ENISA

General Report 2005

ENISA General Report 2005

ENISA (European Network and Information Security Agency)
P.O. Box 1309, 71001 Heraklion - Crete, Greece
Tel: +30 28 10 39 1280 Fax: +30 28 10 39 1410

Chapter 1. Executive summary

Everyday in the modern Information Society, citizens use mobile phones and computers, at home and in offices. Clearly, we are dependent upon these systems to live and to work smoothly, without threats and technical obstacles.

ENISA's mission in this context is to **assist** the EU and its Member States in making networks and information systems more secure.[1] As the information systems encompass virtually all sectors of society and also the private life of citizens, it is a mission with a substantial economic impact. To fulfil its mission, ENISA acts as a forum for exchange of information for all stakeholders, and for increasing coordination and contacts in Network and Information Security (NIS).

ENISA's structure has ensured excellent work relations between the Executive Director and his stakeholders: firstly, the Management Board, and secondly, the Permanent Stakeholders' Group.[2] This way, ENISA aims at ***bridging the gap*** between governments and the main private owners of the electronic networks and developers of information systems, in a public-private partnership dialogue about responsibilities, roles, problems and solutions.

During 2005, with no delay, ENISA started functioning **as a forum of knowledge exchange**, **by co-organizing or participating in 38 conferences**, and by **publishing an "ENISA Quarterly" magazine** for a common, European Network and Information Security discussion. Moreover, the Agency also delivered the first "**Who's Who" Directory** of Network and Information Security actors in Europe.

Additionally, ENISA fulfils its mission by giving advice to the Commission and Member States on the EU perspective in NIS. The Agency received requests from the Commission, Member States and EU bodies.[3] ENISA also finalised the **first CERT**

[1] See Regulation 460/2004 on scope, objectives and tasks of ENISA, Section 1. http://europa.eu.int/eurlex/lex/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML

[2] See Regulation 460/2004, Section 2 Organisation and Chapter 2.3 and 3.2 of the General Report

[3] For example, ENISA delivered a response in the beginning of 2006 to the request in the form of an Opinion to the Commission on the (Dir 2002/58) "Security Measures of Electronic Communication Service Providers" in the context of unsolicited messages.

map in Europe (Computer Emergency Response Teams) and an **inventory** of 104 European CERTs. Furthermore, ENISA has delivered a first **Awareness Raising Information Package**, spreading best practices in this field, which will be continually updated.

By encouraging increased cooperation on NIS, the Agency contributed to reduce obstacles to the NIS, and in that way also facilitating the smooth functioning of the internal market. This is to the benefit to all users of information systems.

All the achievements of ENISA mentioned above occurred in 2005, during what was labelled as a “year of recruitment”. The Agency did this while moving 2.300 km from Brussels, to its location in Crete, Greece and there setting up its headquarters. ENISA is, in all modesty, content, but not yet satisfied. Therefore, it is setting new, ambitious targets for 2006.

1.1 Message of the Executive Director[4]

Dear Members of the Management Board, 2005 has been a decisive year for ENISA towards reaching administrative and operational autonomy.
As Executive Director, I've had the pleasure of witnessing the evolution of ENISA. We have rapidly grown from being a small team with only a few staff members, into to becoming a fully fledged organisation, based in Crete.

Since 1 September 2005, we have been operating ENISA at full speed from our headquarters in Crete in fulfilling the tasks that the European Parliament and the Council assigned to the Agency. Adapting and expanding from a small group of pioneers in January 2005 into the new and larger organisation has been an inspiring challenge. New team members have been signing on to this ship along the way, totalling to 35 temporary agents**.** In addition, four contract agents and, for a while, seven Seconded National Experts were part of our team, of which two later became Temporary agents. Being part of building up the administrative structure and the operative organisation of a new agency is an opportunity that only occurs a few times in life. Therefore it was a source of motivation for all new recruits.

This General Report mainly focuses on the ***operational tasks and deliverables*** that ENISA accomplished, at the same time as it has been resettling twice during its first year. We achieved all deliverables stipulated in the Work Programme of 2005, (see 1.2) plus a few "extra miles":

- Establishing an EU25 Member States' **National Liaison Officers (NLO) network**,
- Introducing **Country Pages**, for an increased exchange of knowledge
- Producing the **ENISA CERTs in Europe map**
- Issuing the **ENISA Quarterly magazine**.

All together, these combined deliverables and extra efforts detailed in the following report, will portray our determined efforts of bringing the European Network and Information Security actors closer to each other , in order for ENISA to become a "hub" for exchange of NIS-information.

[4] See Regulation 460/2004, article 7, for full overview of the ED's responsibilities.

Finally, I thank the EU institutions, in particular the Commissioner for Information Society and Media, Madame Viviane Reding, DGINFSO and DIGIT for the support they provided to ENISA and for the patience they exerted in the difficult moments of the initial life of the Agency. I moreover thank the Management Board members, the Permanent Stakeholder's Group, the Working Group members and the National Liaison Officers for their valuable contributions and input upon which ENISA is dependent in order to become a Centre of Excellence in NIS. I am also grateful to the Greek government and the local authorities in Crete for their assistance and for facilitating our establishment during our first, successful year.

Our primary target audience, for which we work daily, is the EU Member States, the EU institutions and the stakeholders, but the ones that finally may benefit from our efforts are the citizens of Europe, as interconnected information networks stretch into our daily lives of digital banking, hand held devices and computers.

Andrea Pirotti, Executive Director, ENISA

1.2 ENISA 2005 Work Programme achievements

The following tasks were stipulated in the Work Program for 2005 and have been delivered by the Agency:

Work Package (WP) 1.2 Budget and Financing

WORK PACKAGES	DELIVERED	FOR FURTHER DETAILS
✓ Decisions concerning the staff implementing rules including those related to the grading of staff, their allowances and general conditions.	Yes	Chapter 2: 2.8 Human Resources
✓ Initial organisation chart	Yes	Chapter 2: 2.4 Organisational Chart
✓ Two waves of Temporary Staff recruitment process, involving CV evaluation, interviews and contract preparation	Yes	Chapter 2: 2.8 Human Resources
✓ Recruitment of interim staff to support administrative setting (secretarial support and assistance both on human and financial matters)	Yes	Chapter 2: 2.8 Human Resources
✓ Staffing policies and recruitment procedures designed to attract and retain key specialists and skilled managers.	Yes	Chapter 2: 2.7/2.8 Administrative and legal framework/Human Resources
✓ Recruitment of seconded national experts (SNE)	Yes	Chapter 2: 2.8 Human Resources

WP 1.3 Management support and Logistics

WORK PACKAGES	DELIVERED	FOR FURTHER DETAILS
✓ Implementing and testing the various IT supportive budgetary and financial systems. (Licences)	Yes	Chapter 2: 2.7 Administrative and legal framework
✓ Financial circuits, workflows and procedures for the Agency in accordance to Community rules	Yes	
✓ Establishment and Structure of the Budget and its implementation.	Yes	
✓ ABAC (Accrual Based Accounting) new accounting rules and related software tools.	Yes	
✓ Cut-off financial methodology signed by the Executive Director and DG INFSO.	Yes	
✓ Accounting procedures and reporting, external audit and discharge.	Yes	
✓ Budget monitoring and execution	Yes	

WP 2.1 Information and Communication

WORK PACKAGES	DELIVERED	FOR FURTHER DETAILS
✓ Enhanced web page easily updated and gradually turned into a preferential vehicle for Agency's communication.	Yes	Chapter 3:3.6 Communication activities
✓ Activities, advice and preparing communication strategies in order to give visibility to ENISA and its relevant activities and organise annual events dedicated to network and information security	Yes	

WP 2.2 Awareness raising, best practices and Network of Contacts

WORK PACKAGES	DELIVERED	FOR FURTHER DETAILS
✓ Compilation of "sample material" collected by the seconded national experts	Yes	Chapter 3:3
✓ Prepare information packages on security on prime use applications on the basis of material collected and conclusions of ad hoc working group on the subject.	Yes	
✓ Use the results of the inventory study as a source of information for establishing a network of contacts or directory on "who is who in info security"	Yes	
✓ Organise meetings with members of the network of contacts who would be prepared to act locally on the dissemination of customised packages.	Yes	

WP 3.1 Enhancing Co-operation-Information Sharing

WORK PACKAGES	DELIVERED	FOR FURTHER DETAILS
✓ Create a number of ad hoc working groups to address topics of common interest (to be discussed also with the PSG)	Yes	Chapter 3:3.1-3.5
✓ Initial recommendations from the WGs	Yes	

WP 3.2 Co-operation on European Initiatives

WORK PACKAGES	DELIVERED	FOR FURTHER DETAILS
✓ Establish an inventory of NIS-relevant European initiatives and propose enhanced co-operation mechanisms between them.	Yes	Chapter 3.1.2-3.1.4
✓ Promote best practices concerning creation of CERTs/CSIRTs and similar information sharing entities (WARPs).	Yes	Chapter 3.3.1-3.3.4

1.3 The Extra Mile- achievements beyond the 2005 Work Programme

ENISA also achieved some "extra miles" deliveries that are worthy to be highlighted and given some extra attention in this report, as they did not constitute part of the Work Programme for 2005:

- ENISA established a National Liaison Officers (NLO) network, with 25 EU Member States
- ENISA introduced Country Pages, for an increased exchange of knowledge, reports, etc, with the support of the NLO.
- ENISA issued 3 editions of the ENISA Quarterly, reaching thousands of experts, government/EU-actors and stakeholders, working in the field of Network and Information Security, and in that way creating a platform for top level discussions in this field.
- ENISA produced the ENISA-CERTs in Europe map to visualize the local coverage of Computer Emergency Response Teams.

Chapter 2. Building up a new Agency

2.1 History of ENISA- the first steps

The European Council concluded in Stockholm in the spring of 2001, that the Council together with the Commission were to develop a comprehensive strategy on security of electronic networks including practical implementing action. In response, the Commission drafted a Communication entitled Network and Information Security Proposal for A European Policy Approach.[5]

It was later followed up by a resolution, dated 28 January 2002 on a common approach in the area of Network and Information Security and welcoming the intention of the Commission to set up 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*".

As a follow up reaction, the European Parliament adopted an opinion where they strongly requested a European answer to the increasing security problem. The Commission considered how, legally, this task force could be set up, and it turned out that the only practically and legally viable solution was to set up a European agency. The initial idea had been to set up something more "light weight", but as there where no adequate legal forms for this, the Commission presented its Proposal for a Regulation to the European Parliament and to the Council, for the establishment of the European Network and Information Security Agency in 2003 (COM/2003/63 final), which the European Parliament voted for in the first reading during the Italian EU Presidency in 2003. After completing the co-decision procedure, the proposal was

[5] Communication (COM(2001) 298 final, 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).

then formally adopted on 10 March 2004, and thus became the founding regulation 460/2004 for ENISA, which strictly regulates the mission of ENISA.

2.3 Management Board and Permanent Stakeholders' Group

2.3.1 Description and work to date

The Vice Chairman Mr Ferenc Suba, The Chairperson Mrs Kristiina Pietikäinen, and the Executive Director, Mr Pirotti, March 2006.

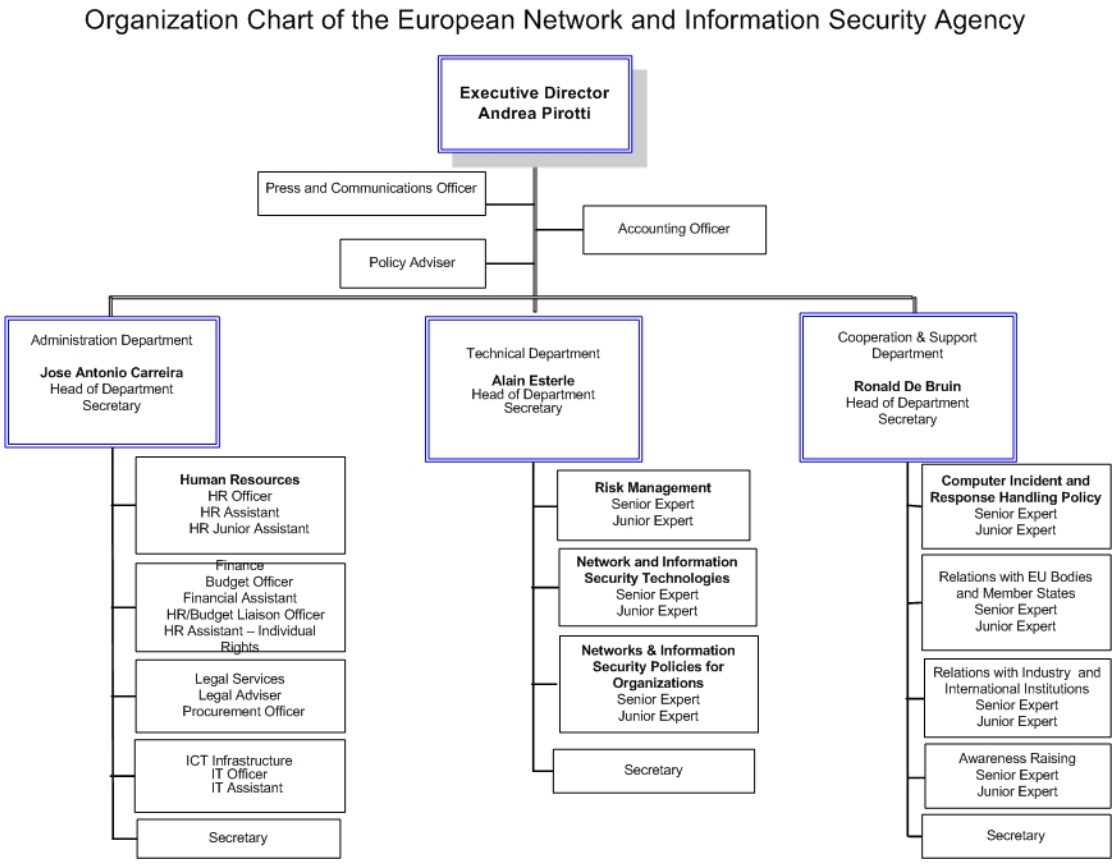
Mrs Luisa Franchina, Mr De Lange, and Mr Pirotti, Rome, October 2005

