Ref: MB 30/09/2005/ (5)
Heraklion 21/10/ 2005

DRAFT FINAL WORK PROGRAMME 2006

Creating the platform
for an EU culture of network and information security

Table of contents

1 INTRODUCTION

This work programme provides the tasks, establishment plan and budget for 2006 for the European Network and Information Security Agency (ENISA)[1], hereafter also referred to as the Agency. In 2006, it will be the first year that almost all staff is in place and that the operational activities will be able to start in earnest. The work in 2006 shall continue building on the work that has been carried out during 2005. It will set the platform for the Agency's efforts to create a culture of network and information security in the European Union, thus contributing to the smooth functioning of the Internal Market.

1.1 Context for ENISA

ENISA was created as a part of the eEurope 2005 action plan and has been supported by the MODINIS work programme. The results of the information security studies launched under the MODINIS programme will be fed into the work of ENISA.[2] Furthermore, the two Council Resolutions of 2002 and 2003[3] set the scene for Member State action and cooperation in this area. The aim has been to strive towards the creation of a culture of network and information security in Europe which involves all stakeholders[4]. eEurope 2005 will now be followed up by the i2010[5] where network and information security plays a key role in e.g. the task of "completing of a single European space".

Regulatory efforts have also been made to support the development of more secure electronic communication networks. Within the telecom regulatory framework legislation, there are a number of security requirements that Member States shall require telecom providers need to comply with.

Furthermore there is a great deal of research being supported in the area of network and information security. The Commission has, through the Community Framework Programmes, supported over many years security related research projects. In the eTen programme[6] trust and security services have been defined as a priority area. In

[1] According to the Financial Regulation the Agency has a right to amend its budget at any time. It should also be noted that the annexed budget prevails all other budget figures provided in the Work Programme.

[2] Four studies have been launched by the Commission under the Modinis programme, that can also serve to support the work of ENISA; 1. Study on Members States', EEE States' and Accession States' activities in the field of Network and Information Security – inventory and best practices guide, 2. availability and robustness of electronic communications, 3. risk assessment and risk preparedness models, 4. Handbook of legislative procedures on computer and network misuse in EU countries.

[3] See Council Resolution of 28 January 2002 on a common approach and specific actions in the area of network and information security, OJ C 43, 16.2..2002 and Council Resolution of 18 February 2003 on a European approach towards a culture of network and information security, OJ C 48, 28.2.2003.

[4] The notion of Culture of Security was introduced in the OECD Guidelines for the Security of Information Systems and Networks, Towards a culture of security, adopted on 25 July 2002.

[5] Communication from the Commission to the Council, the European Parliament, the European Social and Economic Committee and the Committee of the Regions, i2010 – A European Information Society for growth and employment, COM(2005) 229 final.

[6] The European Community Programme designed to help the deployment of telecommunication networks based services (e-services) with a trans-European dimension.

the 5th Framework Programme security and trust was defined as a priority area. The interest in this area has been further reinforced in the Information Society Technology (IST) priority of the 6th Framework Programme under which approximately Euro150 m has been allocated for research on security, dependability, privacy and digital asset management. More opportunities in the research field were made available in later calls, and it can be expected that Community support for research on network and information security will continue to be a priority in the forthcoming 7th Framework Programme.

1.2 Scope and objectives

ENISA shall develop a culture of security, promoting a high and effective level of network and information security. To do this ENISA shall enhance the capabilities of the European Communities, Member States and the business community to prevent, address and respond to issues related to network and information security. The culture of security shall be for the benefit of all stakeholders and contribute to the smooth functioning of the Internal Market. It shall also contribute to this purpose by assisting the Commission and Member States and shall cooperate with the business community to help it meet the requirements of network and information security, including those set out in present and future Community legislation.

ENISA shall be able to provide assistance and give advice to the Commission (e.g., in technical preparatory work for updating and developing Community legislation in the field of network and information security), the European Parliament and Member States in accordance with its Internal Rules of Operation. It shall continue to develop a high level of expertise building on national and Community efforts and use this expertise to stimulate a broad cooperation between actors from both the public and private sectors.

