



General Report 2006



**The Annual Report of the
European Network and
Information Security Agency**



Executive Director Andrea Pirotti with members of the ENISA staff



ENISA – defending the future

Twenty first century life is dominated by technology. We take for granted the modern miracles of computers, the Internet, mobile phones, electronic banking, e-Health and e-Commerce. The Internet and what it has to offer form part of the everyday life of individual citizens. Increasingly we are living in an e-Society.

Communication networks and information systems are also – perhaps more importantly – crucial factors in the development of the European economy. They are essential to the smooth functioning of the Internal Market, both today, and increasingly so for the future of tomorrow.

As these networks and systems are growing ever more complex, they can also be devastated by accidents, mistakes and malicious attacks. Security breaches have already generated substantial economic damage and threatened the infrastructures of industrial and financial systems, power plants and energy networks. They have undermined user confidence, jeopardising the future development of the Information Society in Europe. The future of our Digital Economy needs to be defended – against the threats directed at today's modern society.

Centre of Excellence

Against this background, ENISA was established by the European Union (EU) as a Centre of Excellence in Network and Information Security (NIS). Its task is to assist the EU, its Member States and the business community to prevent, address and respond to network and information security problems.

The Agency's work includes:

- **Advising and assisting** the European Commission and the Member States on information security and in their dialogue with industry to address security-related problems in hardware and software products.
- **Collecting and analysing** data on security incidents and emerging risks in Europe.
- **Promoting** risk assessment and risk management methods to enhance our capability to deal with information security threats.
- **Awareness-raising and co-operation** between different players in the information security field, notably by developing public/private partnerships with industry.

Table of Contents

5	CHAPTER 1 – OVERVIEW
6	Executive Summary
7	A Message from the Executive Director
9	CHAPTER 2 – ENISA AS A FOCAL POINT FOR NIS Fostering information exchange and stimulating collaboration
10	ENISA Relations with EU Bodies and Member States
11	Network of National Liaison Officers (NLOs)
12	'Who is Who' Directory and Database
12	Creating a Network of Contacts
13	CHAPTER 3 – ENISA AS A CENTRE OF EXCELLENCE Offering advice and assistance
14	Acquiring an overview of NIS themes and developments
16	Responding to Requests
17	Security Policies
17	Collection of best practice – the 'Knowledgebase'
18	Trends in security and anti-spam measures
20	Assessment of information security certifications
22	Interoperability authentication description languages
23	Regulatory Aspects of Network and Information Security (WG-RANIS)
24	Computer Emergency Response Teams (CERTs) in Europe
27	Awareness Raising in the Member States
31	Risk Assessment & Risk Management across the EU
33	CHAPTER 4 – A FINGER ON THE PULSE Keeping in touch with industry, consumers and other relevant stakeholders
34	Permanent Stakeholders' Group (PSG)
35	Other relations with industry, international organisations and third countries
36	Communication and outreach activities
39	CHAPTER 5 – KEEPING THE WHEELS TURNING
40	Consolidating the Agency
41	Management Board
42	Organisation chart
43	Physical infrastructure
43	Technical infrastructure
44	Administration
44	General Administration
44	General Services
44	Legal Services
45	Human Resources
46	Finance & Accounting
49	ANNEXES
50	Annex 1 Glossary
51	Annex 2 ENISA 2006 Work Programme Excerpts
54	Annex 3 Members of the Management Board
57	Annex 4 Members of the Permanent Stakeholders' Group (PSG)
58	Annex 5 Members of the Ad hoc Working Groups
59	Annex 6 National Liaison Officers (NLOs)
60	Annex 7 Human Resources



Chapter 1

- **Executive summary**
- **A Message from the Executive Director**

Executive summary

In the modern Information Society, the use of information systems and secure networks has become ubiquitous. Business, citizens and the economy are entirely dependent on them for the proper functioning of the Internal Market. Today, information systems affect virtually all sectors of our society and are part of the everyday life of private citizens. ENISA's mission, therefore, is one with considerable economic impact.

ENISA is to assist the European Union (EU) and its Member States in making networks and information systems more secure. To accomplish this, the Agency acts as a forum for the exchange of information for all stakeholders, and for increasing co-operation in Network and Information Security (NIS).

Work in 2006 built on the achievements of the Agency's first year of operation in supporting the Internal Market. ENISA bridges the gap between governments and the major private owners of electronic networks of information systems. In this public-private partnership, the Agency encourages a dialogue about responsibilities, roles, problems and consequent solutions.

During 2006, ENISA consolidated its position as a Centre of Excellence, by increasing and enhancing its contacts with its 'parental DG', DG INFSO, and many other relevant players.

In addition, ENISA's role includes giving advice to the European Commission and Member States on NIS matters. In 2006 the Agency received and responded to a number of requests for assistance or advice from the Commission, Member States and EU bodies – an increasing occurrence as ENISA is gaining recognition. In all its work, the Agency has benefited substantially from the excellent working relationship between the Executive Director and his stakeholders, in particular with the Permanent Stakeholders' Group.

ENISA's Experts have taken its message around Europe by participating in seminars, conferences and workshops. The Agency has also enhanced its outreach and communication channels in various ways, e.g. including the launching of a new web site, by co-organising and participating in almost 40 conferences and events all over Europe, in the USA and Asia, and through its 'ENISA Quarterly' magazine which provides a forum for discussion on European Network and Information Security.

In 2006 the Agency also produced all the deliverables planned in its work programme. It has updated the map of CERTs (Computer Emergency Response Teams) in Europe (v1.3), an inventory of 112 European CERTs, and produced a step-by-step manual on how to set up a CERT. Furthermore, ENISA has updated and extended its 'Who is Who' Directory of Network and Information Security players in Europe, a revised and updated Awareness Raising Information Package has been introduced, and a User's Guide to Awareness Raising was produced.

The Agency's mission is to create a culture of network and information security in the European Union. As such it is contributing to the smooth functioning of the Internal Market. By encouraging co-operation, the Agency has already made a significant contribution to reducing obstacles to secure NIS, working to the benefit of all users of information systems.

As indicated in the Commission Strategy on NIS of May 2006, ENISA was given an enhanced mandate. Following positive discussions with the Management Board and the Permanent Stakeholders' Group, this role has been incorporated into the draft ENISA Strategy for 2008-2011. The Agency is confident in the direction in which it is proceeding for the forthcoming years.



A Message from the Executive Director



2006 has been the first full operational year for ENISA. As such it has been fundamental in consolidating the Agency's status as a Centre of Excellence in the field of Network and Information Security (NIS). As the Executive Director, I have had the pleasure of witnessing the gradual evolution of ENISA. Staff have been recruited to fulfil the tasks and deliverables outlined in the Work Programme set by our Management Board, in response to the mission given us by the European Parliament and the Council of the European Union.

Achievements of 2006

This General Report focuses primarily on the operational tasks and deliverables that ENISA accomplished in 2006. I am delighted to be able to report that the Agency completed all its deliverables and activities within the deadlines set out in its Work Programme for 2006 (a full list of these deliverables is included as Annex 2).

To mention just a few:

- ENISA produced an inventory of Computer Emergency Response Teams (CERTs) in Europe, and updated its map of CERTs in Europe
- The 'User's Guide to Awareness Raising', was updated and an Information Package produced
- We finalised an inventory of methods, tools and best practice in Risk Management/Risk Assessment and posted it on our web site
- We delivered two studies on anti-spam measures
- We were able to provide advice and assistance in answer to a number of requests from the Member States and the European Commission.

Among other highlights of the year, we were honoured with a visit to our premises by Madame Viviane Reding, the Commissioner for Information Society and Media, who praised ENISA's contribution to the 'smooth functioning of Europe's Internal Market'.

In May we welcomed the decisive European Commission Communication on NIS. The Commission's new Communication Strategy outlines an enhanced role for ENISA in the field of data collection to handle security incidents and measured levels of consumer confidence from all over Europe by developing a trusted partnership with Member States and stakeholders. We are also tasked to examine the feasibility of a multilingual information sharing and alert system.

ENISA emerging as a Key Player in NIS in Europe

With achievements such as these, and despite limited staff resources, ENISA is quickly becoming recognised as a key player in the field of NIS. Our work described in the following pages demonstrates our determined efforts to bring all those involved in European Network and Information Security closer to each other, and to positioning ENISA as a 'hub' for the exchange of NIS information and a think tank in NIS.