The **Management Board** is one of the three founding pillars of ENISA, with the **Permanent Stakeholders' Group** (see 3.2 and Regulation 460/2004 art. 8[6]) and the **Executive Director** (See Regulation art. 7 and introduction message 1.2) being the two others. The Management Board is composed of representatives of the EU25 Member States, plus three Commission representatives, three stakeholders without voting right (from research and academia, the ICT industry and the consumer's organizations) and finally, three observers from the EEA Member States. During 2005, the Management Board met twice and decided upon; the adoption of the Work Programme for 2005 and the 2005 budget, appointed the Accounting Officer and supported the Executive Director's decision for an early move to Crete. Other matters were the Management Board's input was instrumental were; proceeding with the deliberations for a Draft decision on Access to Documents, and the related topic of Confidentiality rules, as well as proceeding with the Request Handling Procedures. Moreover the Management Board gave direction on the National Liaison Officers

[6] http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML or Annex 7, Reg. 460/2004

network, and the Working Groups, the draft Budget as well as Work Programme for 2006. The minutes and decisions of the Management Board's meetings are available on the ENISA website.

2.4 Organisational Chart of ENISA in 2005



2.5 Physical Infrastructure

First row: Mr Ferenc Suba, ED Andrea Pirotti, Mr Fabio Colasanti,
Second row: Mr Edgar De Lange, Mrs Anja Diek, Mr Voudoris,
Signing of the Seat Agreement, 22 April 2005.

During the past year the Agency had to move its headquarter twice. The first time, in February 2005 with great support of DGINFSO and DIGIT, from the initial Brussels premises in Beaulieu, to another Commission building at rue de Belliard, as the original premises no longer were able to accommodate an expanding organisation. In March 2005, the Greek government informed the Agency that all necessary infrastructure would have been made available in Heraklion (Crete) by the beginning of July 2005. Therefore, the Greek government invited the Agency to move there promptly. The Executive Director, with the support of the Management Board, took the decision to move to Crete in August 2005, in order to start operations on 1 September.

During the summer of 2005 ENISA moved to Crete. ENISA's premises, surrounded by an olive grove, are located in the campus of one of the major research centres of Greece, namely FORTH.

ENISA offices in Crete on 14 August 2005.

The Agency agreed with the Greek Ministry of Transports and Communications to receive the complete furniture settings and IT and office equipments and to pay back those items after an open and transparent procurement, carried out by the Greek Government itself – following a national law passed specifically for this purpose.

Thanks to the support of the Greek Ministry of Transports and Communications and the FORTH's Institute for Computer Sciences (ICS), the premises were equipped in August and made ready to welcome on time the newly recruited staff. The Agency started its operations in Heraklion on 1 September 2005, as planned.

ENISA "starting school" on 1 September 2005.

2.6 Technical Infrastructure

The technical infrastructure of ENISA during 2005 was focused on:

- Setting up the ICT section and assign roles and responsibilities,
- Complete the setup and installation of the ICT infrastructure,

ENISA IT Officer Oliver Monballiu setting up the computer system 14 August 2005.

- Ensure the security of the ENISA network,
- Document the ICT infrastructure,
- Define the IT policies and procedures,
- Provide user training.

2.7 Administrative and legal framework

The administration had a vital role to play in overcoming administrative hurdles for a new Agency, in order to get the Agency running at full speed. The administrative work has thus been focused on getting the necessary administrative framework and procedures into place. This includes e.g.:

- establishing procedures for handling tenders,
- establishing staff and recruitment administrative procedures,
- contracting consultancies,
- putting into place an administrative agenda of financial circuits, workflows and procedures, accounting into place,
- recruiting Temporary and Contract Agents.

ENISA received financial independence from DGINFSO as of 1 May 2005. Planning and implementation of a decentralized model for financial management, including setting up financial software, new workflows, delegation of authority and financial actors has also been of high priority for the administration. Staff training in financial management systems, including SI2, has also been executed.

The Procurement and Legal Service has drafted ca 20 procurement contracts and provided guidance as necessary on legal issues associated with procurement actions.[7] The procurement activities have been focused on the following activities:

- Improving Procurement performance (maximize the ratio of good value for money),
- Establishing ENISA's needs for quality, timing and compliance with Financial Regulation and Implementing Rules,
- Increasing common understanding of the procurement directives, regulations, and internal rules.

The procurement activities included e.g.:

- Developing of internal procurement strategies, policies and guidelines,
- Receiving, analysing and consolidating procurement requests,
- Preparing invitations to tender, drafting contracts, supporting the evaluation of tenders, awarding contracts and monitoring a post-award performance,
- Organizing the Purchase Order register and archiving of original PO and related documents,

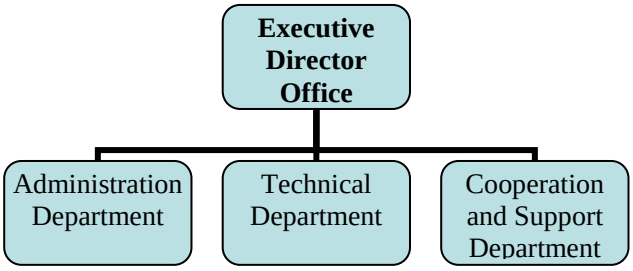
[7] Overview of executed procurement procedures

Negotiated procedures:	Twelve (12) Service and/or Supply contracts were concluded with the following Suppliers: ING, Foenix Metrolofe, Vodafone, Fonema SpA, EEMA, Giaourakis Office Depot, UAB AAA Astorija, ADECCO, M&S Associates LLC, Giorgos Konstantinopoulos, Stefanakis Kiamos.
Restricted procedure	Two (2) Service Contracts were signed with Venus International and Travel Agency Triaema.
Open procedure	One (1) Service Contract with Eworx was concluded.
Purchase Orders	Establishing and maintaining of Purchase Orders archive.

- Organizing internal training in cooperation with Procurement Officer from other agencies.

2.8 Human Resources

Recruiting the staff has been a major administrative achievement of the administration in 2005. As a matter of fact, 2005 was labelled as a "recruitment year". Taking into account the tasks of the ENISA,[8] the organisation of the Agency has been structured into three departments:



The establishment plan of ENISA appended to the budget of the Agency foresees 38 temporary agent posts in 2005, divided in the following three departmental categories above. All posts were published in 2005. This distribution takes into consideration the important role of the Administration Department as support to the two operational departments in the starting-up phase of the Agency:

DEPARTMENTS	Total	Category A*	Category B*	Category C*
Directorate	3	3	0	0
Administration Department	15	7	5	3
Technical Department	9	7	0	2
Cooperation and Support Department	11	8	1	2
TOTAL STAFF	**38**	**25**	**6**	**7**

In order to reach the number of 38 temporary staff by the end of 2005, the HR Unit of the ENISA organised two "recruitment waves" during the first half of 2005. This decision took into consideration one of the most important principles of recruitment procedures of temporary agents, which is the integration of new staff into the structures of the Agency and the move of the Agency to its final location in Heraklion, that was planned for July/August 2005. Therefore, it was not advisable to recruit staff all at the same time, and two waves of recruitment were organised in the first semester of 2005.

The following table depicts the composition and recruitment of the total workforce of the Agency in a chronological way:

[8] (As stated in Article 3 of the Regulation (EC) N. 460/2004 of the European Parliament and of the Council establishing the European Network and Information Security Agency.

	Total employees	*Temporary agents*	*Contract agents*	*Interimaires*	*SNEs*
1 Jan 05	**6**	5	0	1	0
1Feb 05	**11**	5	1	0	5
11 Mar 05	**16**	5	1	3	7
1 Apr 05	**20**	5	1	7	7
1 Sep 05	**28**	25	0	0	3
1 Oct 05	**40**	31	0	6	3
1 Dec 05	**52**	35	4	10	3

Three posts remained to be filled, as the appointed candidates declined the offers made to them:

- HR Assistant
- HR Assistant – Individual rights
- Senior Expert in Relation to Industry and International Institutions.

For further details, please see graphs in Annex 6: Recruitment.

2.9 Budget and accounting

ENISA's budget is funded from a European Community subsidy. Since financial autonomy was granted to the Agency by the European Commission on 1 May 2005, as the required financial actors, systems and procedures were in place, the Agency's first financial year comprises the period 1.5.2005 – 31.12.2005. More, the fact that vast majority of the staff of the two operational Departments took duties in September 2005, prompted the necessary creation of an operational structure and functions for the Agency which were reflected in an amended budget 2005 approved by the Management Board at the end of last year.

The budget of the Agency is distributed in three parts or "titles".
Title 1 covers staff expenditure such as salaries and costs associated to recruitment procedures. **Title 2** covers the functioning of the Agency such as infrastructure, equipment and IT needs. And, **Title 3** corresponds to operational activities.

The execution of the budget has been proceeded with in line with the Agency's Financial Regulation, which is in compliance with the Financial Regulation applicable to the general budget of the European Communities (EC) No 1605/2002 of 25 June 2002.

The Commission transferred a total amount of 4.400.000 euros to ENISA, for the 8-month period (from 1 May 2005 until 31 December 2005) which has been the only source of income for the Agency during the same period.

ENISA put a budget management system into place (SINCOM2) that is applies to all operations proceeded in the Agency, in order to manage all its revenue and expenditure. Financial reporting has been further improved and reinforced by the introduction of a system called Business Objects. The finance data of the Agency is located in a data warehouse shared by several Agencies and located in DG BUDG.

This data warehouse keeps the history of all ENISA's financial transactions and allows to build reports on demand through web interfaces. The Agency also put in place electronic payment systems for a secure payment cycle.

By 1 March 2006, ENISA submitted the **provisional accounts** and the budgetary outturn for the financial year of 2005 to the Court of Auditors. The Court of Auditors shall make its observations by 15 June at the latest. Based on this, the Executive Director will submit the final accounts and the budgetary outturn for the year by 1 July to the Management Board, to the Commission, to the Budgetary Authority and to the Court of Auditors. After the submission of the final accounts, the European Court of Auditors will issue an Audit Report on the Agency's accounts and financial operations for the year 2005.

BALANCE SHEET
31 December 2005

ASSETS

	2005	2004
A. NON CURRENT ASSETS		
Intangible fixed assets		
Computer S/W	11.971	-
Tangible fixed assets		
Plant and equipment	107.692	-
Computer hardware	206.211	-
Furniture and vehicles	18.295	-
TOTAL NON CURRENT ASSETS	**344.168**	**-**
B. CURRENT ASSETS		
Short-term receivables	13.276	-
Cash and cash equivalents	2.510.050	-
TOTAL NON CURRENT ASSETS	**2.523.326**	-
TOTAL ASSETS	**2.867.494**	-

LIABILITIES

	2005	2004
A. CAPITAL		
Accumulated Surplus/Deficit		
Result for the Year	1.098.252	-
TOTAL CAPITAL		
D. CURRENT LIABILITIES		
EC Pre-financing Received	149.144	
EC Interest Payable	32.073	
Accounts Payable	755.903	-
Accrued Liabilities	832.121	-
TOTAL CURRENT LIABILITIES	**1.769.241**	-
TOTAL LIABILITIES	**2.867.494**	-

ECONOMIC OUTTURN ACCOUNT
For the year ending 31 December 2005

	2005	2004
Subsidy from EU general budget	4.250.856	-
TOTAL OPERATING REVENUE	4.250.856	
Administrative Expenses		
Staff Expenses	-1.039.738	-
Fixed Assets Expenses	-31.273	-
Other Administrative Expenses	-1.563.158	-
Operational Expenses	-517.973	-
TOTAL ADMINISTRATIVE AND OPERATIONAL EXPENSES	-3.152.143	-
SURPLUS/(DEFICIT) FROM OPERATING ACTIVITIES	1.098.713	-
Financial Operations Revenue		-
Financial Operations Expenses	-460	-
SURPLUS/(DEFICIT) FROM NON OPERATING ACTIVITIES	-460	-
SURPLUS/(DEFICIT) FROM ORDINARY ACTIVITIES	1.098.252	-
ECONOMIC RESULT FOR THE YEAR	**1.098.252**	**-**

