COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 11.2.2003
COM(2003) 63 final

2003/0032 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

Establishing the European Network and Information Security Agency

(presented by the Commission)

eEurope 2005

EXPLANATORY MEMORANDUM

1. BACKGROUND

Today more than 90% of companies in the European Union have an Internet connection and the majority of them operate a web site. An overwhelming number of employees use a mobile phone, a lap-top, or a similar device to send or retrieve information for their work. Such information can represent a considerable value, for instance describe a business transaction or contain technical knowledge.

Beyond work, computing and networking have become an essential part of people's lives. In 2002 about 40% of EU households had their own Internet connections and more than 2/3 of the population used a mobile phone. Schools and universities have Internet connections and learning and studying using the Internet or a computer is common practice. Public administrations are rapidly moving towards electronic government. Computers and communication networks control infrastructures such as electricity and water supply or public transport systems. Since 11 September 2001 these aspects have also become a matter for national security.

As so much depends on networks and information systems, their secure functioning has become a key concern. Similarly to what has become a natural expectance with e.g. electricity or water supply, people also expect a phone to work when they pick it up. They expect a computer to run properly when they need it. They want to have access to stored information without undue delays or interruptions. Network failures and computer crashes are no longer an isolated problem for computer specialists. The malfunctioning of networks and information systems concerns everybody: citizens, businesses and public administrations.

Security has become an essential feature of many businesses, in particular on-line businesses. It has therefore become an industry with specialised companies selling products and services and is also subject to commercial arrangements. Consumers for instance buy anti-virus software and install firewalls on their computers. Companies invest in security, establish protected intranets and encrypt e-mails or wireless communication. Sensitive data is transmitted using encryption. Some users seem to be well aware of vulnerabilities and means to manage them, others are less informed or concerned.

From today's perspective network and information security is about ensuring the availability of services and data, preventing the disruption and unauthorised interception of communications, confirming that data which has been sent, received or stored are complete and unchanged, securing the confidentiality of data, protecting information systems against unauthorised access, protecting against attacks involving malicious software and securing dependable authentication, i.e. the confirming of an asserted identity of entities or users.

In the near future requirements on security will rapidly change as networking and computing develop further and computing will become more ubiquitous. This means that broadband connections will offer people the possibility to be connected to the Internet at all times, new wireless applications will enable the users to access the Internet from just about anywhere and the possibilities to connect everything from

printers to refrigerators to the Internet, will continue to develop and expand the way people use the Internet.

Managing security has turned out to be a difficult and complex task as the user has to deal with the availability, integrity, authenticity, and confidentiality of data and services. Due to the complexity of technology, many components and actors must play together, and human behaviour has become a crucial factor.

Full security will probably never be achievable at least not at reasonable costs. There will always be weak points, attacks, incidents and failures that will generate damage and undermine trust in systems and services. This is no different from other technologies and aspects of daily life. Society as a whole as well as individuals have to learn how to manage the risks involved in networks and information systems.

2. CAUSE FOR ACTION

Security has become a major policy concern. Governments see a widening responsibility for society and are increasingly making efforts to improve security on their territory. They want to promote security, for instance by giving support to computer emergency response teams, to research and for awareness campaigns. They also equip and train law enforcement to deal with computer and Internet related crime.

Member States are, however, in different stages of their work and the focus of attention varies. Apart from administrative networks such as TESTA there is no systematic cross-border co-operation on network and information security between Member States although security issues cannot be an isolated issue for only one country. There is no mechanism to ensure effective responses to security threats. Implementation of the legal framework varies. Product certification is national whilst key standards are developed by the global industry, and operators and vendors are faced with different attitudes of governments. All this leads to a lack of interoperability that impedes a proper use of the security products and services.

The European Community would benefit from increased co-ordination between Member States to achieve a sufficiently high level of security in all Member States. This is the objective of the Communication of the Commission on Network and Information Security from June 2001,[1] that proposed a number of measures inter alia awareness raising actions, improved exchange of information mechanisms and support for market oriented standardisation and certification.

The Communication also proposed the establishment of a European warning and information system. The Council Resolution of 28 January 2002 on a common approach and specific actions in the area of network and information security developed this concept further. It has become clear that the current institutional arrangements would not allow network and information security to be addressed appropriately at European level.

---

[1] Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, Network and Information Security; Proposal for A European Policy Approach, COM(2001) 298 final.

The Resolution welcomes the intention of the Commission to make proposals for the establishment of a cyber security task force to build on national efforts to both enhance network and information security and to enhance Member States' ability, individually and collectively, to respond to major network and information security problems.

In response to the Commission's suggestions, the European Parliament adopted an opinion whereby it has strongly requested a European answer to the increasing security problem.

In June 2002 the OECD adopted their Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. These guidelines emphasise the importance of applying certain common principles for information security and underpin the work that is taking place on a European level.

3. THE PROPOSAL TO ESTABLISH A NETWORK AND INFORMATION SECURITY UNIT

3.1. Background

The European Parliament, the Council, and the Commission are advocating closer European co-ordination on information security. The setting up of an entity with a legal personality would be the most efficient way to achieve this objective. The proposed Regulation therefore proposes to establish a European regulatory agency in accordance with the provisions of the Commission Communication "The operating framework for the European Regulatory Agencies", COM (2002) 718 final. This agency will be called the European Network and Information Security Agency, hereinafter referred to as "the Agency".

However the specific electronic communications legislation, and in particular the electronic communications framework directive, attribute an important role to national competent bodies. Therefore the Agency will not only provide assistance to the Commission but also to national regulatory authorities.

The proposal reflects a number of concerns that were expressed during the consultation with the Member States carried out by the Commission. Corresponding concerns were also addressed in contributions from the private sector and can be summarised as requiring flexibility, trustworthiness, competence, efficiency and consistency of the proposed Agency. In particular the following requirements have been emphasised:

a) as network and information security is a fast evolving area, the best institutional arrangement may change over time. Therefore the Agency should operate for an limited period after which a review process should be made,

b) the Agency needs to be trusted by public bodies and institutions in the Member States as well as by private sector,

c) the Agency should constitute a centre of expertise by bringing together competent people from all Member States,

d) the Agency needs to be able to act efficiently and quickly. Therefore sufficient human and financial resources will be necessary to enable a smooth and

flexible operation but the Agency should nevertheless be limited to a reasonable size; and,

e) the Commission needs to be able to guide the work of the Agency.

These requirements are the guidance for the proposed Regulation. They explain why the tasks of the Agency are clearly described and at the same time provide for flexibility. They motivate an evaluation of the Agency's operations after the first three years. They make it clear that close co-operation with Member States institutions and bodies as well as with the Community institutions is crucial for the proper functioning of the Agency.

The Agency's work will benefit from scientific support through research activities carried out by the Joint Research Centre and other Community research programmes.

3.2. The choice of the legal basis

Against this background this proposal addresses two closely linked issues of Community interest, namely the proper functioning of the Internal Market and interoperability of electronic trans-European networks. Firstly the introduction of technically complex requirements for security in networks and information systems at Member State and Community level could hamper the full deployment of the Internal Market principles. Secondly, the smooth operation of the Internal Market also depends on the interoperability of security functions in networks and information systems.

The following sections refer to the Sections 1-5 in the proposal.