These objectives and tasks shall, however, not prejudice the competencies of the Member States which fall outside the scope of the EC Treaty.

1.3 Tasks

In order to ensure the fulfilment of its objectives, ENISA's tasks shall mainly be focused on:

- Advising and assisting the Commission and the Member States on network and information security and in their dialogue with industry to address security-related problems in hardware and software products;
- Collecting and analysing information on security incidents and emerging risks;
- Promoting risk assessment and risk management methods to enhance our capability to deal with network and information security threats;
- Awareness raising and cooperation between various actors in the network and information security field, notably by developing public-private partnerships.

The Agency shall conduct its operations based on a work programme adopted in accordance with the ENISA Regulation. The work programme does not prevent the Agency from taking up unforeseen activities that fall under its scope and objectives and within the given budget limitations.

ENISA's work in 2006 shall aim at becoming a European centre of expertise by building on the networks of contacts and information channels that have been set up during 2005. It shall in particular make use of expertise and experiences that already exist in the Member States.

2 ADMINISTRATIVE TASKS

2.1 Staffing

In the course of 2006 ENISA will finalise the recruitment procedure of temporary staff. Staff will increase by 6 new temporary agents and will reach a total number of 44 temporary agents. Additional support of Seconded National Experts and contracts agents will be considered when needed.

The Agency will keep investing in the implementation of the reform of the EU staff policy. Additional investment will be necessary for the management of training, career development and reports related to individual objectives.

Deliverables	Performance indicators	Deadline	Costs
Finalised recruitment of temporary staff	1. Number of applicants 2. Number of posts filled	1. Q1 2. Q2	not applicable
Implementation of career development and training	1. Total number of attended training courses. 2. Number of staff that have completed planned training.	1. Q3 2. Q4	not applicable

2.2 Finance

ENISA is committed to put in place the principles and rules governing the financial procedures. The establishment and implementation of the budget and the preparation of the Agency's accounts are performed through the appropriate timetable and liaison with the Budgetary Authority (European Parliament and Council), Commission and Court of Auditors. The management of resources of the Agency shall be conducted in accordance with the principle of sound financial management (economy, efficiency and effectiveness). The monitoring of a financial reporting cycle as well as a structure of internal control systems and procedures shall be put in place.

Deliverables	Performance indicators	Deadline	Costs
Budget execution and preparation of the accounts.	1. Timely execution of budget and preparation of the accounts; deadlines as stated in the Financial Regulation. 2. Liaison with budgetary authority and Court of Auditors	Ongoing as per the Financial Regulation or otherwise requested	Not applicable
Financial reports; budget and accounting	Meeting the requirements and deadlines set out in the Financial Regulation.	Ongoing according to FR or otherwise	

		requested or deemed necessary	

2.3 Equipment and premises including information and communication systems

The prime objective concerning the infrastructure and IT equipment is to have a fully operational environment for the administrative and operational staff of ENISA. Although the move and set up of ENISA in Heraklion took place in 2005, it can be expected that the relocation to Heraklion will require a continuous investment also in 2006 in order to reach the optimum operational point.

During 2006, the Agency will continue to invest in its corporate information and communication systems, which will be based on secure, reliable and high performance technology. Additional investment might be necessary for office management and building arrangements, but these shall also depend on the contribution of the hosting Member State.

Furthermore, in the course of 2006, ENISA will continue to develop and refine its security policies (put in place in 2005) as applied to its own networks and information systems

Deliverables	Performance indicators	Deadline	Cost
Fully functional Agency information system	Availability of Agency's information systems.	Ongoing	Not applicable
Implementation of office and building arrangements	Availability of office space and equipment	Q2	
Implementation of security policies.	Level of awareness among ENISA staff of the security policies.	Q1	

3 OPERATIONAL TASKS: GENERAL

The Agency will have to update and further develop the knowledge of its staff in order to become a centre of expertise and to handle its tasks. All staff needs to develop their own knowledge, through participation in conferences, training courses and by access to relevant literature, magazines, databases and other information sources.