CASH FLOW TABLE
For the year ending 31 December 05

Cash Flows from operating activities	
Surplus/(deficit) from operating activities	1.095.713
Amortization (intangible fixed assets)	2.257
Depreciation (tangible fixed assets)	29.016
(Increase)/decrease in Short term Receivables	-13.276
Increase/(decrease) in Accounts payable	1.591.024
Increase/(decrease) in Liabilities related to consolidated EC entities	181.217
Net cash Flow from operating activities	**2.885.951**
Cash Flows from investing activities	
Purchase of tangible and intangible fixed assets	-375.441
Net cash flow from investing activities	**-375.441**
Financing activities	
Financial expenses	-460
Net Cash Flow from financing activities	**-460**
Net increase/(decrease) in cash and cash equivalents	2.510.050
Cash and cash equivalents at the beginning of the period	0
Cash and cash equivalents at the end of the period	**2.510.050**

STATEMENT OF CHANGES IN CAPITAL
For the year ending 31 December 05

Equity	Reserves		Accumulated Surplus / Deficit	Economic result of the year	Total Equity
	Fair value reserve	Other reserves			
Balance as of 1 January 2005 (restated)	0	0	0	0	0
Other revaluations	-	-	-	-	-
Reclassifications	-	-	-	-	-
Allocation of the Economic Result of Previous Year	-	-	-	-	-
Amounts credited to Member States	-	-	-	-	-
Economic result of the year	-	-	-	1.095.252	1.095.252
Balance as of 31 December 2005	0	0	0	1.095.252	1.095.252

Chapter 3. Operational activities of ENISA

3.1 Relations with EU institutions and Member States

Mr Pirotti and Mr Salerno, Head of Cabinet at the Italian Ministry of Communications, October 2005,

Mr Pirotti and Mrs Luthanen, former Finnish Minister of Communications, February 2005

3.1.1 Why are relations with EU bodies and Member States important?

ENISA acts as a centre of expertise, advising and assisting the European Union bodies and Member States through fostering information exchange and cooperation between all stakeholders. Hence, it is essential to establish, maintain and develop relationships with and between the EU bodies and Member States. Consequently, in its structure the ENISA Management Board notably comprises delegates for the EU Member States and the Commission (as well as stakeholders, see 2.3 and 3.2, and observers, see 2.3). Moreover, the Agency has created a "Who is Who" Directory, published "Country Pages" on its website, established a network of "National Liaison Officers" and promptly managed requests from the Commission and Member States.

3.1.2 Network of National Liaison Officers

ENISA has set up a network of "National Liaison Officers" (NLO). Although not formally based on the ENISA Regulation, this network is of great value and importance to ENISA, as the National Liaison Officers serve as ENISA's primary contact point into the Member States. On the other hand, ENISA gives the NLO the

possibility of reinforcing the activity of the Agency in the Member States, and to exchange information amongst themselves.

In order to build up good and stable working relations as well as team-spirit in the NLO network ENISA organised a meeting on 18 November 2005, attended by 21 NLO. A main goal of this meeting, which was preceded by seven regional meetings throughout 2005, was to give first hand information about ENISA. On the other hand, ENISA could learn about the expectations of the Member States. ENISA provided an overview of its activities, after which key-priority areas were highlighted.

The second part of the meeting was about informing the Liaison Officers of the activities in the field of NIS of the three major European Institutions: The Presidency of the EU (held by the United Kingdom during the fall of 2005) representing the Council, the European Parliament and the European Commission.

The Panel on the NLO day, 18 November 2005.

Maria Burroughs, spoke on behalf of the UK about the major points of the EU Presidency in relation to the ICT agenda, such as general recognition of the essential contribution of the role of ICT in the Lisbon Agenda, agreement and launch of a 'radical' i2010 program, follow-up activities in the World Summit on Information Society and in particular matters about Internet Governance.[9]

[9] Mrs. Burroughs reported also about the very successful CIIP Meridian Conference (an EU Presidency and G8 event, co-organised with ENISA), which took place in October 2005, Greenwich, attended by 80 government officials from 30 countries.

Dr. Jorgo Chatzimarkakis, Member of the European Parliament outlined a possible future role of ENISA: the Agency could give a considerable contribution in stabilizing the ICT environment, as a basis to achieve the Lisbon Goals.[10]

Mr. Rogier Holla from the European Commission outlined the various activities of the Commission in the field of NIS, e. g. action plans eEurope 2002 and 2005 about Network Security, and the i2010 action plan with 2006: Strategy for a Secure Information Society.

Mr. Pirotti with the three guests: Maria Burroughs (UK Presidency), Rogier Holla (European Commission) and Dr. Jorgo Chatzimarkakis (European Parliament)

The last part of the event was an internal workshop of the Liaison Officers, where, amongst many other issues, future cooperation methods and possibilities were discussed. All participants stated that the meeting was very productive and a real starting point for further activities. One of ENISA's main goals is to serve as a platform for Member States for exchanging information and experiences, not only by a two way cooperation with ENISA, but also amongst the Member States.

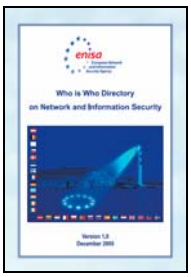
[10] With regard to ICT research, he acknowledged that there is already a lot of work undertaken and ongoing (e.g. ICT in FP6 and FP7, the Galileo satellite project, JRC). ENISA could be seen as a "guard and integrator" in this area.

The National Liaison Officers' Team

Based upon the input from the Member States (through the National Liaison Officers), ENISA has set up and is maintaining "Country Pages"[11] on its website to inform stakeholders about points of contacts and actual activities in the Member States. ENISA managed to have all Member States contributing to this publication.

3.1.4 "Who is Who" Directory

The "Who is Who" Directory is a document, available to the public as download from ENISA website, which provides comprehensive information about contacts and other information of authorities and organizations operating in the field of Network and Information Security in the EU Member States.[12] A printed version of this directory has also been designed and issued at the end of 2005. By end of September, ENISA launched a tender process for a "Who is Who" Database. This database will serve as a multi-purpose database and tool for maintaining a directory of authorities and organizations in the EU Member States and European Bodies.[13]



[11] http://www.enisa.eu.int/country_pages/index_en.htm
[12] http://www.enisa.eu.int/deliverables/index_en.htm
[13] Examples include telecommunications regulators, government information security agencies, but also CSIRTS and the like. Parts of the information in this directory will be published on the ENISA website. In addition, the database will be able to serve as an address stakeholder relationship management system for the internal use of ENISA-staff. The database is expected to be operational by the end of September 2006.

3.1.5 ENISA responding to Requests

ENISA's duty is to handle and respond, at the best of its human resources capacity, to various requests from Member States, the European Parliament and the European Commission. ENISA received three requests in 2005, since starting operations in September.

The European Commission requested the Agency to provide views and opinions on the Draft Impact Assessment Report for the planned Communication on "Increased Security in Electronic Communication."

The Agency received a request from the Communication Regulatory Authority of Republic of Lithuania to support the setting up of the Lithuanian governmental CERT. In response to this request, ENISA co-organised a TRANSITS (Training of Network Security Incident Teams Staff) training course in Vilnius, planned for March 2006. The Agency is co-organising and sponsoring this event also to facilitate training for new CERT specialists across Europe, including but not limiting to the Lithuanian national staff.

Finally, ENISA, upon request from the European Commission at the end of 2005, conducted a study on the technical and organisational measures that electronic communication services providers take with regard to IT security measures and countermeasures against spam. This addressed in particular the EU Directive 2002/58/EC, which has been transposed into national law by the EU Member States in an attempt to harmonise measures in Europe. A questionnaire was sent to National Regulatory Authorities and to electronic communication service providers to understand what specific measures were implemented to put national laws and regulations into practice. The study was concluded by February 2006.

3.2 Relations with industry and international institutions

As electronic communication and information systems mainly are privately owned and developed, industry is a very important stakeholder for ENISA. During 2005 ENISA has begun setting up the appropriate channels to exchange information with various industry sectors in order to be able to maintain a regular dialogue with them. In 2005, a number of bilateral meetings where held with ENISA staff and industry representatives such as ETNO (European Telecommunications Network Operator's association), EICTA (European Information & Communications Technology Industry Association) BSA (Business Software Alliance). The discussions concerned future cooperation and information exchange with industry. Finally, ENISA established preliminary contacts with NIS-representatives for e.g. Japan, Australia, Russia and the US.

Close relations with international organisations active in the area of network and information security also started during 2005. ENISA participated as co-organiser of events together with the ITU (International Telecommunications Union). ENISA also started a dialogue with representatives from the OECD (Organisation for Economic Cooperation and Development) and the Council of Europe to investigate the potential synergies between ENISA's work and the work of these international organisations.

In accordance with the ENISA Regulation, a **Permanent Stakeholders Group** (PSG) was established by the Executive Director, to maintain a regular dialogue with the private sector, consumer organisations, and other relevant stakeholders. After an open call for expressions of interest for experts, the PSG was established on 28 February 2005. Out of a total of 185 applicants, 30 experts were chosen, with proven abilities in the fields relevant to the mandate of the PSG and a capacity to contribute to issues related to the Agency's tasks. The 30 experts cover a broad range of sectors, including the Information and Communication Technology-industries, consumers as well as research and academia in the field of network and information security. The PSG is chaired by the Executive Director.

During 2005 the PSG met three times during 2005, on 28 February, 2 June and 9 December. The main items on the agendas were the visions of the PSG members on Network and Information Security for the coming years, the draft Work Programmes for 2005 and 2006, as well as advising the ED on NIS-matters.

The during the February and June meetings the PSG gave their valuable input on the draft Work Programme for 2005. Also the experts' opinion on ENISA's ad hoc Working Groups was expressed in round table discussions.

During the meeting in December 2006 the PSG discussed their detailed input for the Work Programme 2007. This input was provided well in advance by the members of the PSG, in a form of a completed questionnaire that covered all areas of ENISA's activities. This method of having the PSG to provide elaborate input through electronic consultation prior to the physical meeting proved to be quite successful. Finally, the PSG suggested various methods for improved and even more efficient communication with ENISA.

One of the main items on the agenda of the PSG meetings was the Visions of the PSG members on the future threats of Network and Information Security for the coming years. Based on the fruitful discussions the PSG is preparing a document to summarise their vision, including their expectations from ENISA.

All in all, during 2005 this group of highly respected and recognised NIS-experts assisted the Agency considerably with valuable advice. The PSG is not only valuable because of its input, but also because it is providing valuable NIS contacts and facilitating liaison with the ICT industry.

3.3 Computer Security and Incident Response

3.3.1 What is a CERT and why are CERTs important?

CERT is an abbreviation for the term **C**omputer **E**mergency **R**esponse **T**eam. A CERT is an organization that studies computer and network security in order to provide incident response services to victims of attacks, publishes alerts concerning vulnerabilities and threats, and offers other information to help improve computer and network security.[14]

ENISA, following its regulation, sees the facilitation of CERT cooperation and the enhancement of CERT services by promoting best practices as one of its main tasks. ENISA has to and will take into account work that has already been done in this field by the different CERT communities, and therefore cooperate closely with them.

In the field of CERT cooperation and support, the Work Program 2005 foresaw three deliverables for ENISA:

- setting up an ad hoc working-group on this topic,
- generating an inventory of CERT activities in Europe,
- providing the EU Member States with a clear picture of the CERT situation in Europe along with the level of cooperation and best practices in this field.

These tasks have been delivered as explained in more detail here in after.

3.3.2 Working-group on CERT ENISA cooperation and support

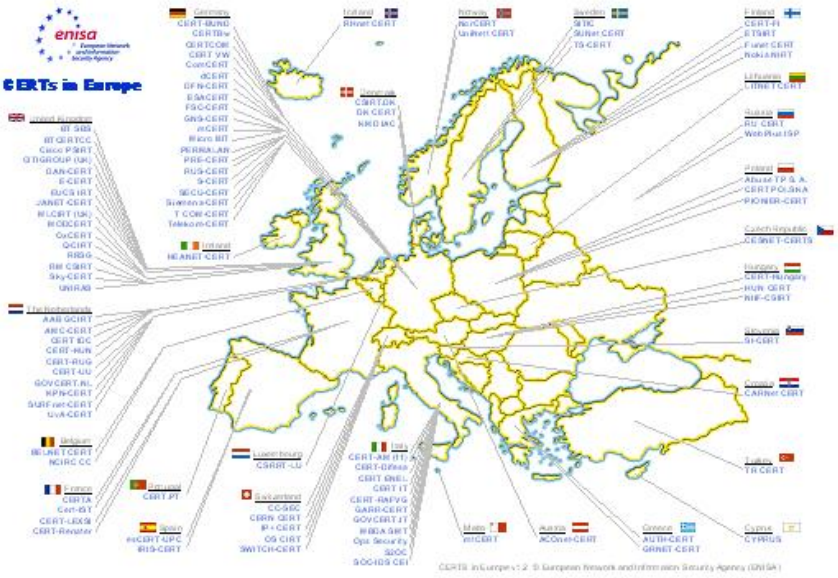
As an ENISA-deliverable, and a special tool for ENISA was the ad hoc Working Group (WG) on CERT-cooperation and support, with nine independent CERT experts

[14] The handling of security incidents, one of the main tasks of a CERT, requires cooperation between teams across institutional and national borders. For this purpose, CERTs have built well functioning communities over the years that meet on a regular basis to discuss technical and operational matters and try to solve problems together. Overall, communities like Terenas TF-CSIRT or the European Government CERT Group EGC are indispensable tools to build bi- and multilateral trust relations by which the exchange of sensitive information – the basis of incident handling – is made possible. A more modern and technically more appropriate term would be **C**omputer **S**ecurity and **I**ncident **R**esponse **T**eam (CSIRT), because over time CERTs extended their services from being a mere reaction force to a more complete security service provider, including preventive services like alerting or education. But as CERT is a widely known “branding name” for not only the teams itself but also the services they provide, this term will be used further on in this text.

met under the patronage of ENISA, in order to support the freshly set up Agency by giving technical advice to ENISA's Executive Director. In three meetings the working-group provided validation of the data stock for the inventory (see next paragraph). The group generated guidelines on how to best establish CERTs and similar facilities and how to enhance CERT-cooperation. Furthermore, they provided ENISA with a **gap analysis** of areas not covered by CERT services. The input was compiled into a final report, as input for the ENISA Management Board.