3.3. Section 1 – objectives and tasks

3.3.1. Objectives

The broad objective of the Agency is to create a common understanding in Europe of issues relating to information security that is necessary to ensure the availability and security of networks and information systems in the Union. To meet this objective the definition of network and information security has to be wide and cover all activities that can have adverse effects on the security of networks and information systems.

The Agency shall be able to provide assistance in the application of Community measures relating to network and information security. The assistance it provides shall help ensure interoperability of information security functions in networks and information systems, thereby contributing to the functioning of the Internal Market. It shall enhance the capability of both Community and Member States to respond to network and information security problems. The Agency will play a key role for the security of Europe's networks and information systems and the development of the information society in general.

3.3.2. Tasks

The Agency will have advisory and co-ordinating functions, where data on information security is gathered and analysed. 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 on European level that in a comprehensive manner can collect and analyse data and provide opinions and advice to support the Community's policy work on network and information security. The Agency will serve as a centre of expertise where both Member States and Community Institutions can seek advice on technical matters relating to security.

The Agency will further contribute to a broad co-operation between different actors in the information security field, e.g. to assist in the follow-up activities in support of secure e-business. Such co-operation will be a vital prerequisite for the secure functioning of networks and information systems in Europe. The participation and involvement of all stakeholders is necessary.

The Agency will contribute to a co-ordinated approach to information security by providing support to Member States, e.g. on the promotion of risk assessment and awareness raising actions. To ensure interoperability of networks and information systems, the Agency will also provide opinions and support for harmonised processes and procedures in the Member States when applying technical requirements that affect security. Not only legal requirements, but to a large extent technical requirements can affect the interoperability and create obstacles to the well functioning Internal Market.

The Agency will further play a supportive role in the identification of the relevant standardisation needs, and in the promotion of security standards and certification schemes and of their widest possible use by the Commission and the Member States in support of the European legislation.

As the network and information security issues are global there is also a need for international co-operation in this field. The Agency will provide support for the Community contacts with relevant parties in third countries.

New vulnerabilities and threats constantly arise in the area of information systems and networks. It is necessary that the Commission should be able to assign additional tasks to the Agency in order to keep up with current technological and societal development, in accordance with the provisions of the operating framework for the European Regulatory Agencies.

3.4. Section 2 – Organisation

3.4.1. *Management*

The organisational structure should facilitate the involvement of the Agency's diverse stakeholders, independence from external pressures, transparency and accountability to the democratic institutions. It is therefore proposed to establish a Management Board consisting of members appointed by the Council and the Commission. For instance, the Commission's representation will include a member of the Security Directorate. It is further proposed that there will be representatives of industry and consumers, proposed by the Commission and appointed by the Council in the Management Board. The industry and consumer representatives shall have no voting rights.

The Agency will be managed by an Executive Director who possesses a high degree of independence and flexibility and who will be responsible for organising the internal functioning of the Agency. The Executive Director will also be responsible for the preparation and implementation of the budget and the work programme of the Agency and for personnel matters. In order to provide the necessary legitimacy, the Executive Director should be appointed by the Management Board by a proposal from the Commission.

As a Community body, the Agency should ensure the best use of the expertise and resources in pursuit of its mission whilst respecting the overarching requirement for independence. It is therefore proposed that the Agency includes a restricted Advisory Board comprising experts whose task it is to facilitate co-operation and information exchange between the Agency and the competent institutions and bodies in the different Member States, e.g. a data protection expert or a research community representative. The Advisory Board will have advisory functions and be responsible together with the Executive Director for drafting the annual work programme of the Agency.

3.5. Section 3 – Operation

3.5.1. *Work programme*

The Agency will need the flexibility to adapt its work to the fast evolving technological advances and to refocus its work. Therefore the Management Board shall adopt a work programme for each year, approved by the Commission after a proposal from the Executive Director. The results of the activities according to each years work programme shall be made in the general report, drafted by the Executive Director and adopted by the Management Board.

3.5.2. *Opinions*

There is a risk that the Agency may become overloaded with requests to deliver opinions and assistance and therefore it should be specified who can make the requests and the process of how the requests should be handled.

3.5.3. *Working groups*

Although the Agency staff will be highly qualified, it can be expected that issues of a more specialised nature may arise. Therefore the Agency shall be able to establish temporary working groups composed of experts in various fields. Pursuant to the transparency policy, representatives of the Commission will be entitled to be present in the meetings of such working groups.

3.5.4. *Independence*

The acceptance of advice and opinions of the Agency by individuals, public administrations and businesses will depend on establishing a model of independence. Therefore the members of the Management Board and the Advisory Board, the Executive Director and the external experts participating in working groups will be obliged to declare the absence of interest which might put their independence in question.

3.5.5. *Transparency and confidentiality*

The Agency will adopt its rules regarding transparency and access to documents in compliance with the decisions of the European Parliament and the Council in the context of Article 255 of the EC Treaty and with Commission Security Provisions[2]

Although a high level of transparency is also necessary for the acceptance of the work of the Agency as well as a wide access to the documents it issues it will also collect information which needs to be kept confidential.

3.6. Section 4 – Financial provisions

For 2004-2008 the Agency needs a budget allocation large enough to hire its personnel as described above and to provide the personnel with proper technological equipment to be able to carry out its tasks and to function smoothly. The budget is specified in the Legislative Financial Statement.

The budget of the Agency will be financed by a contribution from the Community with possible contributions from participating third countries participating in the Agency's work. The Executive Director will be responsible for the establishment of a preliminary draft statement of estimates. The Management Board will provide the Commission with the statement of estimates of revenue and expenditure for processing in accordance with standard budgetary procedures.

The Executive Director will be responsible for the implementation of the budget. The European Parliament, acting on a recommendation from the Council, will give discharge to the Executive Director of the Agency in respect of the implementation of the budget. The Financial Auditor of the Commission will ensure financial audit. The Court of Auditors will examine the accounts and publish an annual report.

3.7. Section 5 – General provisions

3.7.1. *Legal personality and privileges*

The Agency shall have the broadest legal personality in every Member State and will benefit from the same privileges and immunities as set out in the Protocol on the Privileges and Immunities of the European Communities.

3.7.2. *Liability*

The regime of contractual and non-contractual liability of the Agency corresponds to the regime applicable to the Community by virtue of Article 288 of the Treaty.

3.7.3. *Personnel*

As a centre of expertise, it is of vital importance for the Agency to have a sufficient number of highly qualified staff. Professionals with corresponding profiles are currently scarce and very sought after in Europe. The Agency shall recruit both from the public and the private sector. The personnel of the Agency will be subject to the

---

[2] Council Decision 2001/264/EC of 19 March 2001 adopting the Council's security regulations and the Commission Decision C(2001) 3831.

Staff Regulations applicable to Officials of the European Communities and the Conditions of Employment of Other Servants. Without prejudice to the need to have stable, qualified staff in sufficient number, the personnel will be employed on temporary contracts with a maximum duration of five years.

3.7.4. Protection of personal data

The Agency will also process personal data in relation to its tasks and will in this respect apply the applicable regulations for such processing as a Community institution.

3.7.5. *Participation of third countries*

The Agency will be open to participation by third countries which have entered into agreements with the European Community whereby they have adopted and are applying the Community law in the field covered by this regulation.

3.8. Section 6 – Final provisions

3.8.1. *Review*

As network and information security is a highly technological issue and therefore fast evolving, the best institutional arrangement may change over time. Within three years of the starting date established in Article 26, or earlier if considered necessary by the Management Board, a review process should start in order to show the value of continued operations after this initial period of five years and if necessary propose any modification to its future responsibilities, objectives and mandate.