Our indispensable friends and contributors

However, ENISA could not function in a vacuum. Without the active support of the EU institutions and Member States, the Agency could not accomplish its tasks. Therefore, I am pleased to take this opportunity to thank the many individuals who have contributed towards the development of NIS in Europe for their crucial support to our mission: the EU institutions, in particular Madame Reding, European Commission DGs, DG INFSO and DIGIT, and the European Parliament's Committee for Industry, Research and Energy (ITRE).



Commissioner Viviane Reding visited ENISA in April 2006.



The Executive Director (middle) with the Heads of Department, from the left: Dr. Ronald De Bruin and Dr. Alain Esterle

I also thank the members of our Management Board, the Permanent Stakeholders' Group (in particular for their valuable 'Visions for ENISA' document), members of the Working Groups and the National Liaison Officers for their invaluable contributions, feedback and input. ENISA is dependent on a close dialogue with all these key players if it is to develop and function as 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.

Future perspectives


Looking at the year ahead, 2007 will be one of increased activities. At the same time, 2007 will further contribute to the clarification of ENISA's future role and in particular, its future mandate. The Commission Evaluation report is expected to be delivered in the first half of 2007. This will determine what may be needed to adapt and possibly modify the regulation, and indicate the direction for future developments as well as the mandate of the Agency, to equip it for new challenges. The Agency initiated a strategic discussion in 2006 with the Management Board and Stakeholders on the ENISA Strategy for 2008-2011. The Commission Evaluation and the European Parliament's assessment thereof will be decisive in determining what can be implemented and will clarify ENISA's future position.

Meanwhile, as laid down in our Work Programme, our activities in 2007 will broadly be dominated by five operational themes. These themes, developed to assist in enhancing the NIS situation in Europe, are: raising awareness and building confidence, facilitating the working of the Internal Market for e-Communication, mastering emerging technologies and services, bridging security gaps in Europe, and increasing our communication and outreach activities.

Working to the benefit of the citizens of Europe

Finally, since interconnected information networks touch upon all key areas of economy and society, in our daily quest, we bear in mind that the beneficiaries of our efforts are the citizens of Europe. That is indeed a high calling and it is both an honour and a responsibility to share knowledge in each Member State. Our work will, in all modesty, help give citizens the 'Europe of Results' that the Commission President Manuel Barroso has announced is a key priority for the European Union.

Andrea Pirotti
Executive Director



Chapter 2

ENISA AS A FOCAL POINT FOR NIS

Fostering information exchange and stimulating collaboration

- **Relations with EU Bodies and Member States**
- **Network of National Liaison Officers (NLOs)**
- **'Who is Who' Directory and Database**
- **Creating a Network of Contacts**

ENISA Relations with EU bodies and Member States

As a centre of expertise in NIS, ENISA is tasked with advising and assisting the European Union bodies and Member States in the field of Network and Information Security. This is achieved through fostering information exchange and co-operation between all stakeholders all over Europe. Therefore, it is essential for ENISA to maintain and develop established relationships with and between the EU bodies and Member States.

In 2006, ENISA maintained its relationship with EU bodies and Member States which enabled information about ongoing activities and developments in the area of Network and Information Security (NIS) to be disseminated effectively from ENISA and to be gathered from Member States and EU institutions.

Liaison with the relevant Committees in the European Parliament and in the Council of the EU as well as with the European Commission was further strengthened.

There were various meetings with the representatives of EU bodies in 2006. Personal contacts with the European Commission, the European Parliament and the Council have been established and fostered.

In February 2006 the Executive Director gave a presentation to the Committee for Industry, Research and Energy (ITRE) at the European Parliament. Meetings with Members of the European Parliament in Heraklion and in Brussels were also organised.



Executive Director Andrea Pirotti with the Commissioner for Information Society and Media, Viviane Reding

In addition, for example, the Commission's evaluation panel visited ENISA premises in November, 2006 as part of the scheduled mid-term review of ENISA. The Commission's report was delivered to the Commission in January 2007.

Relations with Member States were also maintained and further developed. Visits to two of the EEA countries (Liechtenstein and Iceland) took place, at which presentations on ENISA activities were delivered. These countries subsequently appointed Management



Pictured at ENISA in April 2006 are (left to right) Member of the European Parliament (MEP) Dr. Jorge Chatzimarkakis, Executive Director Andrea Pirotti, Director for Audiovisual, Media, Internet in the Information Society DG, Gregory Paulger, the Commissioner for Information Society and Media, Viviane Reding, and MEP Stavros Arnoutakis.

Mrs. Reding made a first formal visit to ENISA and the local school of European Education, and met with local Cretan authorities. Commissioner Reding commented on her visit:

"I welcome that ENISA has started with its very valuable work in Heraklion. The security of communication networks and information systems is of crucial importance for the competitiveness of Europe's industry, notably SMEs, the undisturbed operation of Europe's public administrations and for the take-up of information and communication technologies and services by citizens. It is essential that in case of security breaches or network attacks, decision-makers throughout Europe, whether public or private, can now rely on the expert advice of ENISA to identify co-ordinated responses in the interests of the smooth functioning of Europe's Internal Market."

Later in the year, the European Court of Justice clarified and confirmed the legal basis of ENISA. This ruling was welcomed by Mrs. Reding:

"Network and Information security is of key economic importance for the stability of the European economy, for the security of our society and to win the trust of consumers in new technologies, The Court's judgment confirms the Commission's view that rules which guarantee such safe, stable and trustworthy IT networks in Europe can be adopted on the basis of the EC Treaty's single market rules. I am particularly glad that today's ruling also gives legal certainty to the staff of ENISA in Greece, which I visited three weeks ago and whose valuable work I saw with my own eyes. I intend to make ENISA a key element of the Commission's future work on network and IT security."

Board members and National Liaison Officers (NLOs), and are now taking an active part in the work of ENISA.

First contacts with Romania and Bulgaria were successfully achieved during the course of the year. Proactive visits to the permanent representations of Romania and Bulgaria took place to facilitate their integration as of 1 January 2007 when these countries joined the EU.

Successful collaboration with stakeholders prompted a number of incoming requests from both the Commission and Member States for advice and assistance in matters of NIS.

Network of National Liaison Officers (NLOs)

The NLOs serve as ENISA's main contact point in the Member States and in the European Institutions, enabling an efficient exchange of information and reinforcing the Agency's activities in the Member States. ENISA's network of National Liaison Officers is of great importance and was further developed during the year.

In 2006 this involved:

- the establishment of personal contacts with all new NLOs
- the drawing up of a mailing list
- the dissemination of ENISA results and deliverables to the NLOs

- the invitation of NLOs to ENISA meetings (such as the workshops on CERTs and Awareness Raising)
- collecting information from NLOs, e.g. for ENISA studies or to establish contacts for building expert communities in different fields
- offering information and advice in response to questions from NLOs about various topics
- networking with NLOs at conferences throughout Europe.

ENISA also organised the second meeting of the NLO network which took place in Rome in October 2006. During this meeting an update of ENISA activities was provided and representatives from the Finnish EU Presidency and from the forthcoming German EU Presidency presented their main objectives in the field of NIS. NLOs from several Member States delivered presentations on some particularly successful initiatives in NIS in their countries, and an interesting exchange of views followed.

The contributions of the NLOs are particularly helpful in providing national NIS material for the 'Country Pages' that ENISA has set up on its web site (www.enisa.europa.eu/pages/country_pages.htm). These pages serve as a platform for the Member States to inform stakeholders and other EU and governmental players all over Europe about contact points and forthcoming and recent activities in the Member States, and to offer updates, reports, studies etc. With this valuable input from Member States, the ENISA web site is becoming the natural 'hub' for exchanging NIS information in Europe.

For a list of NLOs, see Annex 6.



'Who is Who' Directory and 'Who is Who' Database

In 2005, ENISA set up a facilitating tool for NIS contacts: the first European 'Who is Who' Directory in NIS. The Directory provides a comprehensive key contact information guide for the EU, its Member States' authorities and organisations operating in the field of Network and Information Security (NIS). The project began from scratch in 2005, and was further updated and maintained during the course of 2006.

The 'Who is Who' Directory has also benefited significantly from the input of the NLOs. The new version contains European contact points for NIS issues, contacts in the various Member States in the field of consumer protection and awareness raising and contacts within European bodies (the European Parliament, the Commission, the Council) as well as other relevant international institutions.