3.3.3 Inventory of CERT activities in Europe

ENISA, together with the ad-hoc working-group and the CERT community, produced a comprehensive inventory of CERT activities in Europe. Besides lists of known incident response teams this document, which is available from the ENISA website, contains directories of cooperation-, support- and standardisation activities. Also, as an extra supplement, ENISA produced a map, visualizing the local coverage of 104 incident response teams in Europe.[15]

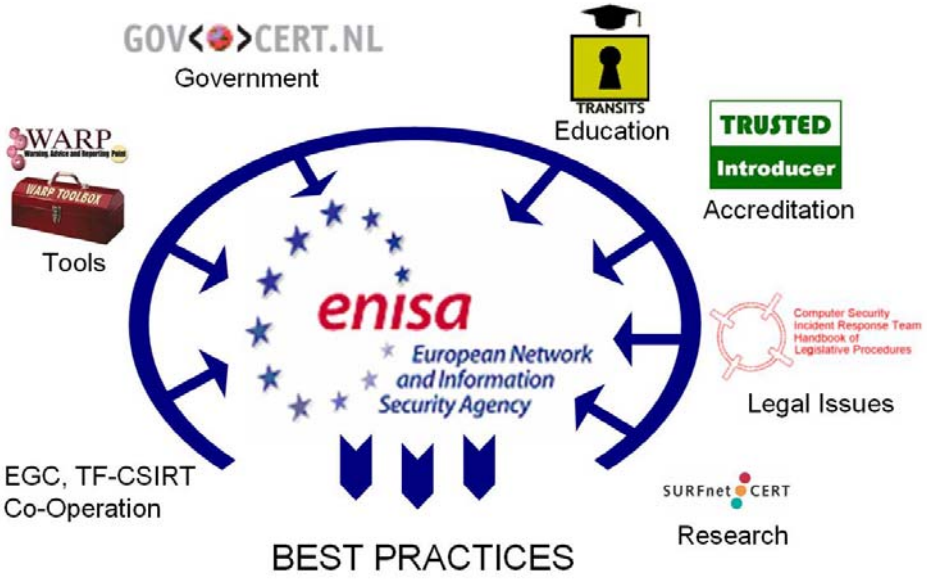


Latest version of the ENISA-CERTs in Europe- map

3.3.4 Workshop on "CERTs in Europe"

[15] http://www.enisa.eu.int/doc/pdf/deliverables/enisa_cert_euromap_v1_2060210.pdf

On 13 December, ENISA gathered representatives from the governments of the EU Member States and the EEA countries to provide them with a status report of the situation in the field of CERT cooperation and support in Europe. In a one-day workshop ten speakers from operational CERTs and various cooperation- and support activities developed a concise, recapitulative overview of the landscape, which ENISA has to take into account in their work in the field of CERTs.[16]



3.4 Awareness Raising

Awareness of the risks and available safeguards are the first line of defence for the security of information systems and networks, as the vast majority of security breaches are the result of a human error rather than technology flaws. In this context, one of the main challenges for ENISA is to facilitate the activities of the EU Member States in raising awareness, and in that way contributing to the implementation of a culture of network and information security. To facilitate raising awareness, ENISA has started to:

[16] Besides these deliverables ENISA initiated contacts with relevant players in the CERT field in Europe: ENISA met representatives from FIRST, TF-CSIRT and the American CERT/CC and Asian-Pacific-CERT. The agency visited WARP communities in the UK and initialised fruitful cooperation with the TRANSITS team, which results in co-organising CERT training courses in Europe in 2006. Also, discussion have been made with the responsible persons for the EU-funded "Legal Handbook for CERTs" regarding the possibilities of handing over the project results to ENISA.

- Collecting material on awareness raising initiatives related to information security,[17]
- Customising information packages for specific target audiences and present them to the Member States,
- Developing a plan to disseminate these customised information packages,
- Setting up an ad hoc Working Group (WG) on Awareness Raising. This WG was asked to:
    - Gather and disseminate information on good examples of awareness through the development of information packages for four priority target groups: silver surfers (citizens sector), SMEs (economic sector), local government authorities (institutional sector), and media (other specific sector). At the end of 2005, the WG submitted its contributions,
    - Provide guidelines on how an information package should be disseminated,
    - Complete an awareness raising road map.

In 2005, the following activities were e.g. carried out in the field of Awareness Raising:

- Dissemination of the main findings among the Member States' representatives

A focused workshop fostered the sharing and dissemination of the main findings among the Member States representatives, as part of the Work Programme 2005[18].

As a deliverable, a first "Information Package: Raising Awareness in Information Security – Insight and Guidance for Members States" was presented.[19] An awareness raising communication strategy was included in the Information Package, highlighting the main process steps and providing tools and templates to optimise the delivery of campaign messages.

---

17 *Identification of best practices and current trends in the awareness raising area*
In order to identify successful practices and learn from measures already underway in the awareness raising field, ENISA has activated relevant stakeholders in the EU Member States. Details on awareness raising initiatives related to information security have been collected. Furthermore, ENISA has looked at materials that were publicly available.

18 The workshop on 14 December 2005 focused on a set of information security challenges affecting SMEs and home users. Through a combination of presentations, case studies and panel debates, participants further explored cutting-edge topics, key issues and emerging good practices. The dissemination workshop has been recognised as a forum to promote an exchange of best practices. http://www.enisa.eu.int/deliverables/index_en.htm

19 The document is to continuously be updated and focused on three target groups: home users, SMEs and media. For each target group, ENISA collected sample material on security of applications of prime use establishing contacts with key stakeholders. The material collected was compiled in a customised information package, providing details on awareness raising initiatives of the Member States related to information security. The Information Package offered insight into the problems and illustrate guidelines to solutions. Reviews of already implemented good practices have revealed:

- The positive influence on the public's behaviour towards information security through Member States' campaigns,
- The need to identify and evaluate the target audience's interests, needs and knowledge properly in campaigns,
- The most appropriate campaign communication channels need to be investigated, so as to optimise the delivery of the campaign message,
- The effectiveness of learning from good campaigning practices for raising awareness in areas outside of information security,
- The need to measure effectiveness as a tool to improve future campaigns,
- The possibility to maximise the potential reach of campaigns, by more co-ordination or partnerships, for example through public-private or cross-Member State initiatives.

3.5 Working Group on Risk Assessment and Risk Management

After starting its operations, the ENISA Technical Department established ad hoc Working Group (WG) on technical and policy aspect on Risk Assessment and Risk Management. Within a series of meetings, the WG has made significant progress towards the generation of the agreed deliverables. By the beginning of 2006, the WG will be in the position to deliver all results described in the Terms of Reference. These results consist of:

- an inventory of existing methods
- an information package for awareness
- a road map document for issues to be considered in the future.

By the end of February 2006, the current appointment of the WG ended. By that time, all results described in the Terms of Reference were delivered. The results of the WG constitute the basis for the ENISA deliverables for 2006 in the area of Risk Assessment and Risk Management as specified in the ENISA Work Programme 2006 and, as such, are of great importance for ENISA.

3.6 Communication activities

3.6.1 Public information and knowledge spreading

In accordance with the job description for the Press and Communications Officer, several contacts with government, stakeholders and EU institutions' Press Officers were made, to establish the principles and policies for a Communication Strategy and communication action plan, exchange of best practices of communication, as well as to lay the fundament for a network of contacts with professionals working with communication in NIS. These contacts also lay the foundation for the Communication Strategy, presented in the end of 2005.

The main tool for ENISA to reach out across Europe with exchange of best practice in the field of information Security is the website. Therefore, a lot of attention was afforded to a web development project launched in July 2005, for developing the initial website, set up and cared for by the Commission. A first phase is focusing on a “look and feel” redesign.[20]

Detail of new website design, displaying dynamism and change in Information Society, with attributes of everyday life, thus, the need for Information Security being paramount in a modern society.

The website was continuously being improved with new features, e.g. photos, video streaming, text content, sign-up function to our publication the ENISA Quarterly, Information Security material and new links.

The public is mainly reached through multipliers of information, i.e. media and the stakeholders at EU and national level. Media was reached through publishing press releases on the web, and by email.[21] During 2005, ENISA created a press release template and released ca 20 press releases on the website since starting operations in September.

[20] An initial analysis of website statistics reveal that during 6 months ENISA had ca 263.000 hits, and ca 60.000 visitors. A subsequent second phase will deal with more advanced and dynamic features (e.g. search functions/ENISA community), while still retaining the specific security measures that ENISA’s mission demands.

[21] For this purpose, a major effort was the building up and establishing of a media news desk register. This media register is continuously being improved and built upon, to increase the reach out to both specialised and general media, and is separated to different national target audiences. In January 2006, it reaches approximately 1000 journalists, interested stakeholders and individuals across the world. Another web communication tool is the statistics of incoming questions, in order to be able to respond to public demand, and by introducing new answers to Frequently Asked Question (FAQ) on the website.

3.6.2 The ENISA Quarterly

As a means to reach information security professionals in Europe, ENISA launched the ENISA Quarterly magazine in 2005.[22] The first edition of this magazine was issued in June, with subsequent ones being published in October and December, steadily improving in quality and in length. The magazine has attracted high quality contributors from across the European Union and the USA, and established itself as a one of the leading information security publications in Europe. At the end of 2005, there were over 500 direct subscribers from all over the world, making the ENISA Quarterly a 5 continents publication, with a steeply increasing subscription curve, beyond preliminary subscription estimates. The print stock of 2.000 physical copies adds to the reach out to the target audiences of ENISA.

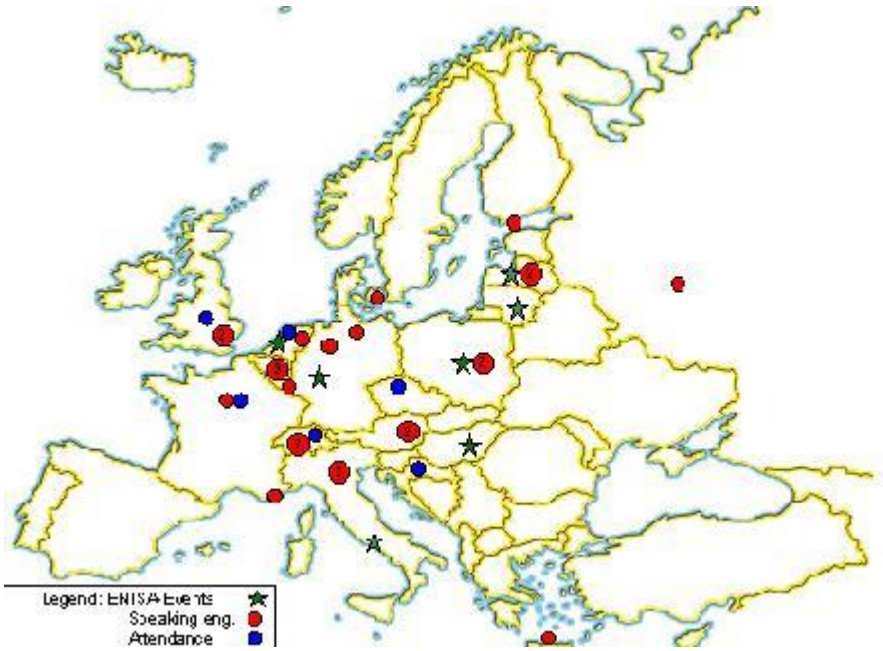
Other publications during the year where ENISA contributed include four Information Security publications.[23] Moreover, some ENISA staff also contributed with individual contributions in the ICT sector magazines. Apart from that, television appearances of the Executive Director occurred in e.g. Finland, Poland, Lithuania, and Greece may be mentioned.

[22] http://www.enisa.eu.int/publications/index_en.htm
[23] CIIP Newsletter, Carlton Publishing, CSIA Newsletter and EuroISPA Newsletter.

3.6.3 Speaking engagements and events

The Executive Director made a dedicated effort during 2005 to promote the establishment of ENISA by speaking at as many conferences as possible. Here speaking in The Hague, Rome, Crete, Budapest, and Lithuania.

