Council.

Article 6

Composition of the Management Board

1. The Management Board shall be composed of one representative of each Member State, and two representatives appointed by the Commission. All representatives shall have voting rights.
2. Each member of the Management Board shall have an alternate to represent the member in their absence.

¹ OJ L 357, 31.12.2002, p. 72.

3. Members of the Management Board and their alternates shall be appointed in light of their knowledge of the Agency's tasks and objectives, taking into account the managerial, administrative and budgetary skills relevant to fulfil the tasks listed in Article 5. The Commission and the Member States should make efforts to limit turnover of their representatives in the Management Board, in order to ensure continuity of that board's work. The Commission and the Member States shall aim to achieve a balanced representation between men and women on the Management Board.
4. The term of office of members of the Management Board and of their alternates shall be four years. That term shall be renewable.

Article 7

Chairperson of the Management Board

1. 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.
2. The Chairperson may be invited to make a statement before the relevant committee(s) of the European Parliament and answer Members' questions.

Article 8

Meetings

1. Meetings of the Management Board shall be convened by its Chairperson.
2. The Management Board shall hold an ordinary meeting at least once a year. It shall also hold extraordinary meetings at the request of the Chairperson or of at least a third of its members.
3. The Executive Director shall take part, without voting rights, in the meetings of the Management Board.

Article 9

Voting

1. The Management Board shall take its decisions by an absolute majority of its members.
2. A two-thirds majority of all Management Board members shall be required for the adoption of the Management Board's rules of procedure, the Agency's internal rules of operation, the budget, the annual and multiannual work programme, the appointment, extension of the term of office or removal of the Executive Director, and the designation of the Chairperson of the Management Board.

Article 10
Executive Board

1. The Management Board shall be assisted by an Executive Board.
2. The Executive Board shall prepare decisions to be adopted by the Management Board on administrative and budgetary matters only.

Together with the Management Board, it shall ensure adequate follow-up to the findings and recommendations stemming from investigations of OLAF and the various internal or external audit reports and evaluations.

Without prejudice to the responsibilities of the Executive Director, as set out in Article 11, the Executive Board shall assist and advise the Executive Director in implementing the decisions of the Management Board on administrative and budgetary matters.

3. The Executive Board shall be made up of five members appointed from among the members of the Management Board amongst whom the Chairperson of the Management Board, who may also chair the Executive Board, and one of the representatives of the Commission.
4. The term of office of members of the Executive Board shall be the same as that of members of the Management Board set out in Article 6(4).
5. The Executive Board shall meet at least once every three months. The chairperson of the Executive Board shall convene additional meetings at the request of its members.

Article 11
Duties of the 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 responsible for:
 - (a) the day-to-day administration of the Agency;
 - (b) implementing the decisions adopted by the Management Board;
 - (c) after consultation with the Management Board, preparing the annual work programme and the multiannual work programme and submitting them to the Management Board after consulting the Commission;
 - (d) implementing the annual work programme and the multiannual work programme and reporting to the Management Board thereon;
 - (e) preparing the annual report on the Agency's activities and presenting it to the Management Board for approval;
 - (f) preparing an action plan following-up on the conclusions of the retrospective evaluations and reporting on progress every two years to the Commission;

- (g) protecting the financial interests of the Union by the application of preventive measures against fraud, corruption and any other illegal activities, by effective checks and, if irregularities are detected, by the recovery of the amounts wrongly paid and, where appropriate, by effective, proportionate and dissuasive administrative and financial penalties;
- (h) preparing an anti-fraud strategy for the Agency and presenting it to the Management Board for approval;
- (i) 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;
- (j) developing and maintaining contact with the Union institutions, bodies, offices and agencies;
- (k) developing and maintaining contact with the business community and consumers' organisations to ensure regular dialogue with relevant stakeholders;
- (l) other tasks assigned to the Executive Director by this Regulation.

3. Where necessary and within the Agency's objectives and tasks, the Executive Director may set up ad hoc Working Groups composed of experts, including from the Member States' competent authorities. 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.
4. The Executive Director shall make administrative support staff and other resources available to the Management Board and the Executive Board whenever necessary.