This review will in particular address the extent to which the absence of law enforcement participation has negatively affected the effectiveness and efficiency of operations of the Agency. In case the evaluation would demonstrate such adverse effects, the Commission will examine the appropriateness of a proposal supplementing this regulation.

3.8.2. Location

The location of the Agency should meet the following criteria:

– easily accessible in terms of communications, especially electronic communication facilities, and have effective and fast transport connections;

– enable the Agency to work closely and efficiently with those institutional services which deal with network and information security issues;

– be cost-effective and enable the Agency to start its work immediately;

– provide for the necessary infrastructure for the personnel of the Agency.

3.8.3. Duration

It is proposed that the Agency becomes operational 1 January 2004 and that it will function for 5 years. The continued operations of the Agency is dependent on the

outcome of the evaluation performed by the Commission in collaboration with the Advisory Board.

2003/0032 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

Establishing the European Network and Information Security Agency

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Articles 95 and 156 thereof,

Having regard to the proposal from the Commission[3],

Having regard to the opinion of the European Economic and Social Committee[4],

Having regard to the opinion of the Committee of the Regions[5],

Acting in accordance with the procedure laid down in Article 251 of the Treaty[6],

Whereas:

(1) Communication networks and information systems have become an essential factor in economic and societal development. Computing and networking are now becoming ubiquitous utilities in the same way as electricity or water supply already are. The security of communication networks and information systems, in particular their availability, is therefore of increasing concern to society.

(2) Network and information security is about ensuring the availability of services and data, preventing the disruption and unauthorised interception of communications, confirmation that data which have been sent, received or stored are complete and unchanged, securing the confidentiality of data, protecting information systems against unauthorised access and against attacks involving malicious software and securing dependable authentication.

(3) The growing number of security breaches has already generated substantial financial damage, has undermined user confidence and has been detrimental for the development of e-commerce. Individuals, public administrations and businesses have reacted by deploying security technologies and security management procedures. Member States have taken several supporting measures, such as information campaigns and research projects, to enhance network and information security throughout society.

---

3 OJ C […], […], p. […].
4 OJ C […], […], p. […].
5 OJ C […], […], p. […].
6 OJ C […], […], p. […].

(4) Reactions of Member States have been disparate and not sufficiently co-ordinated to ensure an effective response to security problems. Due to the technical complexity of networks and information systems, the variety of products and services that are interconnected, and the huge number of private and public actors that bear their own responsibility, a consistent security response at Community level has not been developed yet. A particular problem has been the lack of interoperable security products and services, thereby jeopardising the interoperability of the networks concerned. Equally these characteristics have made the effective application of Community measures subject to rather complex technical analysis and understanding.

(5) The lack of a common European response to the information security problems in the application of Community measures risks undermining the smooth functioning of the Internal Market.

(6) Directive 2002/21/EC of 7 March 2002 on a common regulatory framework for electronic communications networks and services[7] ("the Framework Directive") lays down the tasks of national regulatory authorities, which include encouraging the establishment and development of trans-European networks and the interoperability of pan-European services, co-operating with each other and the Commission in a transparent manner to ensure the development of consistent regulatory practice, contributing to ensuring a high level of protection of personal data and privacy, and ensuring that the integrity and security of public communications networks are ensured.

(7) Directive 2002/20/EC of 7 March 2002 on the authorisation of electronic communications networks and services[8] entitles Member States to attach to the general authorisation, conditions regarding the security of public networks against unauthorised access according to Directive 97/66/EC of 15 December 1997 on the processing of personal data and the protection of privacy in the telecommunications sector.

(8) Directive 2002/22/EC of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services[9] requires that Member States take necessary steps to ensure the integrity and availability of the public telephone networks and that undertakings providing publicly available telephone services at fixed locations take all reasonable steps to ensure uninterrupted access to emergency services.

(9) Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector[10] requires a provider of a publicly available electronic communications service to take appropriate technical and organisational measures to safeguard security of its services and also requires the confidentiality of the communications and related traffic data. The Directive 95/46/EC 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,[11] imposes on Member States to provide that the controller must implement appropriate technical and organisational

---

7 OJ L 108, 24.4.2002, p.33.
8 OJ L 108, 24.4.2002, p.21.
9 OJ L 108, 24.4.2002, p.51.
10 OJ L 201, 31.7.2002, p.37.
11 OJ L 281, 23.11.1995, p.31.

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.

(10) The Framework Directive and Directive 1999/93/EC of 13 December on a Community framework for electronic signatures[12] contain provisions on standards that are to be published in the Official Journal of the European Communities. Member States also use standards from international bodies as well as de facto standards developed by the global industry. It is necessary for the Commission and the Member states to be able to assess which standards meet the requirements of Community legislation.

(11) These Internal Market measures require different forms of technical and organisational applications by the Member States and the Commission. These are technically complex tasks with no single, self-evident solutions. The heterogeneous application of these requirements can lead to inefficient solutions and create obstacles to the Internal Market, as well as jeopardising interoperability of information security functions. This calls for the creation of a centre of expertise at European level providing guidance, assistance and opinions on technical and organisational implementation of such requirements, which may be relied upon by the Commission and the national regulatory authorities and competent bodies of the Member States. Competent bodies in the field of network and information security include law enforcement and judicial authorities in the Member States.

(12) The establishment of a European agency, the European Network and Information Security Agency, hereinafter referred to as "the Agency", operating as a point of reference and establishing confidence by virtue of its independence, the quality of the opinions it issues and the information it disseminates, the transparency of its procedures and methods of operation, and its diligence in performing the tasks assigned to it, would respond to these needs. The Agency should perform its tasks in full co-operation with the Member States and be open to contacts with industry and other interested groups.

(13) The increased Community and global impacts of security incidents call for a timely and effective response to such breaches. However, at present no authorised body in Europe systematically collects data on network and information security that could be used for analysis of security breaches.

(14) Ensuring confidence in networks and information systems requires that individuals, businesses and public administrations are sufficiently informed and knowledgeable in the field of security. Public authorities have taken steps to increase awareness by informing the public. However these measures need to be further developed, in particular, with regard to new vulnerabilities and their risks. An increased information exchange between Member States will facilitate such awareness raising actions.

(15) Despite the need for reliable processes, it is often difficult to assess the trustworthiness of products and services. There are publicly and privately organised evaluation and certification schemes. However, evaluation and certification processes tend to be cumbersome, expensive, and slow. All actors, including public authorities would

---

12 OJ L 13, 19.1.2000, p.12.

benefit from better technical guidance in their efforts to promote efficient certification systems. A technically competent European body for objective advice on the quality of different standards would therefore improve the possibilities to promote reliable security standards, including where appropriate standards for privacy enhancing technologies, in Europe.

(16) Efficient security policies are 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 practices for risk assessment will improve interoperability and increase the security level of networks and information systems in Europe.

(17) The work of the Agency should utilise ongoing research, development and technological assessment activities, in particular those carried out by the Joint Research Centre and by other Community research initiatives.

(18) Network and information security problems are global issues which are confined neither to individual Member States nor to the Community. A security problem can originate in a third country. Products and services are often developed and evaluated in third countries. Once entered into the Community, security products circulate virtually without restrictions and services can be freely offered. There is a need for closer co-operation at global level to improve security standards, improve information, and develop common response mechanisms. Several international partners of the Community have began to set up security bodies to allow for better responses and policy development. Efficient co-operation with these countries and the global community has become a task also at European level.