ENISA participated in or co-organised 38 events and speaking engagements during 2005, where it contributed to a pan-European discussion on NIS issues. In that way, clarified the Agency's mandate and achievements, and contributed to a European NIS-discussion, as well as building important contacts for the future, to an audience of approximately **6.400** conference attendees.



ENISA geographical distributions of events, speaking engagements and furthermore also conference attendance added.

3.6.4 ISSE2005 focus

An event worth taking note of was the ISSE2005 conference in Budapest, attracting 400 leading experts, academics, business, industry and government actors, laying out the guidelines for key strategic NIS choices. The delegates participated in ca 100 workshops and seminars, exchanged best practices and established contacts, to lay the founding stones for a clearer direction for NIS issues in Europe and an increased cross-European NIS-discussion.

Chapter 4. Outlook for 2006

4.1 Future perspectives

The Executive Director, with the Heads of Department.
From the left: Mr Carreira, Mr De Bruin, the ED Mr Pirotti and Mr Esterle

Looking towards the year ahead, we will be in a phase where ENISA is consolidating and asserting its position as a Centre of Expertise and Excellence in the Network and Information Security community. The importance of Security Economics is likely to gain importance, as information security is the fundament for the Digital Economy that reaches into all sectors of society. Its significance can hardly be overestimated in economic terms. The importance of the Information Society is also underlined as a key factor in the European Commission's i2010 initiative to create more jobs in Europe[24].

Risk-preparedness and awareness is a decisive economic factor in our society, as the interconnected networks are such a vital part of our economies. IT has become an inseparable part of our everyday lives. Ensuring functioning business solutions and safeguarding corporate assets through Information Security is therefore an increasing challenge for governments, industry and stakeholders alike.

[24] (europa.eu.int/information_society/eeurope/i2010/index_en.htm).

The Digital Economy and Information Society have brought us tremendous benefits in terms of innovation, access to information, and freedom in our lives. In “The Future of Ideas,” Lawrence Lessig labelled Internet “the greatest technological revolution …since the Industrial Revolution” and named it the “Power of Freedom”. The Internet is inspiring people to become creative, to cheaper and faster travel worldwide, to do digital banking, play games, buy CDs, books, and films on-line. It is true ”Digital Freedom”.

The security threats and loss of confidence in the Internet, along with spam, spim (e.g. in mobiles), botnets, and denial of service, threatens the entire backbone of Information Society. The unprecedented flow of innovation, fun and creativity thanks to the Internet is at peril without higher NIS-levels. Our IT-dependency both in our professional and our private lives, makes it critical to protect the information infrastructure.

Consequently, since the EU recognized the need for closer cooperation between its Member States in dealing with NIS, ENISA has this mission to fulfil.

During 2006, we will continue to work for NIS at a European level by assisting the efforts of the Member States in encouraging European users and European industry to recognise security risks.

Some samples of our future, 2006 activities are a risk management/risk assessment matrix, a redesigned website for spreading knowledge, an Awareness Information Package for SMEs, a Knowledge Database of best practices, a study on accreditation and certification schemes, a “how to” on setting up a CERT roadmap, and a roadmap for creating a common NIS-language between member states. In 2006, ENISA will also facilitate a CERT course in Lithuania and stands ready for requests from other governmental bodies. It is however worth to mention that ENISA does *not* replace existing national NIS structures.

With these projects, ENISA is fulfilling its mission to assist the EU and its member states in enhancing the functioning of our digital systems and the Internet as sources of freedom, innovation, and creativity for our society.

Finally, our focus for the fall semester of 2006 is firstly, the ISSE 2006 conference, this year taking place on 10-12 October, and secondly, a conference in Helsinki, co-organised with the Finnish EU-Presidency.

ANNEXES

ANNEX 1 Glossary

CERT	Computer Emergency Response Teams. "CERT" is an organization that studies computer and network security in order to provide incident response services to victims of attacks, publish alerts concerning vulnerabilities and threats, and to offer other information to help improve computer and network security. (see also: CSIRT)
CERT/CC	Computer Emergency Response Team Coordination Center (USA)
CSIRT	CSIRT (Computer Security and Incident response Team) Over time, the CERTs (see above) extended their services from being a reaction force to a more complete security service provider, including preventive services like alerting or advisories and security management services. Therefore, the term "CERT" was not considered to be sufficient. As a result, the new term "CSIRT" was established in the end of the '90-ies. At the moment, both terms (CERT and CSIRT) are used in a synonymous manner, with CSIRT being the more precise term.
Contract Agent	Staff assigned to a post which is *not* included in the list of posts appended to the section of the budget relating to each EU institution (see Temporary Agent
DG BUDG	Directorate General for Budget (of the European Commission)
DG INFSO	Directorate General for Information Society
DIGIT	Directorate General for Informatics
ED	Executive Director
FIRST	Forum of Incident Response and Security Teams —a global CERT organisation
FP6/FP7	Framework Programme 6/ Framework Programme 7 (EU Research Programmes)
FORTH	Foundation of Research and Technology - Hellas
ICT	Information and Communication Technology
JRC	Joint Research Centre (of the European Commission)
NIS	Network and Information Security
NLO	National Liaison Officer
PSG	Permanent Stakeholders' Group
SI2	SINCOM2, Financial Management System
SNE	Seconded National Expert (Staff assigned to ENISA for a brief period of time)
Temporary Agent	Staff engaged to fill a post which is included in the list of posts appended to the section of the budget relating to each EU institution.
TERENA	Trans-European Research and Education Networking Association
TF-CSIRT	Task Force - Collaboration of Security Incident Response Teams
TRANSIT	Training of Network Security Incident Teams Staff
WARP	Warning, Advice and Reporting Point. Provides Warning, Advice and Reporting services on Internet security-related matters. Similar to a CERT (see above), but without a capability for responding to incidents (other than providing advice).
WG	Working Group, ENISA Ad hoc Working Group on specific technical issue.
WP	Work Packages (from the Work Programme)

ANNEX 2 Management Board members

List of ENISA Management Board Members and Alternates

European Commission	Representative	Alternate
	Fabio **COLASANTI** Director General - Information Society and Media DG	Michael **NIEBEL** Information Society and Media DG -Head of Unit, "Internet; Network and Information Security"
	Francisco **GARCIA MORÁN** Informatics DG –Director General	Marcel **JORTAY** Informatics DG – Head of Unit, "Telecommunications and networks"
	Gregory **PAULGER** Information Society and Media DG -Director, "Audiovisual, Media, Internet"	Soenke **Schmidt** European Commission DG Justice, Liberty and Security, Legal Advisor - advisor on global security matters

Member States representatives Member State Representative Alternate

Austria	Reinhard **POSCH** Chief Information Officer	Herbert **LEITOLD** Institute for Applied Information Processing and Communication
Belgium	Georges **DENEF**, Membre du Conseil de l'IBPT	Rudi **SMET** Ingénieur-Conseiller IBPT
Cyprus	Neophytos **PAPADOPOULOS**, of the Commissioners Office for the control of the Telecommunications and Postal services	Director Antonis **ANTONIADES**, Senior Officer of the Commissioners Office for the control of the Telecommunications and Postal services
Czech Republic	Jan **Hobza**, Ministry of Informatics of the Czech Republic, r*eplaced by* Vladimir **HOREJSI**, Deputy Minister for eGovernment Ministry of Informatics of the Czech Republic	Lenka **Nezdarova**, Ministry of Informatics of the Czech Republic, r*eplaced by* Vit **LIDINSKY** PAIS Conception and Coordination Department Ministry of Informatics of the Czech Republic
Denmark	Yih-Jeou **WANG** Head of Division National IT and Telecom Agency, *replaced by* Finn **PETERSEN** Deputy Director General National IT and Telecom Agency	Charlotte **Jacoby** Head of Section National IT and Telecom Agency, *replaced by* Flemming **FABER** Head of Division National IT and Telecom Agency
Estonia	Mait **HEIDELBERG** IT-Counsellor of the Ministry of Economic Affairs and Communications of Estonia	Jaak **TEPANDI** Head of the Chair of Knowledge-Based Systems, Department of Informatics, Tallinn University of Technology
Finland	Kristiina **PIETIKÄINEN** CHAIR OF ENISA MANAGEMENT BOARD Unit for E-commerce and Data Security Director of Unit for E-commerce and Data Security information society project	Juhapekka **RISTOLA** Ministerial Adviser Ministry of Transport and Communications Finland E-Commerce and Data Security
France	Henri **Serres** Central Director of Information Systems Security, *replaced by* Patrick **PAILLOUX** Central Director of Information Systems' Security, Prime Minister/General Secretariat of National Defence/DCSSI	Stephanie **SCHAER** Central Directorate of Information Systems' Security, Prime Minister/General Secretariat of National Defence/DCSSI
Germany	Christoph **VERENKOTTE**	Anja **DIEK**

	Head of Division IT-Security Policy, Federal Ministry of the Interior	Division IT-Security Policy
Greece	Constantin **VOUDOURIS** Assistant Professor Department of Electronics Tecnological Educational Institute (TEI) of Athens, *replaced by* Nikolaos **VLASSOPOULOS** Hellenic Telecommunications and Post Commission	Nikolaos **VLASSOPOULOS** Hellenic Telecommunications and Post Commission, *replaced by* Constantin **VOUDOURIS** Assistant Professor Department of Electronics Tecnological Educational Institute (TEI) of Athens
Hungary	Dr Ferenc **SUBA** VICE-CHAIR OF ENISA MANAGEMENT BOARD Head of Department Ministry of Informatics and Communications of the Republic of Hungary	Mr. András **GERENCSÉR** Deputy Head of Department Ministry of Informatics and Communications of the Republic of Hungary
Ireland	Aidan **RYAN** Staff Engineer Department of Communications	
Italy	Luisa **FRANCHINA** Director General for Service Regulation and Quality of the Ministry of Community	Claudio **MANGANELLI** President of the National Technical Committee on Information and Telecommunication Security in public administration
Latvia	Raimonds **BERGMANIS** Director, Department of Communications	Ingrida **GAILUME** Head, General and internat. division Department of Communications, Ministry of Transport and Communications
Lithuania	Valdemaras **SALAUSKAS** Secretary of Ministry of transport and communications	Tomas **BARAKAUSKAS** Director of Communication Regulation Authority
Luxembourg	François **THILL** Accréditation, notification et surveillance des PSC	Pascal **STEICHEN**
Malta	Joseph V. **TABONE** Chairman Malta Communications Authority	Colin **CAMILLERI** Chief Technical Officer Malta Communications Authority
The Netherlands	Herman **Grol** Ministry of Economic Affairs Director-General for Telecommunications and Post, r*eplaced by* Edgar R. **DE LANGE** Ministry of Economic Affairs Director-General for Telecommunications and Post	Edgar R. **DE LANGE** Ministry of Economic Affairs Director-General for Telecommunications and Post, *replaced by* Ronald M. **VAN DER LUIT** Senior Policy Adviser, Ministry Of Economic Affairs
Poland	Krzysztof **SILICKI**, M.Sc. Technical Director Research and Academic Computer Network	Tomasz **Affet**, Ministry of Scientific Research and Information Technology, *replaced by* Edward **SELIGA**, Ministry of Interior and Administration, Department for Information Technology Systems in Public Administration
Portugal	Pedro Manuel **BARBOSA VEIGA** Presidente da Fundação para a Computação Cientifica Nacional (FCCN)	Manuel Filipe **PEDROSA DE BARROS** Director de Tecnologias e Equipamentos da Autoridade Nacional das Comunicações (ANACOM)

Slovakia	Mr. Tibor **Papp** Director, Information Society Division Ministry of Transport, Posts and Telecommunications, *replaced by* Mr. Peter **BIRO** Director Information Society Division Ministry of Transport, Posts and Telecommunications	Mr. Peter **BIRO** Director Information Society Division Ministry of Transport, Posts and Telecommunications, *replaced by* Mr. Ján **HOCHMANN** Director Department of information security and standards, Information Society Division Ministry of Transport, Posts and Telecommunications
Slovenia	Gorazd **BOZIC** Head ARNES SI-CERT	Marko **BONAC** Director ARNES SI-CERT
Spain	Rafael **SAGRARIO DURAN** Director General para el Desarrollo de la Sociedad de la Información	Salvador **SORIANO MALDONADO** Subdirector General de Servicios de la Sociedad de la Información
Sweden	Fredrik **SAND** Naringsdepartementet	Charlotte **INGVAR-NILSSON** Legal Advisor National Post and Telecom Agency (PTS)
United Kingdom	Geoff **SMITH** Head of Information Security Policy, Information Security Policy Team	Peter **BURNETT** National Infrastructure Security Coordination Centre

Stakeholders' representatives	**Group Representative**	**Alternate**
Information and communication technologies industry	Mark **MACGANN** Director General, European ICT & Consumer Electronics Industry (EICTA)	Berit **SVENDSEN** Executive Vice President Technology / CTO of Telenor ASA and chairman of Telenor R&D
Consumer groups	Markus **BAUTSCH** Stiftung Warentest, Deputy Head of Department	Jim **MURRAY** BEUC, Director
Academic experts in network and information security	Kai **RANNENBERG** T-Mobile Chair of Mobile Commerce & Multilateral Security Dept. of Information and Communication Systems Goethe University Frankfurt	Niko **SCHLAMBERGER** Statistical Office of the Republic of Slovenia, Secretary

EEA-country representatives (observers)		
Iceland	Hördur **HALLDORSSON** Director of International Division Post and Telecom Administration of Iceland	
Lichtenstein	Kurt **BÜHLER,** Director, Office for Communications	
Norway	Jörn **RINGLUND,** Deputy Director General Ministry of Transport and Communications Department of Civil Aviation, Postal Services and Telecommunications	Eivind **JAHREN,** Deputy Director General, Department of IT Policy Ministry of Modernisation

Note: Names and titles may not be updated as some appointing authorities are to provide an official letter of notification to ENISA, indicating the exact dates of modification of the representative/or alternate.