The updated 'Who is Who' Directory

Building on the information compiled for the Directory, ENISA launched a 'Who is Who' Database, initially for internal purposes. This database serves as a multi-purpose source of information and a tool for maintaining a directory of authorities and organisations in the EU Member States and European bodies. In addition, the database will act as a stakeholder relationship management system for the internal use of ENISA staff. The database includes European telecommunications regulators and government information security agencies, as well as Computer Emergency Response Teams (CERTs) and similar entities. Parts of the information in this directory will eventually become available on the ENISA web site.

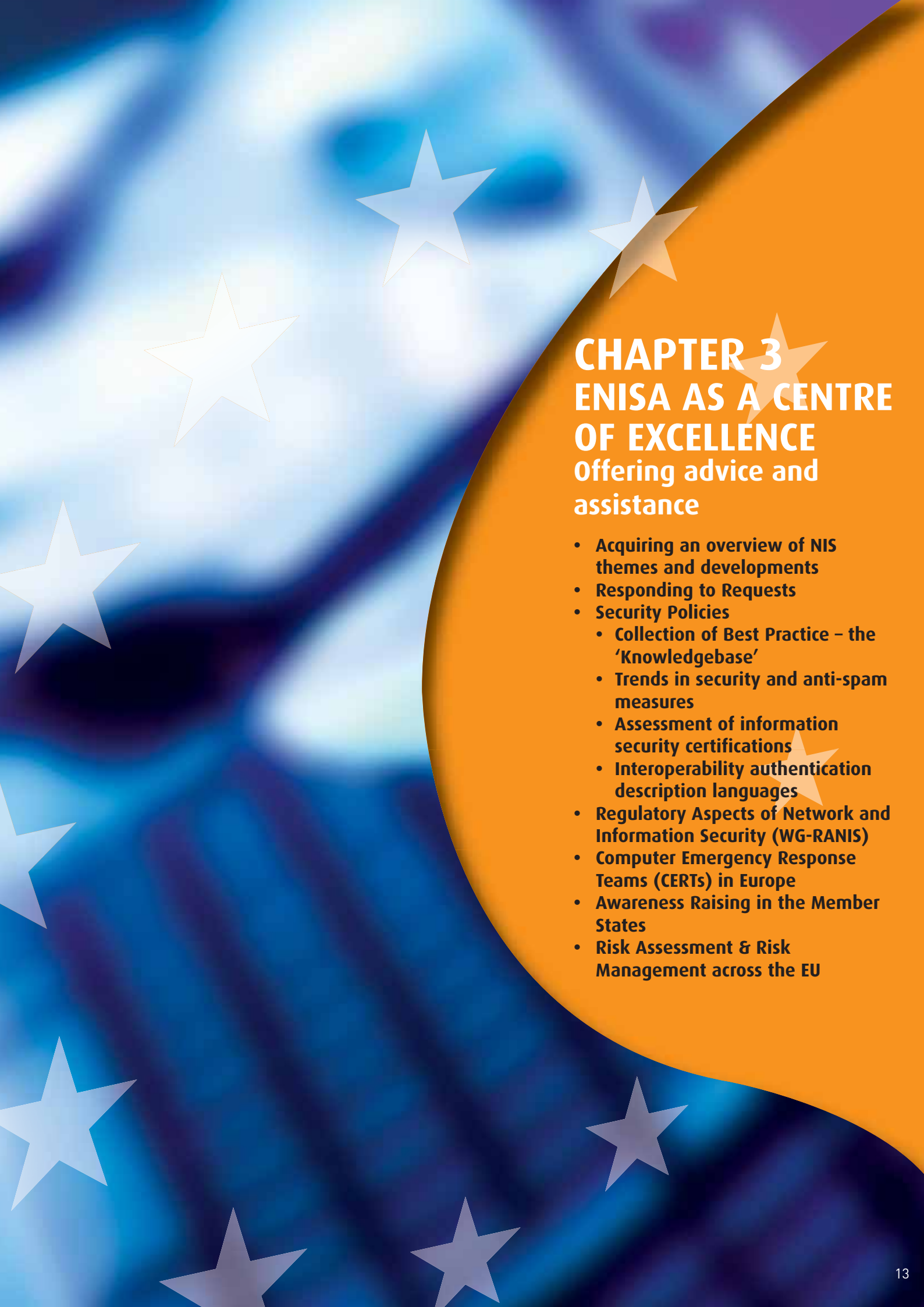
Creating a network of contacts

ENISA is a centre of Network and Information Security (NIS) expertise. This is required in its mandate, and is essential if the Agency is to effectively fulfil its advisory role.

The communities and activities involved in NIS in Europe are many. ENISA has created a good network of contacts, primarily by participating in key NIS events in Europe and world-wide, liaising with experts in different NIS fields, introducing them to ENISA and its activities, and promoting future collaboration. Strengthening this network of contacts has two main advantages: firstly, it can help ENISA maintain close contact with NIS stakeholders and is a valuable source of information to keep its knowledge of relevant technologies updated; secondly, it facilitates outreach to the technical communities.

The ENISA network of contacts includes key people in several standardisation bodies, both among the secretariat staff and technical contributors (who typically come from private companies), members of ad hoc fora and security experts within the private and public sectors and academia. This contact network will be further developed during 2007 and groups of experts will be established to write position papers on selected security topics.





CHAPTER 3

ENISA AS A CENTRE OF EXCELLENCE

Offering advice and assistance

- **Acquiring an overview of NIS themes and developments**
- **Responding to Requests**
- **Security Policies**
 - **Collection of Best Practice – the ‘Knowledgebase’**
 - **Trends in security and anti-spam measures**
 - **Assessment of information security certifications**
 - **Interoperability authentication description languages**
- **Regulatory Aspects of Network and Information Security (WG-RANIS)**
- **Computer Emergency Response Teams (CERTs) in Europe**
- **Awareness Raising in the Member States**
- **Risk Assessment & Risk Management across the EU**

Acquiring an overview of NIS themes and developments

ENISA needs to maintain an overview of ongoing technical developments and activities to understand what is important to Europe (and outside Europe). It also needs to identify overlapping activities and gaps in the provision of security measures, to help overcome fragmentation, and to foster closer collaboration among the different NIS communities and players – all of which is central to ENISA's role.

The technical areas to be investigated are numerous. NIS activities are ongoing in research (both academic and industry), in standardisation bodies and in fora of different types. Work began with the compilation of an inventory of 'fora' where relevant NIS activities were observed. (The term 'fora' is used here in its broadest sense, i.e. any body, group, project etc. discussing technical aspects of NIS.) These fora include groups dedicated to security topics, but also those addressing technical issues with security implications. The main activities of each forum have been identified and briefly described in an internal report.

Some of the identified fora were analysed in greater depth, using information gathered from their web sites and technical reports and, when possible, by participating in one of their meetings. This resulting 'Inventory of Fora' consists of short information about each selected body, a list of the most relevant documents or specifications (particularly standards) the body has produced, and its activities related to NIS. The information collected will be updated regularly and expanded.

Ultimately the Inventory is intended to be exported to a web format, to make it more readily accessible and to allow for easier updating and retrieval of information. The Inventory will form the basis for a richer web portal for ENISA's stakeholders, as a central repository of NIS standards and technical information, and will provide an overview of trends and developments.

Standardisation was the focus for this first draft of the Inventory, to fulfil ENISA's objective of standardisation monitoring. Some of the key bodies were monitored with direct participation. For example, in 2006 ENISA attended the three meetings of the Internet Engineering Task Force (IETF), the standardisation body which has responsibility for Internet architecture and protocols. Security has a deep root in IETF. The organisation has a dedicated Security Area with Working Groups addressing specific security issues but, in reality, security touches every IETF Working Group, as any protocol or system has security implications. ENISA also worked closely with the European Telecommunications Standards Institute (ETSI), by attending, as observers, an ETSI TC TISPAN standardisation meeting on Next Generation Networks (NGN) and their security aspects, an ETSI TC SCP meeting on smart cards, and the ETSI 2006 Workshop

on Security Standardisation. This co-operation has been formalised in a Memorandum of Understanding between ENISA and ETSI, and ENISA plans to continue following ETSI technical meetings in different fields and to strengthen the technical collaboration. The Agency is also currently discussing the possibility of joining the International Telecommunication Union's (ITU's) effort in standardisation tracking (Roadmap).