(19) In order to effectively ensure the accomplishment of the functions of the Agency, the Member States and the Commission should be represented on a Management Board 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, approve its work programme, examine requests for technical assistance from Member States, and appoint the Executive Director. In the light of the highly technical and scientific mission and tasks of the Agency, it is appropriate for the Management Board to consist of members with a high level of expertise in issues within the scope of the Agency's mission appointed by the Council and the Commission.

(20) An Advisory Board should be established in order to advise the Executive Director on co-operation and facilitation of an appropriate exchange of information between the Member States and the Agency. The advisory function of the Advisory Board does also include the preparation of the proposal for the Agency's annual work programme. In determining the membership of the Advisory Board, the relevant expertise should be ensured, including data protection expertise.

(21) The good functioning of the Agency requires that its Executive Director is 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 and flexibility as to the organisation of the internal functioning of the Agency. To this end, the Executive Director should prepare and take all necessary steps to ensure the proper accomplishment of the working programme of the Agency, should prepare each year a

draft general report to be submitted to the Management Board, should draw up estimates of the revenues and expenditure of the Agency and should implement the budget.

(22) The Agency should apply the relevant Community legislation concerning public access to documents[13] and the protection of individuals with regard to the processing of personal data.[14]

(23) To the extent that the Agency will process data related to unlawful acts against information systems, incident handling procedures and threat assessment functions, a certain overall political co-ordination will be required, both at national and European Union level. Such co-ordination should be ensured within the framework of the Advisory Board referred to in Article 7 and be carried out without compromising confidentiality requirements as referred to in Article 13.

(24) 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 essentially from a contribution from the Community. The Community budgetary procedure remains applicable as far as any subsidies chargeable to the general budget of the Communities are concerned; moreover, the Court of Auditors should undertake the auditing of accounts.

(25) The Agency should be initially established for a limited period and its operations evaluated in order to determine whether the duration of its operations should be extended.

HAVE ADOPTED THIS REGULATION:

SECTION 1
OBJECTIVES AND TASKS

Article 1
Objectives

1. A European Network and Information Security Agency is hereby established, hereinafter referred to as "the Agency".

2. The Agency shall facilitate the application of Community measures relating to network and information security and help ensure interoperability of security functions in networks and information systems, thereby contributing to the functioning of the Internal Market. It shall enhance the capability of the Community and the Member States to respond to network and information security problems.

---

[13] 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.

[14] 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.

Article 2
Tasks

In order to achieve the objectives in Article 1, the tasks of the Agency shall be to:

(a) collect and analyse data, including information on current and emerging risks and, in particular, those which would impact on the resilience of critical communications networks and the information accessed and transmitted through them;

(b) provide assistance and deliver opinions within its objectives to the Commission and other competent bodies;

(c) enhance co-operation between different actors operating in the field of network and information security, inter alia by establishing a network for national and Community bodies;

(d) contribute to the availability of rapid, objective and comprehensive information on network and information security issues for all users by, inter alia, promoting exchanges of best practice on methods of alerting users, including those related to computer attack alert systems, and seeking synergy between public and private sector initiatives;

(e) assist when called upon, the Commission and national regulatory authorities in analysing the implementation of network and information security requirements for operators and service providers, including requirements on data protection, that are contained in Community legislation;

(f) contribute to the assessment of standards on network and information security;

(g) promote risk assessment activities and encourage interoperable risk management solutions within organisations;

(h) contribute to the Community approach on co-operation with third countries including facilitating contacts with international fora;

(i) undertake any other task assigned to it by the Commission within its objectives.

Article 3
Definitions

For the purposes of this Regulation the following definitions shall apply:

– '*network'* means transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, networks used for radio and television broadcasting, and cable TV networks, irrespective of the type of information conveyed;

– *'information system*' means computers and electronic communication networks, as well as electronic data stored, processed, retrieved or transmitted by them for the purposes of their operation, use, protection and maintenance;

– '*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 these networks and systems;

– *'availability*' means that data is accessible and services are operational;

– *'authentication*' means the confirmation of an asserted identity of entities or users;

– *'data integrity*' means the confirmation that data which has been sent, received, or stored are complete and unchanged;

– '*data confidentiality'* means the protection of communications or stored data against interception and reading by unauthorised persons;

– *'risk'* means a function of the probability that a vulnerability in the system affects the availability, authentication, integrity or confidentiality of the data processed or transferred and the severity of that effect, consequential to the intentional or non-intentional use of such a vulnerability;

– *'risk assessment'* means a scientific and technologically based process consisting of four steps threats identification, threat characterisation, exposure assessment and risk characterisation;

– *'risk management'* means the process, distinct from risk assessment, of weighing policy alternatives in consultation with interested parties, considering risk assessment and other legitimate factors, and, if need be, selecting appropriate prevention and control options.

SECTION 2
ORGANISATION

Article 4
Bodies of the Agency

The Agency shall comprise:

(a) a Management Board;

(b) an Executive Director and his/her staff;

(c) an Advisory Board and,

(d) where necessary, working groups.

Article 5
Management Board

1. The Management Board shall be composed of six representatives appointed by the Council, six representatives appointed by the Commission, as well as two representatives of industry and one representative of consumers proposed by the Commission and appointed by the Council without the right to vote.

2. Representatives may be replaced by alternates, appointed at the same time. Their term of office shall be two and a half years, and may be extended once.

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

4. The Management Board shall elect its Chairperson from among its members for a two and a half year period, which shall be renewable.

5. The Management Board shall adopt its rules of procedure which the Commission shall have approved. Unless otherwise provided, the Management Board shall act by a majority of its members.

6. The Management Board shall meet at the Chairperson's invitation or at the request of at least a third of its members.

7. The Management Board shall adopt the Agency's internal rules of operation on the basis of a proposal by the Commission. These rules shall be made public.

8. The Management Board shall define the general orientations for the operation of the Agency and ensure that the Agency carries out its tasks under conditions which enable it to serve as a point of reference by virtue of its independence, the quality of the opinions it issues and the information it disseminates, the transparency of its procedures and methods of operation and it diligence in performing tasks assigned to it.

9. Before 31 January each year, the Management Board, having received the Commission's approval, shall adopt the Agency's work programme for that year. The Management Board shall ensure that the work programme is consistent with the Community's legislative and policy priorities in the area of network and information security.

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

11. The financial rules applicable to the Agency shall be adopted by the Management Board after the Commission has been consulted. They may not depart from the framework Financial Regulation adopted by the Commission under Article 185 of the Council Regulation (EC, Euratom) No 1605/2002[15] (hereinafter "the general Financial Regulation") unless specifically required for the Agency's operation and with the Commission's prior consent.

---

[15] OJ L 248, 16.9.2002, p.1.

Article 6
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 by the Management Board on the basis of a list of candidates proposed by the Commission after an open competition following publication in the Official Journal of the European Communities and elsewhere of a call for expressions of interest. Before appointment the candidate nominated by the Management Board shall be invited without delay to make a statement before the European Parliament and to answer questions put by members of his institution. The Executive Director may be removed from office by the Management Board having received the Commission's approval.