ANNEX 3 Permanent Stakeholder's Group members

Name	Country	Organisation
Jaap Akkerhuis	Dutch	NLnetLabs
Charles Brookson	British	Department of Trade and Industry, UK
Giuseppe Carducci Artenisio	Italian	Securteam (Marconi)
Nick Coleman	British	IBM Europe
Andrew Cormack	British	UKERNA
Paul Dorey	British	BP
Philippe Duluc	French	France Telecom
Andreas Ebert	Austrian	Microsoft
Kurt Einzinger	Austrian	ISPA Austria
Cecile Gregoire	Belgian	EuroCommerce
Wim Hafkamp	Dutch	Rabobank
Urho Ilmonen	Finnish	Nokia
Andrzej Kaczmarek	Polish	Polish Data Protection Authority
Sandor Kurti	Hungarian	Kuert Information SecurityGroup
Stephan Lechner	German	Siemens
Petri Lillberg	Finnish	SSH Communications Security
Evangelos Markatos	Greek	ICS - FORTH
Vilma Misiukoniene	Lithuanian	Infobalt Association
Sead Muftic	Swedish	Royal Institute of Technology Stockholm
Magnus Nyström	Swedish	RSA Security
Olivier Paridaens	Belgian	Alcatel
Simon Perry	British	Computer Associates
Norbert Pohlmann	German	University of Applied Sciences Gelsenkirchen
Sachar Paulus	German	SAP
Risto Siilasmaa	Finnish	F-secure
Marta Villen Sotomayor	Spanish	Telefonica
Jacques Stern	French	ENS
Robert Temple	British	BT
Giuseppe Verrini	Italian	Adobe Systems

Anton Zajac	Slovakian	ESET

ANNEX 4 ENISA Ad-Hoc Working Group members

Ad hoc Working Group on CERTs
Gilles ANDRE, SGDN/DCSSI, FR
Henk BRONK, NL
Klaus-Peter KOSSAKOWSKI, Presecure Consulting GmbH, DE
Miroslaw MAJ, Research and Academic Computer Network, PL
Michel MIQUEU,CNES, FR
Gianluigi MOXEDANO, GovCert.it, IT
Sofie NYSTRÖM, Norwegian National Security Authority, NO
David PARKER, NISCC, UK
Tamas TISZAI, Computer and Automation Research Institute, HU

Ad-hoc Working Group on Awareness Raising
Par ANDLER, FI
Ignacio AYERBE GARCIA, ES
Anja HARTMANN, DE
Maylis KARLSSON, SE
Janice RICHARDSON, FR/AUS (Chairperson)
Klaus SCHIMMER, DE

Gigi TAGLIAPIETRA, IT
Peter VAN ROSTE, BE
Christian WERNBERG-TOUGAARD, DK (Vice Chairperson)

Ad-Hoc Working Group on Aspects of Risk assessment and Risk Management
Philippe BOUVIER, Thales Security Systems, FR
Jozsef BREHEL, SeCoN 2000 InfoSeC Inc, HU
Alain DE GREVE, Fortis Bank, BE
Serge LEBEL, Premier Ministre, Dir. Centrale de la Sécurité des Systèmes d'information, FR
Ingrid SCHAUMULLER-BICHL, Self-employed IT security consultant, AT
Juhani SILLANPAA, Ministry of Finance, SF
Massimo SOLARI, Network Integration & Solutions, IT
Marcel SPRUIT, Haagse Hogeschool, NL
Lydia TSINTSIFA, Federal Office for Information Security, DE

ANNEX 5 National Liaison Officers

Austria	Gerald TROST
Belgium	Rudi SMET
Cyprus	Not yet appointed. Currently role shared between Neophytos PAPADOPOULOS and Antonis ANTONIADES
Czech Republic	Vit LIDINSKÝ
Denmark	Charlotte JACOBY
Estonia	Toomas VIIRA
Finland	Tuire SAARIPUU
France	Till December 2005, Stephanie Schaer, now Isabelle VALENTINI
Germany	Anja DIEK

Greece	Georgios DROSSOS
Hungary	Ferenc SUBA
Ireland	Catriona COSTELLO
Italy	Daniele PERUCCHINI
Latvia	Ingrida GAILUME
Lithuania	Tomas LAMANAUSKAS
Luxembourg	Pascal STEICHEN
Malta	Celia FALZON
Norway	Heidi KARLSEN
Poland	Miroslaw MAJ
Portugal	Not yet appointed.(Currently role shared between Pedro VEIGA and Manuel Filipe PEDROSA DE BARROS)
Slovakia	Rastislav MACHEL
Slovenia	Andrej TOMSIC
Spain	Salvador SORIANO MALDONADO
Sweden	Fredrik SAND
The Netherlands	Edgar DE LANGE
United Kingdom	Geoff SMITH

ANNEX 6 Recruitment

The recruitment and selection procedures of ENISA temporary agents were strictly respecting the principles of transparency, objectivity and equal opportunities.[25] In order to ensure full transparency of the process, broad publicity was pursued, and vacancy notes were published:

- On the ENISA website;
- On the website of the European Personnel Selection Office (EPSO);
- On the Intranet of the European Commission;
- On external free websites (i.e. Itaca, Eurobrussels).

Vacancy notices were also sent to Permanent Representations of the Member States to the European Union, to the PSG Members, to the Liaison Officers and to the other European Agencies.

The screening of the applications and the interviews of the best candidates were carried out by a **Selection Committee** of three members (appointed by the Executive Director). The Selection Committees were composed among civil servants of the European Commission (in particular from DG INFSO), temporary agents of other European agencies and the core staff of ENISA.

Contract staff:
A total of four Contract Agents posts were published in July 2005 for the Finance Unit (Financial Assistant and Mission Coordinator), in order to ensure the decentralisation of financial management systems in the Technical and in the Cooperation and Support departments.

Seconded National Expert: The financing and secondment of three National Experts (from Germany, Sweden, and Italy) to ENISA was extended until the beginning of 2006. Two other experts, one from Finland and one from Hungary terminated their time a ENISA in September, whereas two other national experts successfully applied for and became Temporary agents.

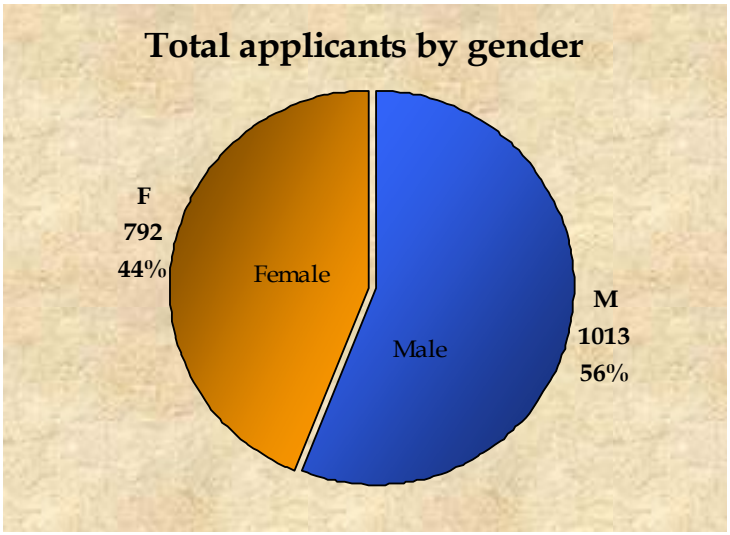
Additional Interim Staff was recruited for a short period of time, to ensure administrative support and reinforce administrative areas (Receptionist, HR, Finance, ICT) as well as other departments, considering the pending recruitment of contract agents. A total of 11 new “interimaires” came on board in September 2005.

The following graphs show some statistics about the applicants for temporary agent posts with the ENISA in 2005. A total of 1.805 applications for 36 posts published in the course of 2005 were received. The graphs concentrate on the three basic indicators:

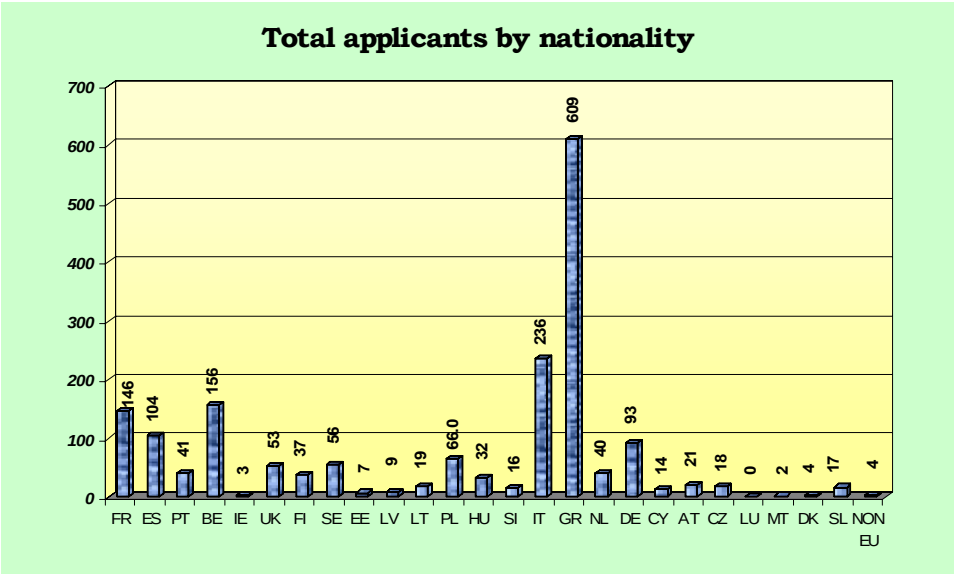
a. Gender of the applicants (male/female);
b. Nationality from the European Member States;
c. Age (considering 5 scales of birth decades).

[25] The recruitments have been done in full accordance with the Staff regulations of Officials of the European Communities and the Conditions of Employment of Other Servants of the European Communities,

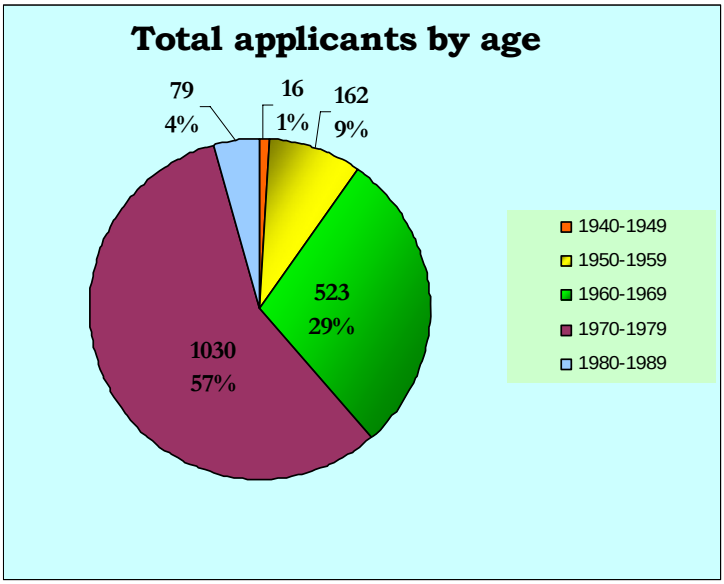
Applicants by gender:



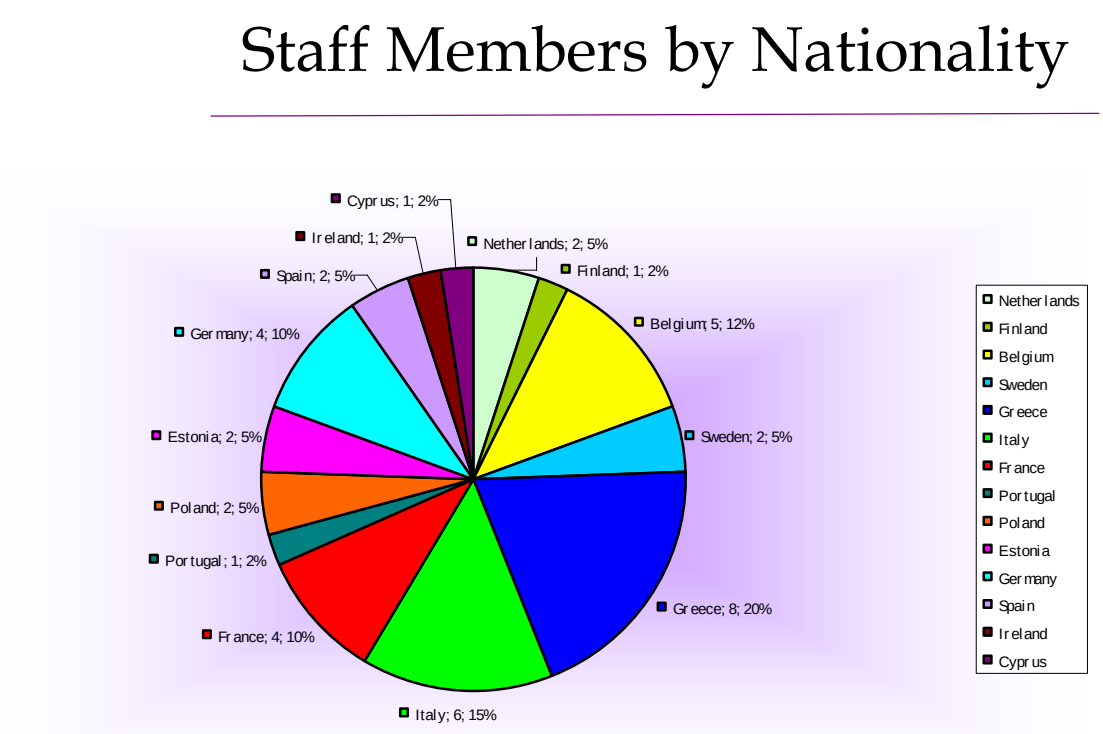
Applicants by nationality:



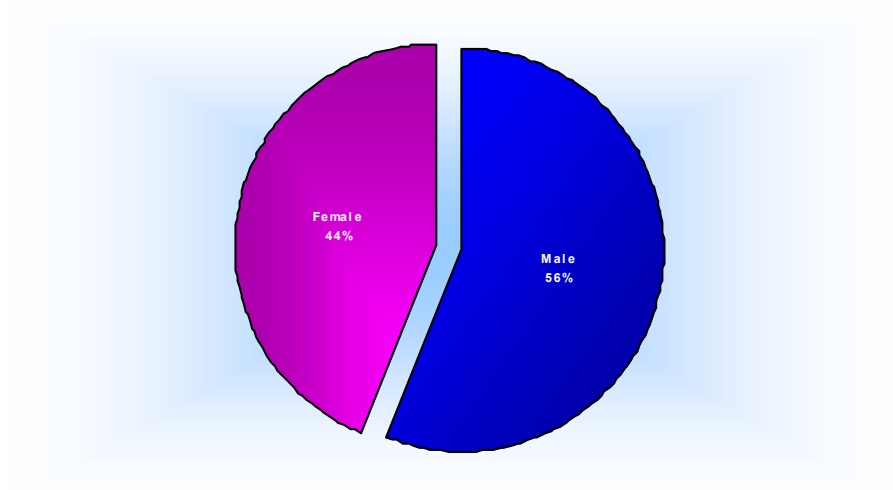
Applicants by age:



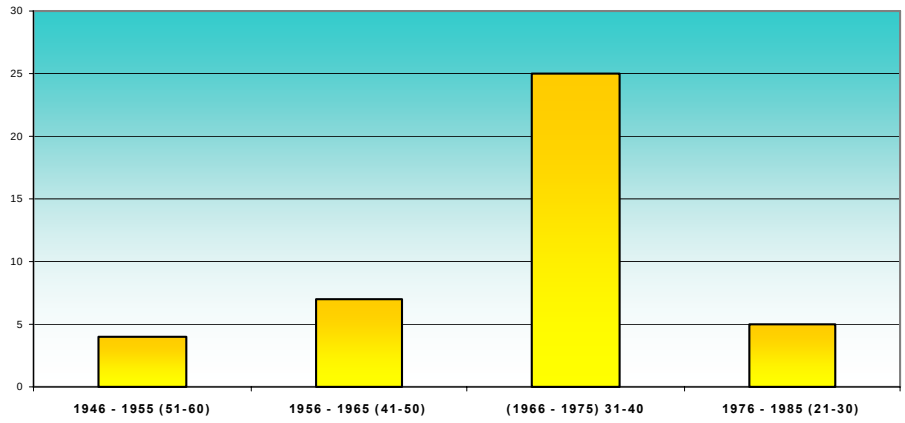
Staff composition:



Staff Members by Gender



Staff Members by Age



5

ANNEX 7 Regulation (EC) No 460/2004

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 (Text with EEA relevance) *Official Journal L 077 , 13/03/2004 P. 0001 - 0011*

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 (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 Article 95 thereof,

Having regard to the proposal from the Commission,

Having regard to the opinion of the European Economic and Social Committee(1),

After consulting the Committee of the Regions,

Acting in accordance with the procedure laid down in Article 251 of the Treaty(2),

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 not least because of the possibility of problems in key information systems, due to system complexity, accidents, mistakes and attacks, that may have consequences for the physical infrastructures which deliver services critical to the well-being of EU citizens.

(2) The growing number of security breaches has already generated substantial financial damage, has undermined user confidence and has been detrimental to 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) 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 risk undermining the smooth functioning of the Internal Market.

(4) 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 (the Framework Directive)(3) lays down the tasks of national regulatory authorities, which include cooperating 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.

(5) Present Community legislation also includes Directive 2002/20/EC(4), Directive 2002/22/EC(5), Directive 2002/19/EC(6), Directive 2002/58/EC(7), Directive 1999/93/EC(8), Directive 2000/31/EC(9), as well as the Council Resolution of 18 February 2003 on the implementation of the eEurope 2005 Action Plan(10).

(6) Directive 2002/20/EC entitles Member States to attach to the general authorisation, conditions regarding the security of public networks against unauthorised access in accordance with Directive 97/66/EC(11).

(7) Directive 2002/22/EC requires that Member States take necessary steps to ensure the integrity and availability of the public telephone networks at fixed locations and that

undertakings providing publicly available telephone services at fixed locations take all reasonable steps to ensure uninterrupted access to emergency services.

(8) Directive 2002/58/EC 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. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data(12), 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.

(9) Directive 2002/21/EC and Directive 1999/93/EC contain provisions on standards that are to be published in the Official Journal of the European Union. 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 track those standards which meet the requirements of Community legislation.

(10) 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. This calls for the creation of a centre of expertise at European level providing guidance, advice, and when called upon, with assistance within its objectives, which may be relied upon by the European Parliament, the Commission or competent bodies appointed by the Member States. National Regulatory Authorities, designated under Directive 2002/21/EC, can be appointed by a Member State as a competent body.

(11) 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 advice it delivers 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 build on national and Community efforts and therefore perform its tasks in full cooperation with the Member States and be open to contacts with industry and other relevant stakeholders. As electronic networks, to a large extent, are privately owned, the Agency should build on the input from and cooperation with the private sector.

(12) The exercise of the Agency's tasks should not interfere with the competencies and should not pre-empt, impede or overlap with the relevant powers and tasks conferred on:

- the national regulatory authorities as set out in the Directives relating to the electronic communications networks and services, as well as on the European Regulators Group for Electronic Communications Networks and Services established by Commission Decision 2002/627/EC(13) and the Communications Committee referred to in Directive 2002/21/EC,

- the European standardisation bodies, the national standardisation bodies and the Standing Committee as set out in Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society Services(14),

- the supervisory authorities of the Member States relating to the protection of individuals with the regard to the processing of personal data and on the free movement of such data.

(13) To understand better the challenges in the network and information security field, there is a need for the Agency to analyse current and emerging risks and for that purpose the Agency may collect appropriate information, in particular through questionnaires, without imposing new

obligations on the private sector or the Member States to generate data. Emerging risks should be understood as issues already visible as possible future risks to network and information security.

(14) Ensuring confidence in networks and information systems requires that individuals, businesses and public administrations are sufficiently informed, educated and trained in the field of network and information security. Public authorities have a role in increasing awareness by informing the general public, small and medium-sized enterprises, corporate companies, public administrations, schools and universities. These measures need to be further developed. An increased information exchange between Member States will facilitate such awareness raising actions. The Agency should provide advice on best practices in awareness-raising, training and courses.

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

(16) Efficient security policies should be based on well-developed risk assessment methods, both in the public and private sector. Risk assessment methods and procedures are used at different levels with no common practice on their efficient application. The promotion and development of best practices for risk assessment and for interoperable risk management solutions within public and private sector organisations will 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 different Community research initiatives.

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

(19) Network and information security problems are global issues. There is a need for closer cooperation at global level to improve security standards, improve information, and promote a common global approach to network and information security issues, thereby contributing to the development of a culture of network and information security. Efficient cooperation with third countries and the global community has become a task also at European level. To this end, the Agency should contribute to Community efforts to cooperate with third countries and, where appropriate, with international organisations.

(20) In its activities the Agency should pay attention to small and medium-sized enterprises.

(21) In order effectively to ensure the accomplishment of the tasks 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 the Agency's work programme, adopt its own rules of procedure and the Agency's internal rules of operation, appoint and remove the Executive Director. The Management Board should ensure that the Agency carries out its tasks under conditions which enable it to serve in accordance with this Regulation.

(22) A Permanent Stakeholders' Group would be helpful, in order to maintain a regular dialogue with the private sector, consumers organisations and other relevant stakeholders. The Permanent Stakeholders' Group, established and chaired by the Executive Director, should focus on issues relevant to all stakeholders and bring them to the attention of the Executive Director. The Executive Director may, where appropriate and according to the agenda of the meetings, invite representatives of the European Parliament and from other relevant bodies to take part in the meetings of the Group.

(23) The smooth 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 a proposal for the Agency's work programme, after prior consultation of the Commission and of the Permanent Stakeholders' Group, 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 a draft statement of estimates of revenue and expenditure of the Agency and should implement the budget.

(24) The Executive Director should have the possibility to set up ad hoc Working Groups to address in particular scientific and technical matters. In establishing the ad hoc Working Groups the Executive Director should seek input from and mobilise the relevant expertise of private sector. The ad hoc Working Groups should enable the Agency to have access to the most updated information available in order to be able to respond to the security challenges posed by the developing information society. The Agency should ensure that its ad hoc Working Groups are competent and representative and that they include, as appropriate according to the specific issues, representation of the public administrations of the Member States, of the private sector including industry, of the users and of academic experts in network and information security. The Agency may, if necessary, add to the Working Groups independent experts recognised as competent in the field concerned. The experts who participate in the ad hoc Working Groups organised by the Agency should not belong to the Agency's staff. Their expenses should be met by the Agency in accordance with its internal rules and in conformity with the existing Financial Regulations.

(25) The Agency should apply the relevant Community legislation concerning public access to documents as set out in Regulation (EC) No 1049/2001(15) of the European Parliament and of the Council and the protection of individuals with regard to the processing of personal data as set out in Regulation (EC) No 45/2001(16) of the European Parliament and of the Council.

(26) Within its scope, its objectives and in the performance of its tasks, the Agency should comply in particular with the provisions applicable to the Community institutions, as well as the national legislation regarding the treatment of sensitive documents.

(27) 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 European Union are concerned. Moreover, the Court of Auditors should undertake the auditing of accounts.

(28) Where necessary and on the basis of arrangements to be concluded, the Agency may have access to the interpretation services provided by the Directorate General for Interpretation (DGI) of the Commission, or by Interpretation Services of other Community institutions.

(29) 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 SCOPE, OBJECTIVES AND TASKS

Article 1

Scope

1. For the purpose of ensuring a high and effective level of network and information security within the Community and in order to develop a culture of network and information security for the benefit of the citizens, consumers, enterprises and public sector organisations of the European Union, thus contributing to the smooth functioning of the internal market, a European

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

2. The Agency shall assist the Commission and the Member States, and in consequence cooperate with the business community, in order to help them to meet the requirements of network and information security, thereby ensuring the smooth functioning of the internal market, including those set out in present and future Community legislation, such as in the Directive 2002/21/EC.

3. The objectives and the tasks of the Agency shall be without prejudice to the competencies of the Member States regarding network and information security which fall outside the scope of the EC Treaty, such as those covered by Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the issues relate to State security matters) and the activities of the State in areas of criminal law.

Article 2

Objectives

1. The Agency shall enhance the capability of the Community, the Member States and, as a consequence, the business community to prevent, address and to respond to network and information security problems.

2. The Agency shall provide assistance and deliver advice to the Commission and the Member States on issues related to network and information security falling within its competencies as set out in this Regulation.

3. Building on national and Community efforts, the Agency shall develop a high level of expertise. The Agency shall use this expertise to stimulate broad cooperation between actors from the public and private sectors.

4. The Agency shall assist the Commission, where called upon, in the technical preparatory work for updating and developing Community legislation in the field of network and information security.