The organisations reviewed so far are:

- European standardisation bodies – the European Telecommunications Standards Institute (ETSI), the European Committee for Electrotechnical Standardisation (CENELEC), the European Committee for Standardisation (CEN)
- International/extra-EU standardisation bodies – the Internet Engineering Task Force (IETF), the International Telecommunication Union (ITU), the US National Institute of Standards Technology (NIST), the International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC), the American National Standards Institute (ANSI)
- Industry associations – the Voice over IP Security Alliance (VOIPSA), the Cyber Security Industry Alliance (CSIA), the Open Mobile Alliance (OMA), the Trusted Computer Group (TCG), the Virtual Private Network Consortium (VPNC), the Information Systems Security Association (ISSA)
- European institutions – EC DG Joint Research Centre (JRC)
- International institutions – the Organisation for Economic Co-operation and Development (OECD), the International Federation for Information Processing (IFIP), the Organisation for the Advancement of Structured Information Standards (OASIS)
- Other fora – the Internet Corporation for Assigned Names and Numbers (ICANN), the Open Group, RIPE



The information gathered for the Inventory formed part of the basis for a deliverable providing an 'Overview of Current Developments in Network and Information Security Technologies'. This 50-page report outlines the main developments observed during the course of work in 2006. Particularly important to note are developments in the field of cryptography (for example, new hash functions, efficient algorithms for high speed implementation and lightweight crypto), and the need for maintaining a European co-ordination of the research teams in this domain is outlined.

Developments in an area of increasing concern – infrastructure security, specifically DNS and routing – were also examined. E-mail authentication techniques are increasingly being standardised and used to combat spam. Other fields assessed include identity management and biometrics, deperimeterisation and Trusted Computing. Emerging technologies which have security implications, such as IPv6, wireless systems, RFID and ubiquitous networks, Voice over IP and multimedia applications, were studied, as well as NGN, the emerging telecommunication architecture implementing network convergence.

The 'Overview of Current Developments in Network and Information Security Technologies' will be updated and expanded in the future, as other security topics and emerging technologies are included.



Responding to Requests

One of ENISA's tasks is to deal with requests from Member States, the European Parliament and the European Commission for advice or assistance.

In 2006 ENISA dealt with a number of requests. In addition to those previously received in 2005, six new requests were received in 2006.

- In 2005 the European Commission had asked ENISA to look into industry measures taken to comply with national measures implementing the provisions of the Regulatory Framework for electronic communications relating to the security of services. The main goal of the study was to obtain information from electronic communication providers regarding their security and anti-spam measures. Two questionnaires were created in order to gather data for the study. One questionnaire was submitted to National Regulatory Authorities, the other to providers. The findings of the survey were compiled in a report which was completed and forwarded to the EC in February 2006. (See p18 for more about this work.)
- ENISA had received a call for assistance from the Communication Regulatory Authority of Lithuania to provide support in setting up the first Lithuanian governmental Computer Emergency Response Team (CERT). As a result of close co-operation with the European CERT community, ENISA's staff was able to respond quickly and helped organise a TRANSITS (Training of Network Security Incident Teams Staff) training course in Vilnius, in March 2006. The event was not limited to Lithuanian staff but was open to new CERT specialists across all of Europe.



Participants in the TRANSITS training in Vilnius

- The Commission invited ENISA's views and opinions on the Draft Impact Assessment Report for the planned Communication on 'Increased Security in Electronic Communication'. Both general and specific comments were presented in the document that was prepared in response.
- ENISA received a request to support the Commission on a number of topics related to electronic signatures. The Agency was asked to give advice regarding the status and potential future development of the Algorithm; to help draft the terms of reference for an analysis of the market for eSignatures; and to advise

on technological developments in this field. ENISA answered this request with a contribution to the eSignatures meeting in May 2006 in Brussels and with a short follow-up on the terms of reference.

- As response to a call for advice and assistance from the Commission, ENISA provided a questionnaire on the status of activities in the area of electronic identity and authentication. To fulfil this request, ENISA participated in a number of workshops throughout the year and delivered presentations. The final deliverable was the Roadmap on eIDM for eGovernment services that ENISA co-drafted, which was accepted by the Member States. The report is available upon request.
- ENISA has also received a request for assistance from the Ministry of Informatics in the Czech Republic to give advice on Public Administration Information Systems (PAIS) and related security requirements. A comprehensive report was prepared in August 2006, outlining the various European legal and regulatory requirements that implementers of such systems face. The report is available upon request.
- Recently, ENISA has received a request from the European Commission (DG INFSO) to examine the feasibility of an EU-wide information and alert system (EISAS). The Agency is currently working on this request.
- ENISA received a request from the European Data Protection Supervisor (EDPS) to help conduct an in-depth security audit. Although ENISA's role does not include engaging in operational activity, the Agency was able to support the EDPS by helping to select appropriate experts from the Member States and providing additional advice. Experts from France, the UK and Germany have now met with the EDPS and the audit has commenced. The report will be available early in 2007.

- ENISA received a request to examine the feasibility of creating a partnership to establish a framework for the collection of data on information security and consumer confidence. This partnership would aggregate information such as volumes and trends of security incidents, but not information about individual events. Such data is already available from some public and private sources, but presented in varying ways, without a common structure, making it difficult for decision-makers to see the big picture. The long term goal of this partnership is to deliver consistent information to policy-makers, allowing them to base their decisions on accurate information on incidents and consumer confidence. Work on this request commenced in October 2006 with ENISA's contribution to a workshop on the exchange of sensitive data between various public and private European partners, and will continue in 2007.

Security Policies

ENISA's Work Programme 2006 lists four deliverables in the area of Security Policies. In addition, there were security policy implications in five Requests for Assistance dealt with during the year. This resulted in a total of nine different activities, covering a wide range of different topics and requiring different expertise and skills.

Work in this area was boosted during 2006 with the appointment of a new Expert and a trainee.

Deliverables

- Collection of Best Practices
- Study on security and anti-spam measures of providers
- Assessment of information security certifications
- Plan for co-ordination of authentication languages

Requests

- Advice on security audit for the EDPS
- Preliminary results on study of security and anti-spam measures of providers
- Advice to the Commission regarding digital signatures
- Advice to the Czech Republic on Public Administration Information Systems
- Preparation for a feasibility study into a partnership to establish a framework for the collection of information security data

Collection of best practice – the ENISA 'Knowledgebase'

Collecting best practice on information security policies and beyond has been an ambitious task and is an ongoing activity. Numerous such collections are already available on the Internet. The specific approach and added value of ENISA's activity is not only to create such a collection, but to design it in a way that it can be used for the development of aggregated, concise best practice guides and policies. The basis of this is a consistent terminology that is used across the database plus an intelligent tagging mechanism for all documents.

An existing document management system has been enhanced with such features, and dubbed the 'Knowledgebase'. Although originally planned only as a store for policy documents, it can also be used for other security documents at ENISA.

The ENISA Knowledgebase has been available since October 2006. The internal test phase will last until mid-2007 when the Knowledgebase will be made available over the Internet to a larger audience.



Trends in security and anti-spam measures

In 2006, ENISA published two reports focusing on developments and trends in security and anti-spam measures.



In December 2005, ENISA received a request from the Commission to commence work immediately on a study on security and anti-spam measures of providers, which had originally been planned as part of the Work Programme 2006 for Q2. With the Commission looking for results in February 2006, it was decided to conduct the study in-house.

The goal of the study was to analyse how providers of electronic communications services (e.g. Internet Service Providers, telecommunication companies) secure their services and protect their clients from spam and security threats. These requirements are expressed in national laws, which are transpositions of EU Directive 2002/58/EC.

Since no network of contacts for providers had been established yet, the questionnaire that was developed was sent to several 'multipliers', i.e. the European Regulators Group (ERG), RIPE and others, to identify what specific measures were actually taken to put national laws and regulations into practice. A slightly adjusted version of the questionnaire was also sent to National Regulatory Authorities (NRAs).

The survey elicited responses from almost 100 electronic communications service providers (Internet Service Providers (ISPs), telecommunications operators etc.) as well as NRAs.