3. The term of office of the Executive Director shall be two and a half years and may be extended once.

4. The Executive Director shall be responsible for:

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

   (b) drawing up a proposal for the Agency's work programmes in consultation with the Advisory Board;

   (c) implementing the work programmes and the decisions adopted by the Management Board;

   (d) ensuring that the Agency carries out its tasks in accordance with the requirements of those using its services, in particular with regard to the adequacy of the services provided;

   (e) the preparation of the Agency's statement of estimates of revenue and expenditure and the execution of its budget;

   (f) all staff matters;

   (g) developing and maintaining contact with the European Parliament and for ensuring a regular dialogue with its relevant committees.

5. Each year, the Executive Director shall submit to the Management Board for approval:

   (a) a draft general report covering all the activities of the Agency in the previous year;

   (b) draft work programme.

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 have it published

7. 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 Economic and Social Committee and the Committee of the Regions, and shall have it published.

Article 7
Advisory Board

1. The Advisory Board shall be composed of nine experts proposed by the Management Board and designated by the Executive Director. Representatives may be replaced by alternates, appointed at the same time. Representatives of the Commission shall be entitled to be present in the meetings and participate in the work of the Advisory Board.

2. Members of the Advisory Board may not be members of the Management Board.

3. The Advisory Board shall be chaired by the Executive Director. It shall meet regularly at the Chairperson's invitation or at the request of at least a third of its members. Its operational procedures shall be specified in the Agency's internal rules of operation and shall be made public.

4. The opinions of the Advisory Board can be put to a vote.

5. The Agency shall provide the technical and logistic support necessary for the Advisory Board and provide the secretariat of its meetings.

6. The Advisory Board shall

   (a) advise the Executive Director in the performance of his duties under this Regulation, in particular in drawing up a proposal for the Agency's work programme.

   (b) advise the Executive Director on ensuring close co-operation between the Agency and the competent institutions and bodies in the Member States, and in particular on ensuring consistency of the Agency's work with activities conducted by Member States.

7. The Executive Director may invite representatives of the European Parliament and other relevant bodies to take part in the meetings of the Advisory Board.

SECTION 3
OPERATION

Article 8
Work programme

The Agency shall base its operations on carrying out the work programme adopted in accordance with Article 5(9). The work programme shall not prevent the Agency from taking up unforeseen activities that fall within its objectives and the given budget limitations.

Article 9
Opinions

1. Requests for opinions and assistance falling within the Agency's objectives shall be addressed to the Executive Director and accompanied by background information explaining the issue to be addressed. The Executive Director shall within 10 working days forward the request to the Commission .

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

   (a) the Commission

   (b) a national regulatory authority as defined in Article 2 of the Framework Directive or another Member State competent body recognised by the Management Board for this purpose.

3. In case the Agency has difficulties meeting a request or when a request is not made in accordance with paragraph 1, or when different requests are made on the same issues, the Executive Director shall consult with the Management Board before taking a decision. If the Agency refuses a request, justification shall be given. The Executive Director may also request the Advisory Board for advice on the prioritisation of requests for opinions.

Article 10
Working groups

1. Where necessary and within its objectives the Agency may establish working groups composed of experts, proposed by the Advisory Board and designated by the Executive Director, in particular regarding technical and scientific matters.

2. Working groups shall be established by the Advisory Board on a proposal from the Executive Director having consulted the Management Board.

3. Representatives of the Commission shall be entitled to be present in the meetings of the working groups.

4. The procedures for the appointment of the experts and the operation of the working group shall be specified in the Agency's internal rules.

Article 11
Independence

1. The members of the Management Board, the Executive Director and the Advisory Board shall undertake to act independently in the public interest. For this purpose, they shall make a declaration of commitment and a declaration of interests indicating the absence of any direct or indirect interests which might be considered prejudicial to their independence. Such declarations shall be made in writing.

2. External experts participating in working groups, shall declare at each meeting any interests which might be considered prejudicial to their independence in relation to the items on the agenda.

Article 12
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 members of the Management Board, the Executive Director and the Advisory Board as well as the declarations of interest made by experts in relation to items on the agendas of meetings of the 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. 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 13
Confidentiality

1. The Agency shall not divulge to third parties information that it processes or receives for which confidential treatment has been requested and justified, except for information which must be disclosed in accordance with national law, in order to protect public security and for the prevention, investigation, detection and prosecution of criminal offences.

2. Members of the Management Board and of the Advisory Board the Executive Director and external experts participating in their working groups, and members of the staff of the Agency, even after their duties have ceased, are subject to the requirements of confidentiality pursuant to Article 287 of the EC Treaty.

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

4. For the purpose of the first paragraph "third parties" shall not include the Commission.

Article 14
Access to 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[16] shall apply to documents held by the Agency.

---

16 OJ L 145, 31.5.2001, p.43.

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

3. Decisions taken by the Agency under Article 8 of Regulation (EC) No 1049/2001 may be appealed by means of a complaint to the Ombudsman or an action before the Court of Justice of the European Communities, under Articles 195 and 230 of the EC Treaty respectively.

SECTION 4
FINANCIAL PROVISIONS

Article 15
Adoption of the budget

1. The revenues of the Agency shall consist of a contribution from the Community and any contribution from third countries participating in the work of the Agency as provided for by Article 22.

2. The expenditure of the Agency shall include the 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 an estimate of the Agency's revenue and expenditure for the coming financial year, and shall forward it to the Management Board, accompanied by a list of posts.

4. Revenue and expenditure shall be in balance.

5. By 31 March at the latest each year, the Management Board, on the basis of a draft drawn up by the Executive Director, shall produce a statement of estimates of revenue and expenditure for the Agency for the following year. This statement of estimates, which shall include a draft establishment plan together with the provisional work programme, shall be transmitted by the Management Board to the Commission and the countries with which the Community has concluded agreements in accordance with Article 22.

6. On the basis of this statement of estimates, the Commission shall enter the corresponding amounts in the preliminary draft general budget of the European Communities, which it shall submit to the European Parliament and the Council (hereinafter referred to as "the budgetary authority") in accordance with Article 272 of the Treaty.

7. The budgetary authority shall determine the appropriations available for the subsidy to the Agency.

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

9. After the adoption of the general budget of the European Communities by the budgetary authority, the Management Board shall adopt the Agency's final budget and work programme, adjusting them where necessary to the Community's

contribution. It shall forward them without delay to the Commission and the budgetary authority.

Article 16
Combating fraud

1. In order to combat fraud, corruption and other unlawful activities the provisions of 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)[17] shall apply without restriction.

2. The Agency shall accede to the Interinstitutional Agreement of 25 May 1999 concerning internal investigations by the European Anti-fraud Office (OLAF)[18] and shall issue, without delay, the appropriate provisions applicable to all the employees of the Agency.

Article 17
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 31 March at the latest following each financial year, the Agency's accounting officer shall communicate 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 within the meaning of Article 128 of the general Financial Regulation.

4. By 31 March at the latest following each financial year, the Commission's accounting officer shall transmit 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 transmitted 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 129 of the general Financial Regulation, the Executive Director shall draw up the Agency's final accounts under his own responsibility and transmit 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 at the latest 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.

---

17 OJ L 136, 31.5.1999 p.1.
18 OJ L 136, 31.5.1999 p.15.

8. The final accounts shall be published.

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

10. The European Parliament, on a recommendation from the Council acting by a qualified majority, 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.