Article 12

Permanent Stakeholders' Group

1. The Management Board, acting on a proposal by the Executive Director, shall set up a Permanent Stakeholders' Group composed of recognised experts representing the relevant stakeholders, such as the ICT industry, providers of electronic communications networks or services available to the public, consumer groups, academic experts in network and information security, and representatives of national regulatory authorities notified under Directive 2002/21/EC as well as of law enforcement and privacy protection authorities.
2. Procedures for, in particular, the number, composition, and the appointment of the members of the Permanent Stakeholders' Group by the Management Board, the 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 Permanent Stakeholders' Group shall be chaired by the Executive Director or by any person the Executive Director appoints on a case-by-case basis.
4. The term of office of the Permanent Stakeholders' Group's members shall be two-and-a-half years. Members of the Management Board may not be members of the Permanent Stakeholders' Group. Experts from the Commission and the Member States shall be entitled to be present at the meetings of the Permanent Stakeholders' Group and to participate in its work. Representatives of other bodies deemed relevant by the Executive Director, who are not members of the Permanent Stakeholders' Group, may be invited to be present at the meetings of the Permanent Stakeholders' Group and to participate in its work.
5. The Permanent Stakeholders' Group shall advise the Agency in respect of the performance of its activities. It 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 13

Work Programme

1. The Agency shall carry out its operations in accordance with its annual and multiannual work programme, which shall contain all of its planned activities.
2. The work programme shall include tailored performance indicators allowing for effective assessment of the results achieved in terms of objectives.
3. The Executive Director shall be responsible for drawing up the Agency's draft work programme after prior consultation with the Commission services. By 15 March each year the Executive Director shall submit the draft work programme for the following year to the Management Board.
4. By 30 November each year, the Management Board shall adopt the Agency's work programme for the following year, after having received the opinion of the Commission. The work programme shall include a multiannual 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.

5. The work programme shall be organised in accordance with the activity-based management 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.
6. 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 publish it. At the invitation of the relevant committee of the European Parliament, the Executive Director shall present and hold an exchange of views on the adopted annual work programme.

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 and Executive Board of the requests received, the potential resource implications, and, in due course, of the follow-up to the requests. If the Agency refuses a request, it shall give a justification.

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 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 to the Management and Executive 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. Members of the Management Board, the Executive Director and officials seconded by Member States on a temporary basis shall each make a declaration of commitments and a declaration indicating the absence or presence of any direct or indirect interest which might be considered prejudicial to their independence. The declarations shall be accurate and complete, made annually in writing and updated whenever necessary.

2. Members of the Management Board, the Executive Director, and external experts participating in ad hoc Working Groups shall each accurately and completely declare, at the latest at the start of each meeting, any interest which might be considered prejudicial to their independence in relation to the items on the agenda, and shall abstain from participating in the discussion of and voting upon such points.
3. The Agency shall lay down, in its internal rules of operation, the practical arrangements for the rules on declarations of interest referred to in paragraphs 1 and 2.

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 17 and 18.
2. The Agency shall ensure that the public and any interested parties are given appropriate, objective, reliable and easily accessible information, in particular with regard to the results of its work. It shall also make public the declarations of interest made in accordance with Article 15.
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. The Agency shall lay down, in its internal rules of operation, the practical arrangements for implementing the transparency rules referred to in paragraphs 1 and 2.

Article 17
Confidentiality

1. Without prejudice to Article 18, the Agency shall not divulge to third parties information that it processes or receives in relation to which a reasoned request for confidential treatment, in whole or in part, has been made.
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 shall comply with the confidentiality requirements under Article 339 of the Treaty on the Functioning of the European Union (TFEU), 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. If required for the performance of the Agency's tasks, the Management Board shall decide to allow the Agency to handle classified information. In that case the Management Board shall, in agreement with the Commission services, adopt internal rules of operation applying the security principles set out in Commission Decision 2001/844/EC, ECSC, Euratom of 29 November 2001 amending its internal rules of procedure¹. Those rules shall cover, inter alia, provisions for the exchange, processing and storage of classified information.

¹ OJ L 317, 3.12.2001, p. 1.

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 be the subject of a complaint to the Ombudsman under Article 228 TFEU or of an action before the Court of Justice of the European Union under Article 263 TFEU.