The results of the survey can be summarised as follows:

- With regard to technical measures, there should be an incentive for providers to contribute to the overall security of interconnected networks rather than protecting merely their own resources. Egress filtering must be encouraged.
- Providers need to be more proactive and monitor their networks for risks of security breaches. Providers should also be asked to report which networks they monitor.
- With regard to organisational measures, the necessity for clear documentation and regular communications on information security should be emphasised. Contact details for e-mail abuse and security violations are also important.
- Providers in Europe are more concerned about spam e-mail that their customers receive than about the spam that they send. With regard to outgoing spam, they rely mostly on legal instruments such as Terms and Conditions. Enforcement could be further improved to also prevent spam originating from Europe.

Survey on Industry Measures taken to comply with National Measures implementing Provisions of the Regulatory Framework for Electronic Communications relating to the Security of Services – available in print and online at: www.enisa.europa.eu/doc/pdf/deliverables/enisa_security_spam.pdf



Follow up work continued with attendance at relevant events and with web-based research.

The second study in this field was published in July 2006. The report contains a synthesis of key facts, conclusions and proposals, based on the findings of the survey. For example, it confirms that ISPs, telecommunication companies and content providers largely comply with European laws. At the same time the report also points out that providers fall short in a number of areas including informing customers about the costs of countermeasures, finding the right balance between privacy and security and protecting neighbouring networks. The report recommends that providers should deepen their analysis of incidents and share information about countermeasures. It suggests that Europe would benefit from a warning mechanism to identify and address imminent threats and, ideally, the reporting of security measures and breaches should be made mandatory.

The report points out that, according to European law, providers must secure their services and implement measures to reduce the burden of spam. However, depending on the nature of the business affected and the kind of anticipated threat, the implementation levels of anti-spam measures vary widely. Technical measures range from traffic filtering and the use of blacklists to quarantining of infected computers. Organisational measures include security process definitions, written guidance for staff and customers and clear contact details for e-mail abuse. An ISP that has enterprise clients chooses different measures compared with one with large numbers of home users.

Important key results in the ENISA study include:

- As filtering is commonly perceived as intrusive, European providers find themselves in a conflict between 'protection of the network', requiring detailed traffic filtering to be effective, and 'protection of privacy'.
- The threats that providers encounter change rapidly. Consequently, continuous updates on security countermeasures and awareness raising strategies are vital. Transparency as to successful measures is thus needed to reduce incidents.
- Although Europe was long seen as a region that is mostly suffering from incoming spam, increasingly Europe is also being identified as the source of spam. The new trend is to send spam from 'botnets' planted in Europe, while spammers themselves reside overseas.
- Moreover, many providers focus on protecting their own network and pay less attention to threats affecting their neighbours.

Overall, the results of this work can be summarised as follows:

- Europe needs to increase the transparency of security measures. This requires the reporting of security breaches and a more proactive approach to raise awareness about security and spam problems.
- Appropriate security has to be defined, including the state of the art and the necessary cost of security measures. It is also necessary to find the right balance between security and privacy in e-mail communications.
- Guidance is needed on best practices and standards for technical and organisational security measures as well as on anti-spam measures.

Security and Anti-Spam Measures of Electronic Communication Service Providers Status and Outlook – available in print and online at: www.enisa.europa.eu/doc/pdf/deliverables/enisa_security_spam_part2.pdf



Assessment of information security certifications

Europe is concerned about the state of information security. There are numerous actual and perceived IT security risks – and these risks have to be managed. To do so, organisations employ experienced staff, define processes and deploy products. But how does an organisation know that staff, processes and products are appropriate to help mitigate risks? The use of accreditation and certification schemes is considered one element in describing the usefulness of a product, process or person. However, a lack of general recognition of certifications hinders an uptake of this market. On the other hand, wide recognition and improved visibility of such schemes would help providers and users of certifications and make the market more open and dynamic.

To address these matters, ENISA organised a workshop on the theme ‘What can we achieve with information security certification? – Voice your opinion on information security certifications in Europe’, which took place during the second half of 2006. The goal was to assemble and discuss opinions about the use of information security certifications in Europe, and to prepare for the promotion of such certification schemes in 2007.

Over 20 presenters from certifying organisations, laboratories, vendors, consultancies, governments and regulatory authorities offered their opinions on certifications to an audience of more than 40 people from 15 countries, mostly from within the EU. In preparation for the event, ENISA had distributed a questionnaire and received 26 responses plus 8 position papers from the industry. In total about 70 experts on information security certifications contributed to this assessment.

Key questions considered in the Information Security Schemes workshop:

- What determines the usefulness of certification schemes? – The market? Governments? An accreditation scheme? Marketing?
- What is the most appropriate way to evaluate the state of a product/person/process prior to issuing a certificate? – An examination or a more or less formal evaluation? A peer review? A third party analysis?
- Are there links between different certification schemes? Is there a common terminology or language for people, process and product certifications?
- Are there areas where European governments should mandate the use of schemes? On the other hand, are there areas in which governments should not interfere?
- What are the pros and cons of Common Criteria? Can we make a security ‘driver’s license’ mandatory for IT security professionals? Should there be an accreditation of personal security certification schemes? Is it useful to require compliance with ISO 27001 for government contracts?



In the workshop, the experts discussed whether and how accreditation and certification schemes help to ascertain value and when a scheme can be considered successful. The workshop participants also discussed whether user organisations, governments and vendors need to do more – or if they should do less – with regard to such schemes.

During the course of the workshop it became clear that certifications of organisations, certifications of people and certifications of products have to be dealt with separately, even though there are some commonalities and a certain overlap. In addition, information security certifications should be seen in context with other certifications, such as privacy certifications, certifications of physical security and other IT or process certifications.

ENISA does not seek to endorse any specific information security certificate. However, there are some characteristics that are common to many different certification schemes.



Findings from the Workshop

- Showing the value of any certificate is challenging. Among other things, its perceived value depends on its pervasiveness, appropriateness, accuracy and acceptance.
- The more thorough an evaluation for a certificate, the more lengthy and costly the process. Finding the right balance between time/cost and thoroughness also depends on the scope of the certificate.
- There is a trade-off between volume and quality. A certification scheme needs a certain volume of certificates to be visible in the market. On the other hand, the entity to be certified has to undergo a thorough evaluation process to ascertain quality. The more complex the evaluation process, the slower the uptake of any given scheme.
- Information security is a rapidly evolving space. A renewal of the certificate is necessary after a certain period of time.
- Having a certificate and being secure are not the same. Certified entities can be vulnerable (even though that does not invalidate the certificate in its original scope).
- Some certification schemes are complex and pose a heavy burden on those who undergo certification, making certification difficult for small and medium-sized organisations. In such cases, a simplified version of the certificate and additional guidance would be valuable.
- Whether specific certificates should be required by law remains a topic of controversial discussion.

A draft report was presented as a deliverable to ENISA's stakeholders (the EU Commission, Member States, industry and academic representatives). The results are available in the form of an ENISA report that describes the different opinions and outlines ways to promote information security certifications in 2007 and beyond.

Further analysis and promotion of information security certification schemes will continue throughout 2007, including a discussion with European experts on certifications about specific schemes.

Interoperability authentication description languages

A clear language for describing authentication methods is vital in establishing the trustworthiness of electronic transactions, both for citizens and for governments and enterprises. It is important to be able to evaluate and compare available methods using consistent and relevant descriptions. An initial study period by ENISA revealed that a number of parallel initiatives already exist in this area. The objective now is to harmonise the results into a common language with a view to interoperability, liability control and clarity for end-users.

First European Workshop on Authentication Description Languages

As the first step in a process leading to interoperability of languages for describing authentication methods, ENISA organised a workshop in November 2006, which brought together experts working in this area to discuss what action should be taken. The event was attended by experts from industry, research and governments who wanted to use or promote a common language. The output of the discussions was brought together to create an action plan for 2007-2009.

Probably the most important part of the action plan is the setting up of an interest group to work towards an interoperability standard for authentication descriptions. This follows an agreement made between the delegates of the workshop. The final deliverable of this interest group will be a formal specification of a language and a definition of assurance mechanisms for the language.

Initially the interest group will work on use-cases to provide a full set of requirements and benchmarks for the language. The use-cases include e-Government, Federated Identity Management, anonymous access control via selective attribute disclosure, GRID and academic scenarios, network layer and Mobile authentication. The group will then divide the work on the language into the following packages:

- High-level concepts for authentication classification
- Detailed low-level authentication description language
- Assurance mechanisms for descriptions

The action plan also foresees the creation of a directory of relevant materials and work.