Based on the Communication Strategy developed in 2005, a "Communication Implementation Plan" for 2006 shall lay down the actual execution of ENISA's strategy. This implementation plan shall go into detail on the specific messages that are communicated through which channels and to which target audiences. Channels include, but are not limited to, conferences, ENISA website, ENISA newsletter, ENISA yearly report and joint events.

In particular will the improvement of the ENISA web site will be essential for the widespread use in the Internal Market of ENISA's efforts.

Legal base; ENISA-Regulation Articles 2.3 and 3 e)

In 2006 the Agency will be ready to support the organisation of an independent, not-for-profit and high level European conference in partnership with a third party e.g. an existing conference organiser or the current EU presidency. The Agency should also take the opportunity to organise smaller events, like work shops on specific themes to involve Member States, the European Commission and the industry. The themes for the work shops should be carefully chosen and could include the outcome of the work of the ad hoc working groups or to have a first exchange of ideas and raise interest among the stakeholders before the launch of new working groups. Examples of topics could be risk analysis and risk management tools and methodologies, awareness raising, security in wireless networks, certification, policy, regulatory aspects, accreditation etc.

Legal base; ENISA-Regulation 3 e) and f)

ENISA will have to identify the developments in the area of network and information security and to reach out with its findings to a broad audience. To help achieve this, a newsletter in electronic form shall be issued covering ENISA's own work as well as important technical and policy developments.

Legal base; ENISA-Regulation Article 3 a), e) and k)

ENISA shall also be able to respond to requests for advice and assistance from the European Parliament, the Commisssion or competent bodies in the Member States. Depending on the efforts this task will require, the performance indicators will have to be adjusted accordingly.

Legal base; ENISA-Regulation Articles 2 a), 3 b), 3 d) and 10

Deliverables	**Performance indicators**
Plan for building up "library".	Appropriate coverage of literature and subscriptions.
Communication Implementation plan 2006	Availability and quality of the plan 2006
Updated web site	1. Web site statistics 2. Availability of web site
Draft communication implementation plan 2007	Timely presentation of the draft
Conference	1. Number of participants in Conference 2. Number of submitted papers
4-5 Workshops	Number of work shops
4 Issues of the newsletter	1. Number of articles submitted to the newsletter 2. Number of authors that have contributed to the newsletter

Response to requests	1. Number of requests handled. 2. Duration between the request and the response.

4 OPERATIONAL TASKS: TECHNICAL

4.1 Risk management

ENISA will generate a survey of best practices in the area of risk management[7] where the focus will be on ICT-related risks. This will help in understanding how risks are evaluated and managed in various sectors (e.g. telecommunication, financial sector, etc) and company types (e.g. multinational organisations, large companies, SMEs). In addition to that an objective will be to establish a common language in the area of risk analysis and risk management. This will facilitate the communication between stakeholders in exchanging information about the methodologies and best practices used (e.g. towards negotiations about security characteristics of products, services and processes). The focus shall be on stakeholder groups from Member States and sectors that due to their financial and organisational characteristics have had less means to develop their own methods or carry out risk analysis and risk assessment.

Many risk assessment and risk management methods are national and others cover specific sectors or areas. ENISA shall focus on making a comparison of these methods in order to establish best practices and provide an overview over what the methods cover, where the differences are and which methods that are best for certain sectors or types of companies. ENISA should build on the report delivered by the ad hoc working groups experts on risk analysis and management established in 2005. As it has been proven difficult for in particular SMEs to find suitable methods to perform risk assessment and risk analysis, ENISA shall during 2006 pay specific attention to methods that can be used by this group of enterprises. Specific information packages for SMEs shall be provided. Such information packages could e.g. include information on the methods that are most relevant for the particular stakeholder group and examples of best practices.

Deliverables	**Performance indicators**	**Deadline**	**Budget**
A matrix presenting the different RM-RA methods versus their attributes will be drawn. After a selection of RM-RA methods in consideration of their attributes, a more detailed analysis of this part of the matrix will be made. A functional test will be carried out.	Completeness of the listed methodologies, Availability for the public of this information, table, analysis and results of the functional test.	Q2	102000

7

Information package for SMEs.	Completeness and usefulness of the information package as assessed by an enquiry through a questionnaire filled in by representatives of SMEs.	Q4	

Legal base: ENISA-Regulation 3 a), d), h) and i)

4.2 Technical and procedural security policies

Network and information security policies are not only about technical, but also about organisational and legal issues such as information systems ownership and sharing of responsibilities between actors. ENISA shall help the identification of best practices for technical and procedural security policies for SMEs and other sectors. Such practices should aim at facilitating commercial transactions and business continuity.