SECTION 5
GENERAL PROVISIONS

Article 18
Legal personality and privileges

1. The Agency shall be a body of the Community. 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. The Protocol on the Privileges and Immunities of the European Communities shall apply to the Agency and its staff.

Article 19
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 Communities shall have jurisdiction to give judgement 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 20
Staff

1. The staff of the Agency shall be subject to the rules and regulations applicable to officials and other staff of the European Communities.

2. Without prejudice to Article 5, the powers conferred on the appointing authority by the Staff Regulations and on the authority authorised to conclude contracts by the Conditions of employment of other servants, shall be exercised by the Agency in respect of its own staff.

Article 21
Protection of personal data

When processing data relating to individuals the Agency shall be subject to the provisions of 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.[19]

Article 22
Participation of third countries

1. The Agency shall be open to the participation of countries which have concluded agreements with the European Community by virtue of which they have adopted and applied Community 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 networks operated by the Agency, financial contributions and staff.

SECTION 6
FINAL PROVISIONS

Article 23
Review clause

1. Within three years of the starting date established in Article 26, or earlier if considered necessary by the Management Board, the Commission in collaboration with the Advisory Board, shall carry out an evaluation on the basis of the terms of reference agreed with the Management Board. The evaluation shall

   (a) assess the working practices and the impact of the Agency

   (b) substantially review the objectives and mechanisms established;

   (c) envisage, if necessary, the appropriate changes, in the light of institutional and legal developments in the European Union and with specific regard to broader security issues, including public security concerns and law enforcement participation.

2. The evaluation shall be made public.

---

[19] OJ L 8, 12.1.2001, p 1.

3. The Commission shall undertake the evaluation notably with the aim to determine whether the duration of the Agency should be extended beyond the date specified in Article 26.

Article 24
Administrative control

The operations of the Agency are subjected to the supervision of the Ombudsman according to the provisions of Article 195 of the Treaty.

Article 25
Seat

The seat of the Agency shall be decided by the competent authorities, at the latest six months after the adoption of this regulation, on a proposal from the Commission.

Article 26
Duration

The Agency shall be operational from 1 January 2004 until 31 December 2008.

Article 27
Entry into force

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

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

Done at Brussels, […]

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

LEGISLATIVE FINANCIAL STATEMENT

Policy area: Information Society

Activity: Network and information security

TITLE OF ACTION: PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL ESTABLISHING THE EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY

1. BUDGET LINE + HEADING

A new budget line will be proposed (this action is part of APS 2003)

2. OVERALL FIGURES

2.1. Total allocation for action (Part B): € million for commitment

24,300 M € for EUR 15 (EUR+ 10 will mean another 9 M € which will make the total cost for this action € 33,3 M)

This action was retained by the Commission in its Communication to the European Parliament and the Council of 27 February 2002 (SEC(2002) 217/9).

2.2. Period of application

2004 - 2008

2.3. Overall multiannual estimate of expenditure

(a) Schedule of commitment appropriations/payment appropriations (financial intervention)

€ million (*to three decimal places)*

	2004	2005	2006	2007	2008	Total
Commitments	2,500	5,000	5,600	5,600	5,600	24,300
Payments	2,500	5,000	5,600	5,600	5,600	24,300

(b) Technical and administrative assistance and support expenditure

Commitments							
Payments							

Subtotal a+b							
Commitments							
Payments							

(c) Overall financial impact of human resources and other administrative expenditure

Commitments/ payments							

TOTAL a+b+c						
Commitments	2,500	5,000	5,600	5,600	5,600	24,300
Payments	2,500	5,000	5,600	5,600	5,600	24,300

2.4. Compatibility with financial programming and financial perspective

Proposal will entail reprogramming of the relevant heading in the financial perspective.

2.5. Financial impact on revenue:[20]

Proposal has no financial implications (involves technical aspects regarding implementation of a measure)

3. BUDGET CHARACTERISTICS

Type of expenditure		**New**	**EFTA contribution**	**Contributions form applicant countries**	**Heading in financial perspective**
Non-comp	Diff/	YES	YES	NO	**3**

4. LEGAL BASIS

Articles 95 and 156 of the Treaty.

5. DESCRIPTION AND GROUNDS

5.1. Need for Community intervention [21]

The ex ante evaluation demonstrates that the various alternative possibilities e.g. creation of an internal network within the Commission, network of correspondents of Member States, did not meet the objective qualitative criteria (transparency, cost efficiency and visibility), nor the added-value of the creation of an regulatory agency type of structure.

The first alternative not being achievable as the Commission does not have the necessary expertise on network and information security in-house. The latter, a network of national correspondents, has major disadvantages as

[20] For further information, see separate ex ante evaluation.
[21] For further information, see separate ex ante evaluation.

- the Commission looses its supervisory functions of the work a network would require more financial and human resources as the functions will not be centralised, but multiplied in all Member States.

- awareness on the trans-national dimension is limited, as one can expect that national authorities will primarily focus on national concerns

- visibility of the work is limited and not offering a single point of contact for international discussions, which are absolutely necessary in this area.

As a result the current proposal is following the structural outline as indicated in the recently adopted Commission Communication on an operating framework for European Regulatory Agencies (COM(2002)718 final of 11 December 2002). The primary goal is to focus activities (as can be deducted from the task list) on regulatory issues and at the same time providing support to Member States and the Commission on highly technical and technological matters related to network and information security.

Such an increased focus and increased visibility of a Community co-ordinated response to ever increasing security threats is particularly necessary after the September 11th events when the issue of network and information security became a high political priority.

5.1.1. Objectives pursued

As so much depends on networks and information systems, their secure functioning has become a key concern. Information systems are crucial for the whole economy, not only for most industry sectors, but also vital for the public sector and for private citizens. The malfunctioning of such systems concerns everybody, individuals, public administrations and businesses.

Security has therefore become a major policy concern. Governments see a widening responsibility for the society and are increasingly making efforts to improve security on their territory. Member States are, however, in different stages of their work and the focus of attention varies. There is no systematic cross-border co-operation on network and information security between Member States although security issues cannot be an isolated issue for only one country. There is no mechanism to ensure effective responses to security threats. Implementation of the legal framework differs. There is a lack of interoperability that impedes a proper use of the security products.

Whilst it is not necessary to achieve full harmonisation of policies, the Union would benefit from increased co-ordination between Member States and a sufficiently high level of security in all Member States. The Internal Market would benefit from a co-ordinated European approach to network and information security and from receiving the compiled know-how from Member States. It would at the same time support innovation and the ability of European enterprises to compete at a global level.

The proposed Agency is intended to enhance network and information security in Europe and to enhance Member States' ability, individually and collectively, to respond to major network and information security problems.

5.1.2. Measures taken in connection with ex ante *evaluation*

The Commission Communication on Network and Information Security: Proposal for a European Policy Approach, COM (2001)298 final proposed a number of measures in order to strengthen information security in Europe. The Council Resolution of 28 January 2002 on a common approach and specific actions in the area of network and information security, developed this concept further. It has however become clear that the current institutional arrangements does not allow to address network and information security appropriately at European level.

The Resolution therefore also welcomes a proposal from the Commission on the establishing of a "Cyber Security Task Force" to respond to network and information security problems. This Cyber Security Task Force has now taken the shape of a time limited regulatory agency.

A number of alternatives to an agency have been considered, but not found adequate for the tasks foreseen for such an entity. A more detailed analyses of the considerations behind the establishment of a new agency can be found in the ex ante evaluation.