Other important conclusions from the workshop incorporated in the action plan were:

- The language should also consider how to describe reputation-based authentication. Reputation as a means of authenticating users (for example in spam filters) is a growth area, which also carries important threats such as denial-of-reputation.
- In order to establish true cross-border interoperability of authentication tokens, the concepts of the language should be interpretable across different legal systems. For example, the privacy level of a given mechanism may be interpreted differently in different jurisdictions.
- If authentication contexts are to be quantified (i.e. levels applied), then a clear basis must be established for the application of the levels. Current candidates for criteria can be broadly divided into risk level, attack level and confidence level.
- The language should allow description of privacy and anonymisation features of authentication contexts.
- The language should include the ability to describe enrolment procedures used in creating authentication mechanisms.



The Tower of Babel by Pieter Breugel, the Elder

Regulatory Aspects of Network and Information Security (WG-RANIS)

ENISA is co-ordinating an ad hoc Working Group on Regulatory Aspects of Network and Information Security (WG-RANIS), whose task is to collect EU regulatory information related to Network and Information Security (NIS) and to consider appropriate regulatory principles of existing EU regulation.

Network and Information Security has long been subject to regulatory action at EU level. In recent years this trend has continued at varying speeds. There are currently several examples of legal requirements affecting information security in legislation, such as telecommunications, data protection, e-Government, corporate governance, identity management, financial legislation etc. WG-RANIS addresses EU regulations and

legislation that have developed and which are within the scope of the technical and organisational measures associated with electronic transactions in the internal market. The Group's deliverables are made available primarily for internal ENISA purposes.

WG-RANIS has produced a deliverable (currently pending approval by the Agency) which includes:

- An inventory of EU-regulatory activity on Network and Information Security.
- A brief overview of existing principles for Network and Information Security.

For a list of the members of WG-RANIS, see Annex 5.



Computer Emergency Response Teams in Europe

CERT is the abbreviation for the term Computer Emergency Response Team, a synonym for CSIRT, Computer Security and Incident Response Team. A CERT is an organisation 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.

One of ENISA's main tasks is to facilitate the setting up of CERTs, CERT co-operation and the enhancement of CERT services, by collecting and promoting good practice, in particular among European CERTs.

The handling of security incidents, one of the first duties of a CERT, requires co-operation between teams across institutional and national borders, for which, over time, CERTs have built up well functioning communities. Several security communities in Europe such as TF-CSIRT, E-COAT, the EGC and WARP have collaborated to ensure a more secure Internet for several years now. These communities meet on a regular basis to discuss technical and operational matters to try to solve problems together. Overall, CERT communities are indispensable tools to build bi- and multi-lateral trust relations.

Through continuous, close co-operation, trust is gradually built up. This exchange of sensitive information has established the basis for incident handling.

ENISA therefore takes into account work that has already been undertaken in this field by the different CERT communities, and co-operates closely with them. CERTs had existed and co-operated for more than a decade when ENISA entered the scene. Reinventing wheels and burdening the European CERT communities with unwanted ideas is an obvious danger that ENISA's CERT experts have successfully avoided from the very beginning.

Setting up and facilitation of co-operation in 2006

The ENISA Work Programme for 2006 included two main projects:

- A guide on how to set up a CERT (including a checklist)
- A report on CERT co-operation and its further facilitation

2005

Stocktaking



2006

Setting up & Co-operation



2007

Support operation (+ broaden focus!)

- Quality assurance
- Advanced Training

Prepare to contribute to "NIS brokerage"!

2008

Finalise basic work

A sound set of basic documents should be available now.

The FUTURE:

Now extensively collect good practices and contribute to NIS brokerage!

Continuous work in the field of CERTs – ENISA and CERTs: the 'big picture'

How to set up a CERT – the guide



The CERT Step-by-Step Guide

This unique, concise but comprehensive process description was published in October 2006 and was received very positively by ENISA's stakeholders and the CERT communities. There are several aspects of the document that are particularly appreciated by readers:

- it is a complete but concise process description of every aspect of setting up a CERT
- it contains numerous illustrations (workflows, models, statistics), wrap-ups, examples and exercises
- it is generic enough to serve several target groups
- it is supplemented by numerous references to other sources
- it is based on 'real life' experiences

The guide on how to set up a CERT is available on ENISA's web site:
www.enisa.europa.eu/cert_guide/index_guide.htm

How to set up a CERT – the project plan

The guide is complemented by a project plan aimed at helping the reader to implement the exercises in the guide. The plan is available in MS Project and in a generic XML format that can be loaded in any software tool for project management. It includes all the tasks laid down in the guide and is supplemented by an example timeline.

The checklist is also available from ENISA's web site:
www.enisa.europa.eu/cert_guide/pages/14.htm



CERT co-operation – the report

The third ENISA deliverable produced in this field in 2006, 'CERT co-operation and its further facilitation by relevant stakeholders', is the first document of its kind. It not only tells the story of co-operation in Europe and beyond, but also summarises the lessons learned and makes recommendations to relevant stakeholders as to how co-operation can be improved. This document is aimed primarily at management, policy-makers, teams and other stakeholders who, in one way or another, are involved in CERT co-operation.

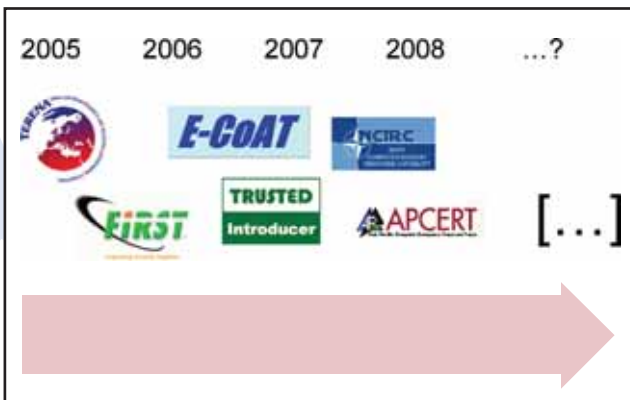


2nd Workshop 'CERTs in Europe'

For the second time ENISA gathered participants from the EU Member States and the European CERT communities for its one-day workshop, 'CERTs in Europe', that took place in Brussels on 5 October. Supported by presentations by well known experts (for example Georgia Killcrece from the CERT Co-ordination Center (CERT/CC) who came all the way from Pittsburgh, USA), ENISA introduced its latest deliverables. The audience was well balanced between experts from the various CERT communities in Europe and beyond (TF-CSIRT, FIRST, CERT/CC) and project managers who are charged with the setting up of such a team in their home countries. As well as the valuable information that was shared via the expert presentations, these 'newcomers' had a unique opportunity to discuss their concerns, problems, expectations and plans with the experts convened there.

Expanding the CERTs network

Besides these deliverables, ENISA initiated contacts with all relevant players in the CERT field, meeting representatives from FIRST, TF-CSIRT, the American CERT/CC and Asian-Pacific-CERT. The Agency enhanced its fruitful co-operation with the TRANSITS team, which resulted in co-organising CERT training courses in Europe (in Lithuania and in Switzerland).



In a further effort to promote collaboration between CERT contacts, in co-operation with the Institute of Electrical and Electronics Engineers (IEEE) Computer Society Task Force on Information Assurance, ENISA supported the third DIMVA (Detection of Intrusions & Malware and Vulnerability Assessment) conference in Berlin, Germany. An annual conference organised by the German Informatics Society's special interest group on Security – Intrusion Detection and Response (SIDAR), DIMVA brings together experts from throughout Europe and beyond to discuss the state of the art in the areas of, for example, intrusion detection, malware detection and network forensics, and vulnerability assessment.

ENISA promoted a workshop on the setting up of new CERTs for key players from Azerbaijan, Armenia, Belarus, Georgia, Kazakhstan, Kyrgyzstan, Moldova,

Turkmenistan, Ukraine and Uzbekistan. Hosted by CERT Polska, the Polish national CERT, the workshop aimed to guide and assist these countries in setting up and running teams, and to bring them up to date with the latest developments in the field of CERTs. ENISA welcomed the emergence of this new CERT community in the central and eastern parts of Europe and will continue to offer assistance.

ENISA recognised as member of FIRST



Marco Thorbruegge

ENISA's Senior Expert for CERTs, Marco Thorbruegge, was granted the status of a 'Liaison Member' of the international organisation, the 'Forum for Incident Response and Security Teams' (FIRST) – one of only 16 worldwide. This is a recognition that ENISA staff are well respected as experts in their field all over the world.