ENISA shall make an inventory of what kind of measures and principles providers of electronic communications services have adopted or shall adopt in order to comply with the requirements for technical and organisational measures to safeguard the security of their services according to the national legislation implementing EU legislation in the field. Such measures should include those to fight unsolicited electronic mail (spam), "spyware" and other forms of "malware" that affect the provision of electronic communication networks and services according to the Directive 2002/58/EC on processing of personal data and the protection of privacy in the electronic communications sector. The objective is to identify best practices for such measures and actions. Based on that, ENISA shall provide advice to the Commission and Member States

The availability of accreditation and certification schemes can also contribute to the trustworthiness of electronic products and services by raising the level of security. Information about such schemes should be widely disseminated among stakeholders. In order to be able to promote the use of existing schemes, ENISA shall start making an assessment of the need to facilitate the functioning and accessibility of accreditation and certification schemes and how this could be done in cooperation with the relevant standardisation bodies. The certification work shall include consideration of management system certification as well as product certification.

Authentication methods are vital for the trustworthiness of electronic transactions and lot of work has been undertaken by various organisations in this area. ENISA should contribute by . The objective shall be to facilitate the interoperability and mutual recognition of electronic authentication methods, including electronic signatures.

Deliverables	**Performance indicators**	**Deadline**	**Budget**
Knowledgebase of Best Practices: data, figures, advice, knowledge accessible via an IT tool through Internet. The SME-	Quality and usefulness of the best practices among SMEs as indicated by the users of the knowledgebase.	Q4	102000

user will inject its needs into this IT tool as well as the features of its situation; the tool would send back the best practices which would have been collected. The Deloitte study will be considered in this respect as a potential input.			
Study listing measures adopted and made available by providers of electronic communication services to comply with legal requirements regarding technical and organisational measures to safeguard the security of their services.	Timeliness and completeness of the study.	Q2	
Begin an assessment of the need to facilitate the functioning and accessibility of accreditation and certification schemes	Timeliness and approach of the assessment.	Q4	
Make plan for how to create a common language between Member States to identify the levels of security that can be met by various authentication methods.	Timeliness and completeness of the plan.	Q4	

Legal base: ENISA-Regulation 3a), c), g)

4.3 Network and information security technologies

ENISA shall promote a culture of security also among users, producers, and designers of network and information security technologies.[8] ENISA should identify relevant fora where it can contribute to this task.

With a view to the smooth functioning of the Internal Market ENISA shall track the development of standards and work with vendors to facilitate the incorporation of security research and standards into mass-market products and services. This work will take place within a wider activity of identifying technical issues, trends, and developments in network and information security. For this purpose, ENISA shall make an overview of the major technical developments in the field of network and information security.

ENISA shall also follow the technical developments in Member States and industry through participation in relevant Member State and EU events and workshops on issues involving network and information security technologies..

[8] In 2006 the results from the MODINIS study on availability and robustness of electronic communication infrastructures will be available as a basic input for this task.

ENISA shall ensure that it has up to date technical knowledge on NIS developments, through the maintenance of strong contacts with the relevant EU, International, and industry organisations and bodies.

The Agency shall contribute to the promotion of research and other forms of cooperation and investigation in the area of network and information security. ENISA shall also continue contributing to the promotion of the implementation of a Culture of Security in ICT-related research, in particular such research that is supported by the Commission and Member States.