Article 3

Tasks

In order to ensure that the scope and objectives set out in Articles 1 and 2 are complied with and met, the Agency shall perform the following tasks:

(a) collect appropriate information to analyse current and emerging risks and, in particular at the European level, those which could produce an impact on the resilience and the availability of electronic communications networks and on the authenticity, integrity and confidentiality of the information accessed and transmitted through them, and provide the results of the analysis to the Member States and the Commission;

(b) provide the European Parliament, the Commission, European bodies or competent national bodies appointed by the Member States with advice, and when called upon, with assistance within its objectives;

(c) enhance cooperation between different actors operating in the field of network and information security, inter alia, by organising, on a regular basis, consultation with industry, universities, as well as other sectors concerned and by establishing networks of contacts for Community bodies, public sector bodies appointed by the Member States, private sector and consumer bodies;

(d) facilitate cooperation between the Commission and the Member States in the development of common methodologies to prevent, address and respond to network and information security issues;

(e) contribute to awareness raising and the availability of timely, objective and comprehensive information on network and information security issues for all users by, inter alia, promoting exchanges of current best practices, including on methods of alerting users, and seeking synergy between public and private sector initiatives;

(f) assist the Commission and the Member States in their dialogue with industry to address security-related problems in the hardware and software products;

(g) track the development of standards for products and services on network and information security;

(h) advise the Commission on research in the area of network and information security as well as on the effective use of risk prevention technologies;

(i) promote risk assessment activities, interoperable risk management solutions and studies on prevention management solutions within public and private sector organisations;

(j) contribute to Community efforts to cooperate with third countries and, where appropriate, with international organisations to promote a common global approach to network and information security issues, thereby contributing to the development of a culture of network and information security;

(k) express independently its own conclusions, orientations and give advice on matters within its scope and objectives.

Article 4

Definitions

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

(a) "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, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable TV networks, irrespective of the type of information conveyed;

(b) "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;

(c) "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;

(d) "availability" means that data is accessible and services are operational;

(e) "authentication" means the confirmation of an asserted identity of entities or users;

(f) "data integrity" means the confirmation that data which has been sent, received, or stored are complete and unchanged;

(g) "data confidentiality" means the protection of communications or stored data against interception and reading by unauthorised persons;

(h) "risk" means a function of the probability that a vulnerability in the system affects authentication or the availability, authenticity, 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;

(i) "risk assessment" means a scientific and technologically based process consisting of four steps, threats identification, threat characterisation, exposure assessment and risk characterisation;

(j) "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;

(k) "culture of network and information security" has the same meaning as that set out in the OECD Guidelines for the security of Information Systems and Networks of 25 July 2002 and the Council Resolution of 18 February 2003 on a European approach towards a culture of network and information security(17).

SECTION 2 ORGANISATION

Article 5

Bodies of the Agency

The Agency shall comprise:

(a) a Management Board;

(b) an Executive Director, and

(c) a Permanent Stakeholders' Group.

Article 6

Management Board

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

(a) information and communication technologies industry;

(b) consumer groups;

(c) academic experts in network and information security.

2. Board members shall be appointed on the basis of their degree of relevant experience and expertise in the field of network and information security. Representatives may be replaced by alternates, appointed at the same time.

3. The Management Board shall elect its Chairperson and a Deputy Chairperson from among its members for a two-and-a-half-year period, which shall be renewable. The Deputy Chairperson shall ex-officio replace the Chairperson in the event of the Chairperson being unable to attend to his/her duties.

4. The Management Board shall adopt its rules of procedure, on the basis of a proposal by the Commission. Unless otherwise provided, the Management Board shall take its decisions by a majority of its members with the right to vote.

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

5. Meetings of the Management Board shall be convened by its Chairperson. The Management Board shall hold an ordinary meeting twice a year. It shall also hold extraordinary meetings at the instance of the Chairperson or at the request of at least a third of its members with the right to vote. The Executive Director shall take part in the meetings of the Management Board, without voting rights, and shall provide the Secretariat.

6. 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.

7. The Management Board shall define the general orientations for the operation of the Agency. The Management Board shall ensure that the Agency works in accordance with the principles laid down in Articles 12 to 14 and 23. It shall also ensure consistency of the Agency's work with activities conducted by Member States as well as at Community level.

8. Before 30 November each year, the Management Board, having received the Commission's opinion shall adopt the Agency's work programme for the following year. The Management Board shall ensure that the work programme is consistent with the Agency's scope, objectives and tasks as well as with the Community's legislative and policy priorities in the area of network and information security.

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

10. 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 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 the Council Regulation (EC, Euratom) No 1605/2002 on the Financial Regulation applicable to the general budget of the European Communities(18), unless such departure is specifically required for the Agency's operation and the Commission has given its prior consent.

Article 7

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 Union and elsewhere of a call for expressions of interest. The Executive Director shall be appointed on the grounds of merit and documented administrative and managerial skills, as well as competence and experience relevant for network and information security. 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 that institution. The European Parliament or the Council may also ask at any time for a hearing with the Executive Director on any subject related to the Agency's activities. The Executive Director may be removed from office by the Management Board.

3. The term of office of the Executive Director shall be up to five years.

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 after prior consultation of the Commission and of the Permanent Stakeholders Group;

(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 draft 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;

(h) developing and maintaining contact with the business community and consumers organisations for ensuring a regular dialogue with relevant stakeholders;

(i) chairing the Permanent Stakeholders' Group.

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) a 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 European Economic and Social Committee and the Committee of the Regions and shall have it published.

8. Where necessary and within the Agency's scope, objectives and tasks, the Executive Director may establish, in consultation with the Permanent Stakeholders' Group, ad hoc Working Groups composed of experts. The Management Board shall be duly informed. 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.

Where established, the ad hoc Working Groups shall address in particular technical and scientific matters.

Members of the Management Board may not be members of the ad hoc Working Groups. Representatives of the Commission shall be entitled to be present in their meetings.

Article 8

Permanent Stakeholders' Group

1. The Executive Director shall establish a Permanent Stakeholders' Group composed of experts representing the relevant stakeholders, such as information and communication technologies industry, consumer groups and academic experts in network and information security.

2. The procedures regarding in particular the number, the composition, the appointment of the members by the Executive Director and the operation of the Group shall be specified in the Agency's internal rules of operation and shall be made public.

3. The Group shall be chaired by the Executive Director. The term of office of its members shall be two-and-a-half years. Members of the Group may not be members of the Management Board.

4. Representatives of the Commission shall be entitled to be present in the meetings and participate in the work of the Group.

5. The Group may advise the Executive Director in the performance of his/her duties under this Regulation, in drawing up a proposal for the Agency's work programme, as well as in ensuring communication with the relevant stakeholders on all issues related to the work programme.

SECTION 3 OPERATION

Article 9

Work programme

The Agency shall base its operations on carrying out the work programme adopted in accordance with Article 6(8). The work programme shall not prevent the Agency from taking up unforeseen activities that fall within its scope and objectives and within the given budget limitations.

Article 10

Requests to the Agency

1. Requests for advice and assistance falling within the Agency's scope, 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 Commission of the received requests. If the Agency refuses a request, justification shall be given.

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

(a) the European Parliament;

(b) the Commission;

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

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

Article 11

Declaration of interests

1. The Executive Director, as well as officials seconded by Member States on a temporary basis shall make a declaration of commitments 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 ad hoc 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 the Executive Director and by officials seconded by Member States on a temporary basis, as well as the declarations of interest made by experts in relation to items on the agendas of meetings of the ad hoc Working Groups.

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

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

2. Members of the Management Board, the Executive Director, the members of the Permanent Stakeholders Group, external experts participating in ad hoc Working Groups, and members of the staff of the Agency including officials seconded by Member States on a temporary basis, even after their duties have ceased, are subject to the requirements of confidentiality pursuant to Article 287 of the Treaty.

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.

Article 14

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 the Regulation (EC) No 1049/2001 within six months of the establishment of the Agency.

3. Decisions taken by the Agency pursuant to Article 8 of Regulation (EC) No 1049/2001 may form the subject of a complaint to the Ombudsman or of an action before the Court of Justice of the European Communities, under Articles 195 and 230 of the 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 24.

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 a draft statement of estimates of the Agency's revenue and expenditure for the following financial year, and shall forward it to the Management Board, together with a draft establishment plan.

4. Revenue and expenditure shall be in balance.

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

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

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

8. On the basis of this statement of estimates, the Commission shall enter in the preliminary draft general budget of the European Union the estimates it deems necessary for the establishment plan and the amount of the subsidy to be charged to the general budget, which it shall submit to the budgetary authority in accordance with Article 272 of the Treaty.

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

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

10. The Management Board shall adopt the Agency's budget. It shall become final following final adoption of the general budget of the European Union. Where appropriate, the Agency's budget shall be adjusted accordingly. The Management Board shall forward it without delay to the Commission and the budgetary authority.

11. The Management Board shall, as soon as possible, notify the budgetary authority of its intention to implement any project which may have significant financial implications for the funding of the budget, in particular any projects relating to property such as the rental or purchase of buildings. It shall inform the Commission thereof.

Where a branch of the budgetary authority has notified its intention to deliver an opinion, it shall forward its opinion to the Management Board within a period of six weeks from the date of notification of the project.

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)(19) shall apply without restriction.

2. The Agency shall accede to the Interinstitutional Agreement of 25 May 1999 between the European Parliament and the Council of the European Union and the Commission of the European Communities concerning internal investigations by the European Anti-fraud Office (OLAF)(20) 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 1 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 in accordance with Article 128 of Council Regulation (EC, Euratom) No 1605/2002 of 25 June 2002 on the Financial Regulation applicable to the general budget of the European Communities(21) (hereinafter referred to as 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 budgetary authority.

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

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/she shall also send this reply to the Management Board.

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

11. The European Parliament, 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 status

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.

Article 19

Staff

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

2. Without prejudice to Article 6, 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.

The Agency may also employ officials seconded by Member States on a temporary basis and for a maximum of five years.

Article 20

Privileges and immunities

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

Article 21

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 judgment pursuant to any arbitration clause contained in a contract concluded by the Agency.

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

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

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

Article 22

Languages

1. The provisions laid down in Regulation No 1 of 15 April 1958 determining the languages to be used in the European Economic Community(22) 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 Community language of their choice.

2. The translation services required for the functioning of the Agency shall be provided by the Translation Centre for the Bodies of the European Union(23).

Article 23

Protection of personal data

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

Article 24

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 initiatives undertaken by the Agency, financial contributions and staff.

SECTION 6 FINAL PROVISIONS

Article 25

Review clause

1. By 17 March 2007, the Commission, taking into account the views of all relevant stakeholders, shall carry out an evaluation on the basis of the terms of reference agreed with the Management Board. The Commission shall undertake the evaluation, notably with the aim to determine whether the duration of the Agency should be extended beyond the period specified in Article 27.

2. The evaluation shall assess the impact of the Agency on achieving its objectives and tasks, as well as its working practices and envisage, if necessary, the appropriate proposals.

3. The Management Board shall receive a report on the evaluation and issue recommendations regarding eventual appropriate changes to this Regulation to the Commission. Both the evaluation findings and recommendations shall be forwarded by the Commission to the European Parliament and the Council and shall be made public.

Article 26

Administrative control

The operations of the Agency are subject to the supervision of the Ombudsman in accordance with the provisions of Article 195 of the Treaty.

Article 27

Duration

The Agency shall be established from 14 March 2004 for a period of five years.

Article 28

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 Strasbourg, 10 March 2004.

For the European Parliament

The President

P. Cox

For the Council

The President

D. Roche

(1) OJ C 220, 16.9.2003, p. 33.

(2) Opinion of the European Parliament of 19 November 2003 (not yet published in the Official Journal) and Council Decision of 19 February 2004.

(3) OJ L 108, 24.4.2002, p. 33.

(4) Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services (Authorisation Directive) (OJ L 108, 24.4.2002, p. 21).

(5) 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) (OJ L 108, 24.4.2002, p. 51).

(6) Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive) (OJ L 108, 24.4.2002, p. 7).

(7) 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) (OJ L 201, 31.7.2002, p. 37).

(8) Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (OJ L 13, 19.1.2000, p. 12).

(9) Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) (OJ L 178, 17.7.2000, p. 1).

(10) OJ C 48, 28.2.2003, p. 2.

(11) Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector (OJ L 24, 30.1.1998, p. 1). Directive repealed and replaced by Directive 2002/58/EC.

(12) OJ L 281, 23.11.1995, p. 31. Directive as amended by Regulation (EC) No 1882/2003 (OJ L 284, 31.10.2003, p. 1).

(13) OJ L 200, 30.7.2002, p. 38.

(14) OJ L 204, 21.7.1998, p. 37. Directive as amended by Directive 98/48/EC (OJ L 217, 5.8.1998, p. 18).

(15) 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).

(16) 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).

(17) OJ C 48, 28.2.2003, p. 1.

(18) OJ L 357, 31.12.2002, p. 72.

(19) OJ L 136, 31.5.1999, p. 1.

(20) OJ L 136, 31.5.1999, p. 15.

(21) OJ L 248, 16.9.2002, p. 1.

(22) OJ 17, 6.10.1958, p. 385/58. Regulation as last amended by the 1994 Act of Accession.

(23) Council Regulation (EC) No 2965/94 of 28 November 1994 setting up a Translation Centre for bodies of the European Union (OJ L 314, 7.12.1994, p. 1). Regulation as last amended by Regulation (EC) No 1645/2003 (OJ L 245, 29.9.2003, p. 13).