The Working Group CERT Services

Building on the findings of the Ad hoc Working Group on CERT Co-operation and Support, which was active in 2005, in 2006 the newly created Working Group CERT Services (WG-CS) dealt with questions related to the provision of adequate security services ('CERT services') to specific (categories or groups of) users.

The new Group's first task was to look into possible measures for the assurance of an appropriate level of quality for providing security services by CERTs and similar facilities. The result of this work will be used in the inventory of quality assurance measures which ENISA is scheduled to deliver in 2007.

A second task for the Working Group was to categorise users and user groups for 'CERT services', to produce a list of appropriate facilities for providing these services and users' expectations of them.

Finally, the Group made suggestions to close some of the gaps in coverage with security services, ascertained in the gap analysis of the 2005 Working Group.

For a list of the members of the Ad hoc Working Group on CERTs, see Annex 5.

Awareness Raising in the Member States

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 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. In that way the Agency is contributing to the implementation of its mission to facilitate the establishment of a culture of network and information security.

The following activities were carried out in the field of Awareness Raising as part of ENISA's 2006 Work Programme:

- Compilation of 'A Users' Guide: How to Raise Information Security Awareness'
- Developing 'Information Security Awareness Programmes in the EU – Insight and Guidance for Member States'
- Organising a workshop to disseminate the main findings to the Member States representatives

'A Users' Guide: How to Raise Information Security Awareness'



This Guide provides practical advice for Member States to help them prepare and then implement awareness-raising initiatives related to information security.

The information covered within the document features step-by-step advice which could form the basis of an effective awareness campaign targeted at different audiences, such as public and private organisations. The Guide identifies the main processes and activities necessary to run an awareness campaign. The processes have been defined as follows: plan and assess; execute and manage; evaluate and adjust. For each process a few activities have been identified. A series of steps and recommendations have been

included in this section to help the reader implement awareness initiatives and programmes. Moreover, the Guide suggests using a number of tools for which templates and samples have been included in the document (e.g. a lessons learned template; a work plan sample; a target group data capture form etc.).

Specifically, the report:

- Illustrates a sample strategy for how to plan, organise and run an information security awareness-raising initiative
- Highlights potential risks associated with awareness initiatives in an effort to avoid such issues in future programmes
- Provides a framework to evaluate the effectiveness of an awareness programme
- Offers a communication framework
- Contributes to the development of an information security culture in Member States by encouraging users to act responsibly and thus operate more securely

'A Users' Guide: How to Raise Information Security Awareness'

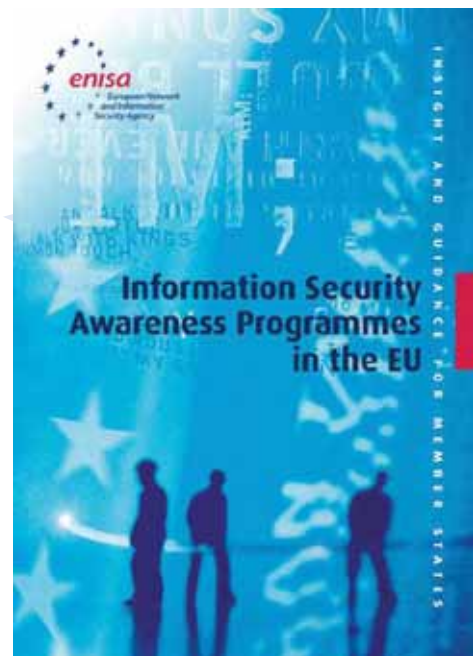
Primary areas of focus include:

- **Effective Communication Planning**
A communication strategy is at the centre of any effective awareness programme, but the strategy needs to be adapted to a specific context, i.e. it must:
 - be based on communication goals and principles
 - be aligned with target group needs
 - take into account different target groups
 - cover both regular and situational communication needs
 - be adapted to target group feedback
- **Change Management Approach**
Applying a change management approach to an awareness initiative is crucial as it helps close the gap between a particular issue and human responses to the need to change, even in the case of a cultural change.
- **Measurement of the Value of Awareness Programmes**
The need for security awareness is widely recognised. However, not many public or private organisations have tried to formally quantify the value of awareness programmes. Evaluation of a campaign or programme is essential to understand its effectiveness as well as to make adjustments based on what has been learned to date. Evaluation metrics cannot be universally applied to all target groups since needs and situations differ greatly.

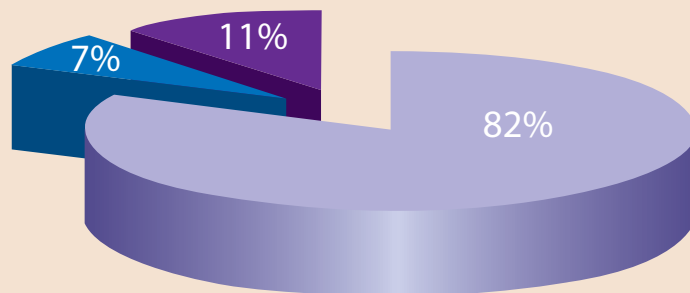
'Information Security Awareness Programmes in the EU – Insight and Guidance for Member States'

The Agency has developed 'Information Security Awareness Programmes in the EU – Insight and Guidance for Member States' which provides an overview of EU awareness programmes either undertaken or underway within Member States.

The information was compiled from the responses received from countries and PSG members to an ENISA questionnaire.



ENISA Questionnaire - Countries' Contributions



28 countries received the ENISA questionnaire

■ 23 countries replied to the questionnaire (82%)

■ 2 countries, of which 1 EEA did not reply to the questionnaire (7%)

■ 3 countries, of which 1 EEA supplemented with other material than the questionnaire (11%)

This information was supplemented by interviews, research and additional material. It is envisaged that the details contained will be used to help disseminate practical information about good practice, as well as to offer an opportunity to monitor progress in national approaches to addressing information security awareness. ENISA has also constructed good practice recommendations and offers guidance on running awareness raising campaigns. This includes information on metrics and key performance indicators (KPIs). A roadmap was also created to show a holistic progression of awareness raising initiatives.

ENISA Questionnaire - Sections

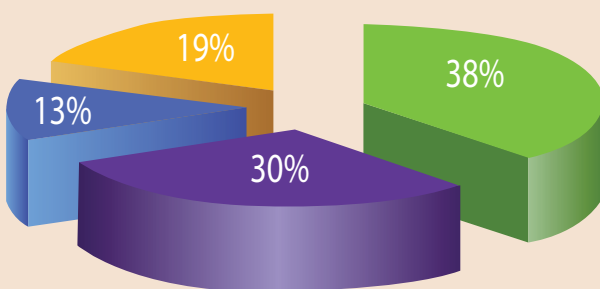
Section	Topic	Inputs	
		Member States	PSG
Section 1	Government as developer of legal, regulatory and institutional arrangements to raise awareness	✓	
Section 2	Government as user of information systems	✓	
Section 3	Local government as user of information systems	✓	
Section 4	Government as partner with business and industry	✓	✓
Section 5	Government as partner with civil society	✓	✓
Section 6	Metrics and key performance indicators (KPIs)	✓	✓

Findings from ENISA's research

Analysing the initiatives and efforts by Member States, several trends and commonalities were identified with the work completed to date:

- The total number of awareness raising initiatives in the EU has slightly risen over the last year.
- Two-thirds of awareness programmes conducted have been run in the north of Europe.
- As in the past, the difference in nature and number of awareness initiatives derives from the different levels of information security understanding and culture within the countries.
- Almost every programme in Member State countries targeted the Small and Medium Enterprises (SME) and Home User groups.

Awareness Programmes by Target Group



- 20 awareness initiatives targeted Home Users (38%)
- 16 awareness initiatives targeted SMEs (30%)
- 10 awareness initiatives targeted Local Government (19%)
- 7 awareness initiatives targeted ISPs (13%)
- 0 awareness initiatives targeted the media (0%)

- Awareness raising collaboration is growing with Internet Service Providers (ISPs).
- As in the past, phishing, spam and protection through firewalls are the main themes that are covered.
- Awareness raising subjects that are growing in coverage include the use of mobile devices and WiFi.
- Web sites and training remain the most used communication channels to deliver the message as part of any awareness raising initiative.
- Media is still primarily being used as a channel of communication, and not as a target group. Responses from Member States detailed in the Information Package confirm this.