Deliverables	Performance indicators	Deadline	Budget
Analysis of the major technical developments in the field of network and information security technologies in relation with standardisation with a view to produce Report on information gathered from technical fora, consisting partially in updating already existing reports and publications (e.g. CEN - ETSI)	Timeliness of the overview of technical developments in relation with standardisation. Dissemination of results through web site and other means (conferences, workshops, etc.)	Q3	102000
Presence of ENISA in various fora. Establishment of a network of contacts in the technical, development, standardisation and research community in order ENISA to contribute to the promotion of research activities in the area of NIS	Number of contacts in the technical, development, standardisation, and research community and active input/advice to this community.	Q4	

Legal base; ENISA-Regulation 3 a), f), g) and, h)

5 OPERATIONAL TASKS: COOPERATION AND SUPPORT

5.1 Computer incident and response handling

ENISA shall facilitate the promotion of the setting up of CERTs or similar facilities particularly in those Member States that lack such facilities and wish to close this gap.

For these tasks it is essential to discuss with existing CERT organisations and to take into account work that is already done (such as the IST project TRANSIT). In 2006 ENISA shall connect with CERT organisations, such as the TF-CSIRT group, the European Government CERT Group or other relevant entities, such as the abuse teams organised in the E-Coat group or WARPs.

In order to promote and facilitate the setting up of CERTs and similar facilities in the Member States, ENISA shall provide a road map for the setting up of such organisations in terms of training, equipment, management and make contact with the CERT communities and other tasks in order to facilitate establishing new teams. This Roadmap shall be complemented by a checklist, which can be adopted by the stakeholders for easer implementation of the roadmap in practice. It shall furthermore provide a road map for how to further improve CERT cooperation in all relevant areas.

Deliverables	Performance indicators	Deadline	Budget
Written report on step-by-step approach on how to set up a CERT or similar facilities, including examples.	Comprehensiveness of the report and feasibility of the described approach.	Q3	102000
Excerpt of roadmap in itemised form allowing an easy application of the roadmap in practice.	Quality and usability of this itemised checklist.	Q3	
Written plan on how cooperation between CERTs or similar facilities can be facilitated by relevant stakeholders.	Comprehensiveness of the plan and feasibility of the suggested approach.	Q4	

Legal base: ENISA-Regulation Article 3 c), d) and e)

5.2 Awareness raising

During 2006, ENISA will continue identifying current best practices from the Member States. The Agency will mainly focus on the public sector. Additional experience (i.e. from the private sector) will be gradually incorporated into the initial package and further analysis will be performed. The information collected will be based on output coming from workshops held with key stakeholders. ENISA will ensure that the collection of Member States best practices will be available e.g., through its web site.. For this purpose, ENISA shall develop a European best practice guide on how to raise awareness with various target groups.

ENISA shall also continue the work from 2005 by preparing customised information packages**.** For this purpose, ENISA shall ensure that the list of target groups which have been identified is completed and covers all categories which need customised information packages. A priority plan for the coming years' work will be finalised. Examples are primary and secondary school pupils, SMEs, home users of various age groups, wireless network users, etc. ENISA shall also provide assistance on how to disseminate customised information packages to Member States. The follow up of awareness raising is to empower the users of each target group to handle their threat situation. Therefore best practises in risk assessment and risk management shall be included in the information packages.

Deliverables	Performance indicators	Deadline	Budget
Written report on Member States best practices in awareness raising for particular target groups, including examples.	Number and usability of best practices.	Q3	177000
Written report on how awareness raising with various target groups can be facilitated within Europe.	Completion of report.	Q2	
CD-ROM with information on best practices customised to various target groups, including examples.	Quality and usability of customised information package on CD ROM.	Q3	
Written plan on how the customised information packages could be disseminated within Europe.	Comprehensiveness of the plan and feasibility of the suggested roadmap.	Q3	

Legal base; ENISA-Regulation Article 3 b), e) and k)

5.3 Relations with EU bodies and Member States

As ENISA is heavily dependent on the cooperation with EU and Member State bodies, a primary task is to build a basis for their support as well as the acceptance for the Agency's work. This is a continuous and horizontal task which shall foster fruitful cooperation and information exchange. The objective in keeping up relations with EU bodies and Member States is to establish and keep good and stable relations to be able to disseminate information from ENISA and to gather relevant information from Member States and EU institutions on ongoing activities and developments in the area of network and information security.