SECTION 4

FINANCIAL PROVISIONS

Article 19

Adoption of the budget

1. The revenues of the Agency shall consist of a contribution from the Union budget, contributions from third countries participating in the work of the Agency as provided for in Article 30, and voluntary contributions from Member States in money or in kind. Member States that provide voluntary contributions may not claim any specific right or service as a result thereof.
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, 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 shall, on the basis of a draft statement of estimates of revenue and expenditure drawn up by the Executive Director, produce a statement of estimates of revenue and expenditure for the Agency for the following financial year.

6. The Management Board shall, by 31 March each year, send that statement of estimates, which shall include a draft establishment plan together with the draft work programme, to the Commission and the third countries with which the Union has concluded agreements in accordance with Article 30.
7. The Commission shall forward that statement of estimates to the European Parliament and the Council together with the draft general budget of the Union.
8. On the basis of that statement of estimates, the Commission shall enter in the draft budget of the 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 European Parliament and the Council in accordance with Article 314 TFEU.
9. The European Parliament and the Council shall authorise the appropriations for the subsidy to the Agency.
10. The European Parliament and the Council 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 definitive adoption of the general budget of the Union. Where appropriate, the Management Board shall adjust the Agency's budget and work programme in accordance with the general budget of the Union. The Management Board shall forward the budget without delay to the European Parliament, the Council and the Commission.

Article 20
Combating fraud

1. In order to facilitate the combating of fraud, corruption and other unlawful activities under Regulation (EC) No 1073/1999¹, the Agency shall, within six months from the day it becomes operational, accede to the Interinstitutional Agreement of 25 May 1999 concerning internal investigations by the European Anti-fraud Office (OLAF) and shall adopt the appropriate provisions applicable to all the employees of the Agency, using the template set out in the Annex to that Agreement.
2. The Court of Auditors shall have the power of audit, on the basis of documents and on the spot, over all grant beneficiaries, contractors and subcontractors who have received Union funds from the Agency.
3. OLAF may carry out investigations, including on-the-spot checks and inspections, in accordance with the provisions and procedures laid down in Regulation (EC) No 1073/1999 and Council Regulation (Euratom, EC) No 2185/96 of 11 November 1996 concerning on-the-spot checks and inspections carried out by the Commission in order to protect the European Communities' financial interests against fraud and other irregularities² with a view to establishing whether there has been fraud, corruption or any other illegal activity affecting the financial interests of the Union in connection with a grant or a contract funded by the Agency.

¹ 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) (OJ L 136, 31.5.1999, p. 1).

² OJ L 292, 15.11.1996, p. 2.

4. Without prejudice to paragraphs 1, 2 and 3, cooperation agreements with third countries and international organisations, contracts, grant agreements and grant decisions of the Agency shall contain provisions expressly empowering the Court of Auditors and OLAF to conduct such audits and investigations, according to their respective competences.

Article 21

Implementation of the budget

1. The Executive Director shall be responsible for the implementation of 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 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 147 of the Financial Regulation.
4. By 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 European Parliament and the Council.

5. On receipt of the Court of Auditor's observations on the Agency's provisional accounts, pursuant to Article 148 of the 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, by 1 July following each financial year, transmit the final accounts, including the report on the budgetary and financial management for that financial year and the Court of Auditor's observations, 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 and shall also send to the Management Board a copy of that reply.
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 165(3) of the Financial Regulation.
11. The European Parliament, acting on a recommendation from the Council, shall, before 15 May of year N+2, give a discharge to the Executive Director in respect of the implementation of the budget for the year N.

SECTION 5

STAFF

Article 22

General provisions

The Staff Regulations and the Conditions of Employment of Other Servants and the rules adopted by agreement between the Union institutions for giving effect to those Staff Regulations shall apply to the staff of the Agency.

Article 23

Privileges and immunity

Protocol No 7 on the Privileges and Immunities of the European Union annexed to the Treaty on European Union and to the TFEU shall apply to the Agency and its staff.

Article 24

Executive Director

1. The Executive Director shall be engaged as a temporary agent of the Agency under Article 2(a) of the Conditions of Employment of Other Servants.

2. The Executive Director shall be appointed by the Management Board from a list of candidates proposed by the Commission, following an open and transparent selection procedure.