5.2. Action lines envisaged

5.2.1. Objectives

The broad objective of the Agency is to create a common understanding in Europe of issues relating to information security that is necessary to ensure the availability and security of networks and information systems in the Union.

The Agency shall be able to:

– provide **assistance in the application of Community measures** relating to network and information security.

– the assistance it provides shall help ensure **interoperability** of information security functions in networks and information systems, thereby contributing to the **functioning of the Internal Market**.

– enhance the capability of both Community and Member States to **respond to network and information security problems**.

The Agency will play a key role for the security of Europe's networks and information systems and the development of the information society in general.

5.2.2. Tasks

The Agency will:

– have advisory and co-ordinating 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 on European level that in a comprehensive manner can collect and analyse data and provide

opinions and advice to support the Community's policy work on network and information security.

– **serve** as a **centre of expertise** to which both Member States and Community institutions can turn to for **opinions and advice on technical matters** relating to security.

– contribute to a **broad co-operation between different actors** in the information security field, e.g. to assist in the follow-up activities in support of secure e-business. Such co-operation will be a vital prerequisite for the secure functioning of networks and information systems in Europe. The participation and involvement of all stakeholders is necessary.

– contribute to a co-ordinated approach to information security by providing **support to Member States**, e.g. on the **promotion of risk assessment** and awareness raising actions.

– 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 co-operation** in this field which becomes more and more necessary as network and information security issues are global.

5.3. Methods of implementation

The proposal is to establish a regulatory agency for an initial period of five years as an entity outside the Commission, "the Agency". The Agency will have legal personality.

The Agency will comprise a Management Board, an Executive Director and an Advisory Board. The overall responsibility for the policy work, management issues and the appointment of the Executive Director lies with the Management Board.

The Advisory Board will be composed of experts and have advisory functions to ensure the close co-operation with Member States and relevant organisations in Member States.

6. FINANCIAL IMPACT

6.1. Total financial impact on Part B - (over the entire programming period)

As the main task for the Agency is to act as a centre of expertise, its staff will itself to a large extent provide the opinions and advice. This also means that the administrative costs for the Agency take up an important share of the overall budget.

6.1.1. Financial intervention

Commitments (in € million to three decimal places)

Breakdown	2004	2005	2006	2007	2008	Total
Contribution to the Agency	2,500	5,000	5,600	5,600	5,600	24,300
TOTAL	2,500	5,000	5,600	5,600	5,600	24,300

6.1.2. Technical and administrative assistance, support expenditure and IT expenditure (commitment appropriations)

	2004	2005	2006	2007	2008	Total
1) Technical and administrative assistance						
a) Technical assistance offices						
b) Other technical and administrative assistance: - intra muros: - extra muros: *of which for construction and maintenance of computerised management systems*						
Subtotal 1						
2) Support expenditure						
a) Studies						
b) Meetings of experts						
c) Information and publications						
Subtotal 2						
TOTAL	0	0	0	0	0	0

6.2. Calculation of costs by measure envisaged in Part B (over the entire programming period)

The table below shows the break down of costs for the Agency during its proposed time of operation. The method of calculation differentiates between the current situation of 15 EU Member States and the entrance of 10 new Member States during the course of 2004. A specification of the figures will be found below in (a) –(f).

		2004		2005		2006		2007		2008		Total	
		EUR 15	EUR +10	EUR 15	EUR +10	EUR 15	EUR +10	EUR 15	EUR +10	EUR 15	EUR +10	EUR 15	EUR +10
Human resources		1,080	0,540	3,132	0,972	3,348	1,404	3,348	1,404	3,348	1,404	14,256	5,184
		(10*108)	(5*108)	(29*108)	(9*108)	(31*108)	(13*108)	(31*108)	(13*108)	(31*108)	(13*108)		
Equipment Furniture		0,100	0,050	0,025	0,020	0,025	0,020	0,025	0,020	0,025	0,020	0,200	0,080
	IT	0,220	0,120	0,480	0,170	0,528	0,200	0,528	0,200	0,528	0,200	2,284	0,770
	Web site	0,150	0,050	0,050	0,000	0,050	0,000	0,050	0,000	0,050	0,000	0,350	0,000
Operations	Publications	0,035	0,010	0,050	0,050	0,050	0,050	0,050	0,050	0,050	0,050	0,235	0,200
	Conferences	0,100	0,000	0,150	0,000	0,200	0,000	0,200	0,000	0,200	0,000	0,850	0,000
	Mission	0,140	0,060	0,200	0,065	0,200	0,065	0,200	0,065	0,200	0,065	0,940	0,260
	Meetings	0,090	0,040	0,165	0,060	0,165	0,060	0,165	0,060	0,165	0,060	0,750	0,240
	Translations	0,160	0,050	0,200	0,250	0,200	0,300	0,200	0,300	0,200	0,300	0,960	1,150
Studies		0,420	0,080	0,550	0,220	0,825	0,300	0,825	0,300	0,825	0,300	3,445	1,120
Total		2,495	1,000	5,002	1,807	5,591	2,399	5,591	2,399	5,591	2,399	24,270	9,004
Rounding off		2,500	1,000	5,000	1,800	5,600	2,400	5,600	2,400	5,600	2,400	24,300	9,000
Total EUR 15 and EUR +10		3,500		6,800		8,000		8,000		8,000		33,300	

(a) Preparatory work

The Agency shall start its operations in January 2004.

Although not directly related to this budget item, there is a budget provided through the Modinis programme in the 2003 Budget[22]. Under the this programme one of the main actions is "improvement of Network and Information Security" and the "preparation for the establishment of the cyber-security task-force", as foreseen in the Council Resolution of 28 January 2002 and in the *e*Europe 2005 Action Plan, through, inter alia, financing surveys, studies, workshops on subjects such as security mechanisms and their interoperability, network reliability and protection, advanced cryptography, privacy and security in wireless communications.

(b) Human resources (incl. buildings and related administrative expenditure)

The Agency will need highly specialised and qualified staff to handle the foreseen tasks. Professionals with corresponding profiles are currently scarce and very sought after in Europe. The Agency shall recruit both from the public sector and the private sector. Its staff shall comprise 31 people, when fully operational with 15 Member States. Five of these shall handle the general management and administration of the Agency, and 26 will be recruited for the operational tasks mentioned in Article 2 of the draft Regulation. The numbers on management and administrative support are based on the experience gathered by existing Community agencies.

Of the 26 staff in charge of operational tasks 1 will constitute the secretariat, and the rest will be recruited with specific experience: 6 from risk analysis and risk management, 6 from network monitoring, 3 from technical components of networks and information systems, 2 from information and communication, 4 from computer incident and response handling and 4 from co-ordination of information security activities conducted by Member State authorities. The composition of these persons is based on a thorough analyses after discussions with security directorates of national authorities and similar security bodies in both private and public sectors, e.g. computer security incident response teams. It takes into account the expected workload and is directly related to the task-list of the Agency. The numbers are reduced to a strict minimum as a result of budgetary restrictions.

When fully operational, the total yearly costs for staff for 15 Member States will be 3,348 M € based on an average Commission staff cost of 108.000 € per official and year, which includes building and related administrative expenditures.

As it is expected that full recruitment will not be reached at once, the table in 6.2 is based on gradual recruitment model of 10 people in 2004, 29 people in 2005 and reaching the full 31 people by 2006.