In order to follow closely what is happening in Member States and the EU in general and ensure that the work of ENISA is known to EU and Member States' bodies ENISA should further update and maintain the "who is who" directory of contacts that was started during 2005. Furthermore the cooperation mechanisms proposed in 2005, including the network of national liaisons in each Member State, liaisons to the relevant committees in the European Parliament and to the European Commission shall be implemented and further elaborated.

The ENISA web site country pages provide an overview of the state of play in the Member States regarding activities in the area of network and information security, such as listing the different national entities dealing with network security issues or awareness raising strategies. Although the input is supplied by the Liaison Officers, ENISA has to make sure that the given information is complete, relevant and up to date.

ENISA will furthermore manage the Network of National Liaison Officers to enable it to carry out its work.

Deliverables	Performance indicators	Deadline	Budget
Document listing relevant Member State organisations in Europe, including name of authority, area of responsibility and contact information in the context of the "who is who directory".	Number of Member State entries in the "who is who directory"	Ongoing	117000
Document listing relevant EU institutions and bodies in Europe, including name of authority, area of responsibility and contact information.	Number of EU institutions and bodies in the "who is who" directory.	Ongoing	
Country pages on ENISA website, including national authorities, other bodies and organisations, activities and events, developments and best practices/case studies (update)	Number of updated country pages	Ongoing	
Well established and functioning network of national liaison officers ensuring rapid information exchange between Member States and ENISA	Effectiveness of meetings and surveyed overall satisfaction level of the liaison officers	Ongoing	

Legal base: ENISA-Regulation Article 3 b) and d)

5.4 Relations with industry and international institutions

ENISA's tasks are to a large extent dependent on cooperation between all stakeholders, and involvement of the stakeholder groups is a task that needs further development during 2006. ENISA will provide the secretariat of the PSG meetings and give appropriate administrative support to enable the Group to carry out its work. It is vital for ENISA to establish the appropriate relations with key players in order to find out about the state of the art of network and information security in order to limit the gap to state of practice.

In 2005, ENISA published a call for interest on ad hoc Working Groups, resulting in a list of available experts. In 2006, ENISA shall keep the list of potential members for the ad hoc Working Groups updated.

ENISA shall examine closely and provide an overview of the activities in the most relevant international fora in the area of network and information security. The main objective will be to collect existing materials on the promotion of network and information security and see how they can be applied in the EU.

Deliverables	Performance indicator	Deadline	Costs
Well established and functioning PSG ensuring adequate advice on Work Programme and establishment of Working Groups to the Executive Director of ENISA.	Number of meetings and surveyed overall satisfaction level of the PSG members.	Ongoing	42000
Well established and functioning Working Groups ensuring independent advice on scientific matters to the Executive Director of ENISA.	Number of experts in the working group list, number of working group meetings, surveyed level of satisfaction of the WG members.	Ongoing	
Brief written plan, including list of relevant players and ways of establishing contacts at which level (e.g., liaison, observer, member, etc.) with international fora and industry key players active in the area of network and information security.	Relevance of established network of contacts.	Q1	

Legal base; ENISA-Regulation Article 3 c), e), f) and j) and PSG Decision Article 5

Annex 1 Draft Budget 2006

Enisa 2006 Draft Budget

REVENUE					
Title Chapter	Heading	Financial year 2005	Financial year 2006	% Share (Total)	Remarks
9	REVENUE	6,800,000	6,800,000		
90	Subsidy from the EU general budget	6,800,000	6,800,000		