For the purpose of concluding the contract of the Executive Director, the Agency shall be represented by the Chairperson of the Management Board.

Before appointment, the candidate selected by the Management Board shall be invited to make a statement before the relevant committee of the European Parliament and to answer Members' questions.

3. The term of office of the Executive Director shall be five years. By the end of that period, the Commission shall undertake an assessment which takes into account the evaluation of the performance of the Executive Director and the Agency's future tasks and challenges.
4. The Management Board may, acting on a proposal from the Commission which takes into account the assessment referred to in paragraph 3 and after obtaining the views of the European Parliament, extend once the term of office of the Executive Director for no more than five years.
5. The Management Board shall inform the European Parliament about its intention to extend the Executive Director's term of office. Within three months before any such extension, the Executive Director shall, if invited, make a statement before the relevant committee of the European Parliament and answer Members' questions.

6. An Executive Director whose term of office has been extended may not participate in another selection procedure for the same post.
7. The Executive Director may be removed from office only by decision of the Management Board.

Article 25

Seconded national experts and other staff

1. The Agency may make use of seconded national experts or other staff not employed by the Agency. The Staff Regulations and the Conditions of Employment of Other Servants shall not apply to such staff.
2. The Management Board shall adopt a decision laying down rules on the secondment to the agency of national experts.

SECTION 6

GENERAL PROVISIONS

Article 26

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.
4. A branch office established in the metropolitan area of Athens shall be maintained in order to improve the operational efficiency of the Agency.

Article 27

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 of the European Union 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 28

Languages

1. Regulation No 1 of 15 April 1958 determining the languages to be used in the European Economic Community¹ 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 official language of the institutions of the Union 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.

¹ OJ 17, 6.10.1958, p. 385.

Article 29

Protection of personal data

1. When processing data relating to individuals, in particular while performing its tasks, the Agency shall observe the principles of personal data protection in, and be subject to, the provisions of Regulation (EC) No 45/2001.
2. The Management Board shall adopt implementing measures referred to in Article 24(8) of Regulation (EC) No 45/2001. The Management Board may adopt additional measures necessary for the application of Regulation (EC) No 45/2001 by the Agency.

Article 30

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 legal acts 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 those countries will participate in the Agency's work, including provisions relating to participation in the initiatives undertaken by the Agency, financial contributions and staff.

Article 31

Security Rules on the protection of classified information

The Agency shall apply the security principles contained in the Commission's security rules for protecting European Union Classified Information (EUCI) and sensitive non-classified information, as set out in the annex to Decision 2001/844/EC, ECSC, Euratom. This shall cover, inter alia, provisions for the exchange, processing and storage of such information.

SECTION 7

FINAL PROVISIONS

Article 32

Evaluation and review

1. By ...* the Commission shall commission an evaluation to assess, in particular, the impact, effectiveness and efficiency of the Agency and its working practices. The evaluation shall also address the possible need to modify the mandate of the Agency and the financial implications of any such modification.
2. The evaluation referred to in paragraph 1 shall take into account any feedback made to the Agency in response to its activities.

* OJ: Please add date 5 years from the day of entry into force of this Regulation.

3. The Commission shall forward the evaluation report together with its conclusions to the European Parliament, the Council and the Management Board. The findings of the evaluation shall be made public.
4. As part of the evaluation, there shall also be an assessment of the results achieved by the Agency, having regard to its objectives, mandate and tasks. If the Commission considers that the continuation of the Agency is justified with regard to its assigned objectives, mandate and tasks, it may propose that the duration of the mandate of the Agency set out in Article 36 be extended.

Article 33

Cooperation of the host Member State

The Agency's host Member State shall provide the best possible conditions to ensure the proper functioning of the Agency, including the accessibility of the location, the existence of adequate education facilities for the children of staff members, appropriate access to the labour market, social security and medical care for both children and spouses.

Article 34

Administrative control

The operations of the Agency shall be supervised by the Ombudsman in accordance with Article 228 TFEU.

Article 35
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 36
Duration

The Agency shall be established for a period of seven years from ...⁺.

⁺ OJ: Please add the date of entry into force of this Regulation.

Article 37
Entry into force

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

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

Done at ...,

For the European Parliament
The President

For the Council
The President