According to the proposed Article 20, the staff of the Agency shall be subject to the rules and regulations applicable to officials and other staff of the European

---

[22] A political agreement was reached on the Telecom Council on 5 December, the formal adoption will take place at the Telecom Council in March 2003.

Communities.

Field of activity	TOTAL	A-grade	B-grade	C-grade
General administration • Executive director • Financial staff • IT staff • Secretariat	5	 1 1 1	 1	 1
Network and information security experts • Experts • Secretariat	26	 25		 1
TOTAL	31	28	1	2

(c) Equipment costs

Furniture: The procurement of furniture and office equipment will be 0,1 M € the first year and 0,025M€ the following years. Office space and related administrative expenditure are covered in the staff costs.

IT: Given the task assigned to it, the Agency will be a likely target of hacking and other security attacks. It must be sufficiently protected against such threats. Highly advanced IT-equipment with high security will be particularly necessary for this Agency. Because of the need to ensure top-level protection the total cost for IT-equipment per official per year is estimated at an average between 15.500 and 18.000 €. **In total the costs for IT will be 0,22 M € for the 1st year, 0,48 M € for the second year and 0,528 M € p.a. for the following years**

Maintenance of web site: Making information available to both the general public as well as the specialised audience will be a key factor in the tasks of the Agency. This will be done essentially through web based operations. The minimal cost (covering only basic information needs) for this is estimated at 0,15 M € the first year and 0.05 M € in annual costs after that.

(d) Functional costs

Publications*:* As the web site will serve as platform for most of the publications the Agency will however to some extent publish official reports and information material also in paper format, notably for information of the relevant Community Institutions. The costs for such publications are expected to be 35.000 € the first year and 50.000 € the following years.

Conferences*:* 0.1 M € should be used for arranging conferences the first year, 0,15 the second year and 0.2 M € for the following years. These conferences will mainly aim at ensuring dissemination of the results of the work of the Agency to a wider audience, of both public and private entities.

Missions: close networking with Member States as well as, given the global nature of the problem of network security, with third countries are a key part of the strategy of the Agency. The costs for missions to accomplish these tasks is estimated at 0,14 M € the first year and 0,2 M € p.a. for the following years.

Meetings*:* The draft Regulation foresees the creation of a Management Board and an Advisory Board as well as the setting up of working groups. The details of the functioning of these entities (frequency of meetings etc.) will be laid down in the internal rules of procedure of the Agency. However, given common practice, 3 annual meetings of the Management Board and a monthly meeting of the Advisory Board are used as a basis for the calculation of estimated costs.

The total number of meetings of Management and Advisory Board will amount to 15 a year. Meeting room and translations amounts to 7000 € a meeting and travel costs another 700 €. The annual costs is thus 115.000 Euro.

The working groups will probably be established after some time. There will be fewer meetings by expert groups during the first year.

Translation: To cut costs and time taken for translation, the Agency's in-house work and documents for the Commission will be available in just one of the working languages. However, documents to and from the Member States may need to be translated. The cost of these translations will have to be adjusted in light of experience. A sum of 0,16 M € for the first year and 0,2 M € per year for the following years is planned to cover the costs.

(e) Studies and research

The highly specialised nature of network and information security and the changing nature of the networked world will bring new and unforeseen challenges at global level. As the staff of the Agency will be limited it will be necessary use the assistance of outside experts for some tasks. Such outside expertise will be used e.g. for studies that gather data and statistics, impact of technological evolution on the security aspects such as risk assessment and risk management models, the inclusion of results of research activities on future and emerging technologies, and also information on network security solutions developed in third countries.

On the basis of the information gathered, the Agency will notably provide assistance and deliver opinions to the Commission and other competent bodies, propose solutions to enhance co-operation between the actors, contribute to the availability of rapid, objective and comprehensive information, and contribute to the Community approach on co-operation with third countries.

The total cost for studies will be 3.445 M €. For the first years the Agency might not be fully operational and it is estimated that 0,42 M € for 2004 and 0,55 M € for 2005 will be used for studies, while it will amount to 0,825 M € during the following years. The average costs for studies are somewhere between 0,2 M € and 0,3 M €.

(f) Calculations with the 10 new countries

With 10 new countries the number of *staff* will increase correspondingly as there will be a need for Member States involvement and expertise also from the new countries. Such increase will be made gradually with 5 persons in 2004, 9 in 2005 and 13 extra persons in the years 2006-2008. Of those 13 people 10 will be representing the new countries and 3 will have secretarial /over head functions.

The higher number of employees will also increase the need for *furniture and IT equipment* for these persons. The increase of costs for equipment will be linear with the number of new employees, except for the first year when the costs will be higher (see calculations above).

Conferences are not expected to require any further costs with the new countries, but the *publications* will have to be made for a larger audience and will therefore be more costly. There will also be a need for *missions* to the new countries in order to bring them on board in the co-operation and information exchange schemes etc. There will be more people participating in the *meetings* and there will also be an extra need for *translations* with the new countries. The calculations of these costs have been made with the same ratio as with 15 Member States.

The amount dedicated for *studies* will also have to be increased with the new countries, as it is important to get a full picture of the information security situation in these countries and what special needs that might arise in relation to their inclusion in the Union. In 2004 it will be too early for anything but a more basic study, but in 2005 it is important to get the full picture of the new countries, and it will be relatively a higher cost for studies this year.

7. IMPACT ON STAFF AND ADMINISTRATIVE EXPENDITURE

The need for human an administrative resources shall be covered within the allocation granted to the managing DG in the framework of the allocation procedure.

7.1. Impact on human resources

Types of post		Staff to be assigned to management of the action using existing and/or additional resources		Total	Description of tasks deriving from the action
		Number of permanent posts	Number of temporary posts		
Officials or temporary staff	A B C	2 1		2 1	

Other human resources –private sector experts –END -Auxiliaries				
Total	3		3	

7.2. Overall financial impact of human resources

Type of human resources	Amount (€)	Method of calculation *
Officials Temporary staff	324.000	
Other human resources -private sector experts -END -Auxiliaries (give budget line)		
Total	324.000	

The amounts are total expenditure for twelve months.

7.3. Other administrative expenditure deriving from the action

Budget line (number and heading)	Amount €	Method of calculation
Overall allocation (Title A7) A0701 – Missions A07030 – Meetings A07040 – Conferences A0705 – Studies and consultations Other expenditure (specify) -Office space -Running costs	10.000	Approx. 6 missions a year
Information systems (A-5001/A-4300)		
Other expenditure - Part A (specify)		
Total	10.000	

The amounts are total expenditure for twelve months.

Specify the type of committee and the group to which it belongs.

I.	Annual total (7.2 + 7.3)	334.000
II.	Duration of action	5 years
III.	Total cost of action (I x II)	1.670.000 €

8. FOLLOW-UP AND EVALUATION

8.1. Follow-up arrangements

In order to ensure that Community funds are used efficiently, the Commission shall ensure that activities under this Regulation are only engaged upon following public procurement procedures, and that the activities are properly monitored and evaluated.

8.2. Arrangements and schedule for the planned evaluation

The Commission together with the Advisory Board will carry out a review of the working practices of the Agency and the impact of the Agency acting as such. Such a review shall be carried out within three years of the starting date, i.e. before 31 of December 2007.

9. ANTI-FRAUD MEASURES

The control of payments for any service, or studies requested is carried out by the Agency's services 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 made between the Agency and recipients of any payments.