EXPENDITURE					
Title Chapter	Heading	Appropriations 2005	Appropriations 2006	% Share (Total)	Remarks
TITLE 1	PERSONNEL	3,300,000	3,600,000	53%	**Staff costs: salaries, social welfare, allowances, recruitment costs, removal expenses, Interim Agents, consultants and other management costs**
11	Salaries	2,258,306	3,250,000	48%	Salaries of Temporary Agents and Contract Agents, including allowances such as household, schooling and expatriation allowances. Seconded National Experts allowances. Employer's social security contribution (insurance agints sickness, occupational diseas
12	Recruitment expenditure	564,804	220,000	3%	Reimbursement costs of interviewing candidates and selection procedure: travel expenses, daily allowance and accomodation. Cost for taking up on duties and/or end of contract (installation and transfer allowances, removal expenses and temporary daily subs
13	Socio-medical infrastructure and Training	63,000	100,000	1%	Medical service. Training and language courses.
14	Other staff related expenditures	413,890	30,000	0%	Management costs for the Commission (i.e.PMO), special grants, Interim Agents and Consultants.
TITLE 2	FUNCTIONING OF THE AGENCY	2,500,000	1,350,000	20%	**Administration and infrastructure costs**
20	Buildings and associated costs	604,430	320,000	5%	Building rental and associated costs, such as insurance, water, electricity-heating, cleaning and maintenance, fittings, security equipment and services
21	Movable property and associated costs	540,000	130,000	2%	Purchase/hiring of furniture. Technical installations and purchase/renting of office machines (fax, photocopiers, electronic equipment). Transport equipment. Documentation and library costs. Other maintenance and repairs.
22	Current administrative expenditure	189,436	160,000	2%	Stationary, postal and telecomunications as well as other legal and financial expenses. Departmental removals and associated handling costs. Other insurances.
23	Informatics	600,000	200,000	3%	Software, hardware, consultancy and maintenance. Web-site development.
24	Meetings, Missions and Representation costs	508,134	480,000	7%	Enisa administration meetings, missions and representation costs, such as Management Board's, Executive Director's meetings & missions and administration staff's meetings & missions.
25	Translation & interpretation services	58,000	60,000	1%	Translation and interpretation costs from Community services and other external services
TITLE 3	OPERATIONAL EXPENSES	1,000,000	1,850,000	27%	**Operational activity costs**
30	Meetings and Missions related to operational activities	516,561	571,000	8%	Expenditure to cover the organisation of meetings, missions and representation expenses related to the operational activities of the Agency
31	Conferences, workshops and communications		535,000	8%	Expenditure related to the organisation of conferences & joint events as well as workshops
32	Operational activities	483,439	744,000	11%	Core task of the agency involving Network and Information Security inventories, studies, dissemination, as well as purchase of related material

Annex 2

ENISA ESTABLISHMENT PLAN

Categories and grades	Posts					
	2004		2005		2006	
	Authorised		Authorised		Authorised	
	Perm.	Temp.	Perm.	Temp.	Perm.	Temp.
A*16	-	-	-	-	-	-
A*15	-	1	-	1	-	-
A*14	-	-	-	-	-	-
A*13	-	-	-	-	-	-
A*12	-	-	-	3	-	-
A*11	-	-	-	-	-	-
A*10	-	-	-	4	-	-
A*9	-	8	-	6	-	1
A*8	-	-	-	2	-	3
A*7	-	5	-	9	-	-
A*6	-	-	-	-	-	-
A*5	-	-	-	-	-	-
Total grade A	***0***	***14***	***0***	***25***	***0***	***4***
B*11	-	-	-	-	-	-
B*10	-	-	-	-	-	-
B*9	-	-	-	-	-	-
B*8	-	-	-	-	-	-
B*7	-	-	-	-	-	-
B*6	-	-	-	-	-	-
B*5	-	-	-	6	-	1
B*4	-	-	-	-	-	-
B*3	-	-	-	-	-	-
Total grade B	***0***	***0***	***0***	***6***	-	***1***
C*7	-	-	-	-	-	-
C*6	-	-	-	-	-	-
C*5	-	-	-	-	-	-
C*4	-	-	-	0	-	1
C*3	-	-	-	-	-	-
C*2	-	1	-	5	-	-
C*1	-	-	-	2	-	-
Total grade C	***0***	***1***	***0***	***7***	***0***	***1***
D1	-	-	-	-	-	-
D2	-	-	-	-	-	-
D3	-	-	-	-	-	-
D4	-	-	-	-	-	-
Total grade D	***0***	***0***	***0***	***0***	***0***	***0***
Total staff	**0**	**15**	**0**	**38**	**0**	**44**

Organisational Chart of the European Network and Information Security Agency