ENISA identified several key prerequisites and actions that are required for a successful awareness raising initiative:

- The message delivered has to be appealing and perceived as 'of value' to the target group – the audience should be properly evaluated with interests, needs and knowledge identified.
- Communication channels should be analysed to identify then use the optimal delivery mechanisms – preferred communication channels per target group should be understood and utilised.
- Public-private partnerships should be used to leverage synergies to help make sure that the initiative has the resources and expertise to deliver the right message to the right people, using the most effective channels.
- Multipliers such as teachers and the media should be used to help increase the scope and coverage of any awareness raising initiative.
- Metrics and KPIs should be used to measure the effectiveness of an initiative – lessons learned through analysis of quantitative and qualitative data can be used to help improve future campaigns.



2nd Awareness Raising Dissemination Workshop

In October 2006, ENISA's Awareness Raising unit organised its second Workshop on Awareness Raising Dissemination to share its findings within the EU Member States. The workshop brought together policy-makers who are responsible or involved in awareness raising activities in their home countries.

Through a combination of presentations, case studies and panel debates, participants explored cutting edge topics, key issues and emerging good practice in the awareness raising field. Particular focus was placed on public-private partnerships, SMEs, children and recent and successful government collaborative initiatives with ISPs aimed at raising awareness among users. In addition, the issue of appropriate metrics to evaluate the effectiveness of awareness programmes was discussed in depth. The workshop included several speakers who provided some of the material used for the compilation of ENISA's deliverable, the 'Information Security Awareness Programmes in the EU – Insight and Guidance for Member States'.

It was concluded that it is crucial to:

- draw from the experience of other countries as awareness training and campaigns around Europe present many similarities
- share knowledge as to how to raise information security awareness, and
- review and re-use material available in different countries.

To this end, ENISA will continue to promote the exchange of information and provide material that could be customised and presented to the EU Member States to facilitate their work on awareness raising. ENISA and the EU Member States will intensify their efforts to influence the public's behaviour towards information security positively, changing the mindset of the human element in order to achieve greater self-awareness.

Other awareness raising activities



ENISA promoted Safer Internet Day, which was held on 7 February under the patronage of Commissioner Viviane Reding. The Agency participated in the

conference organised by Iceland and took part in the Safer Internet Day blogathon, which was organised with about 30 countries and 10 organisations, stretching over several time zones, and executed in several languages. During this event, parents, teachers and young people shared experiences and cultural attitudes about their use of new technologies. The aim was to raise awareness about important ethical, legal and safety issues, such as the posting of personal information and the publishing of copyright material.



Risk Assessment and Risk Management across the EU

ENISA tasks in the area of Risk Assessment and Risk Management include:

- the promotion of Risk Management activities within public and private sector organisations
- the generation of a 'common language' in the area of Risk Management to facilitate communication between stakeholders
- the generation of surveys providing overviews of existing tools and best practice
- the promotion of the development of interoperable Risk Management solutions
- the integration of Risk Management/Risk Assessment (RM/RA) with corporate governance.

In 2006 RM/RA work mainly addressed problems such as:

- the low awareness of Risk Management activities within public and private sector organisations
- the absence of a 'common language' in the area of Risk Management to facilitate communication among stakeholders
- the lack of surveys on existing methods, tools and good practice.

The Agency's tasks include the collection of examples of best practice, the sharing of information and the facilitation of co-operation between relevant European initiatives with the aim of reaching a common superior level of security culture.

Making information on Risk Assessment and Risk Management widely available

Today, a number of different approaches to risk assessment and risk management exist in the various Member States of the European Union (e.g. with BS7799 in the UK, EBIOS in France and the IT Baseline Protection Handbook in Germany). There are also other methods for the management of information security that include specific recommendations for the assessment of risks. While the various approaches have many things in common, there are a number of important differences.

It seems that there is no general 'one-size-fits-all' approach to risk assessment and risk management for organisations of different sizes and with different backgrounds. Large organisations with dedicated security management teams usually also have the resources and the knowledge needed for selecting a suitable approach for risk assessment and risk management and for establishing the corresponding processes. On the other hand, smaller organisations, and particularly Small and Medium-sized Enterprises (SMEs), often have neither the staff nor the resources to conduct a risk assessment on their own. Even selecting a suitable consulting company to assist in setting up a risk management operation can be a very challenging task for small organisations.

Achievements in 2006 include:

- an inventory of existing RM/RA methods and tools (which is a continuous task)
- RM/RA information packages for SMEs
- an overall Risk Management road map document for issues to be considered in the future
- An information package for SMEs demonstrating how a small company can effectively cope with Risk Management/Risk Assessment at lowest possible cost

A specialised ENISA deliverable was prepared which gives advice to decision-makers in SMEs on how to initiate and maintain Risk Management/Risk Assessment strategies at the lowest possible cost. One of the options suggested is a guide to good practice in self assessment. The applicability of such good practice is demonstrated by means of two examples from SMEs.

In the second half of 2006 ENISA delivered the first EU/European database of information on Risk Management/Assessment in the form of a web site (www.enisa.europa.eu/rmra). This focused particularly on the presentation of a common language and featured inventories of existing methods and tools.

In the future, ENISA will expand this information database with new methods and tools, examples and demonstrators, and will cover additional aspects of Risk Management/Risk Assessment. By analysing existing RM/RA methods and tools, by providing information for applying these methods within SMEs and finally by disseminating this information, ENISA will promote the use of RM/RA in different target groups.

For a list of members of the Ad hoc Working Group on Technical and Policy Aspects of Risk Assessment and Risk Management, see Annex 5.



The Risk Assessment and Risk Management team

ENISA's Risk Management/Risk Assessment web site

The site covers numerous aspects of Risk Management/Risk Assessment including:

- Visualisation and detailed presentation of phases and activities of Risk Management/Risk Assessment
- Positioning of Risk Management within an Information Security Management System
- Inventory of 13 methods used in Europe with extensive information about each method
- Inventory of 12 tools used in Europe with a description of their functionality
- Comparison functions for methods and tools
- An overall detailed road map
- A glossary of terminology
- Downloads of the available report and description templates for methods and tools

How to select and use the right RM/RA methods and tools?

During 2006, the Working Group on Risk Assessment and Risk compiled an overview of existing RM/RA methods, highlighting both their similarities and their differences. Important organisations active in the field of Risk Assessment and Risk Management methodologies were also identified and their relationships described. This information, together with extensive data on RM/RA tools, was introduced on to the ENISA web site.

The Working Group chose several different types of organisations (notably SMEs) and suggested a suitable approach to risk assessment and risk management for each type. The goal was to allow the organisations to perform a risk assessment with reasonable effort and to establish an efficient system for managing the risk to information security. ENISA is now using this information to prepare a guide for SMEs on how to apply RM/RA methods. This guide will also include possible alternatives for the performance of assessments, either self-assessments or assessments through outsourcing the relevant effort.

Finally, the Working Group developed a roadmap on the steps which need to be taken, and by whom, in order to enhance the compatibility and interoperability of different methods of risk assessment and risk management. The objective was to improve the comparability of risk assessments between different organisations. This road map has been adopted by ENISA and is also on the ENISA RM/RA web site.

Current and Emerging Risks

ENISA conducted a study of emerging risks as background to initiatives in 2007 on current and emerging risks. As RM/RA methods and tools available today are not fully compatible in their ability to identify and assess emerging or future risks, ENISA is seeking to identify what kind of information is needed to conduct

Risk Assessment for risks which are relevant during the next two to three years.

In addition, ENISA also began work on 'Emerging Risks related Information Collection and Dissemination', with the aim of identifying which kind of information is necessary to perform Risk Assessment or Risk Management in the future within different timeframes. It is clear that one of the biggest challenges in Risk Assessment is that, after defining the correct scope of the RM or RA, one needs to identify the relevant information, the information sources needed to assess risks and how to disseminate this information. This project will provide examples of relevant information together with information sources for timeframes from today right through to future risks realised after 10 years.

ENISA Workshop on Risk Management

ENISA organised a workshop on Risk Management in Rome, Italy, as part of a series of events designed to:

- Communicate achieved results
- Gather user feedback and user requirements
- Disseminate results and information
- Inform stakeholders about new developments in Risk Management.

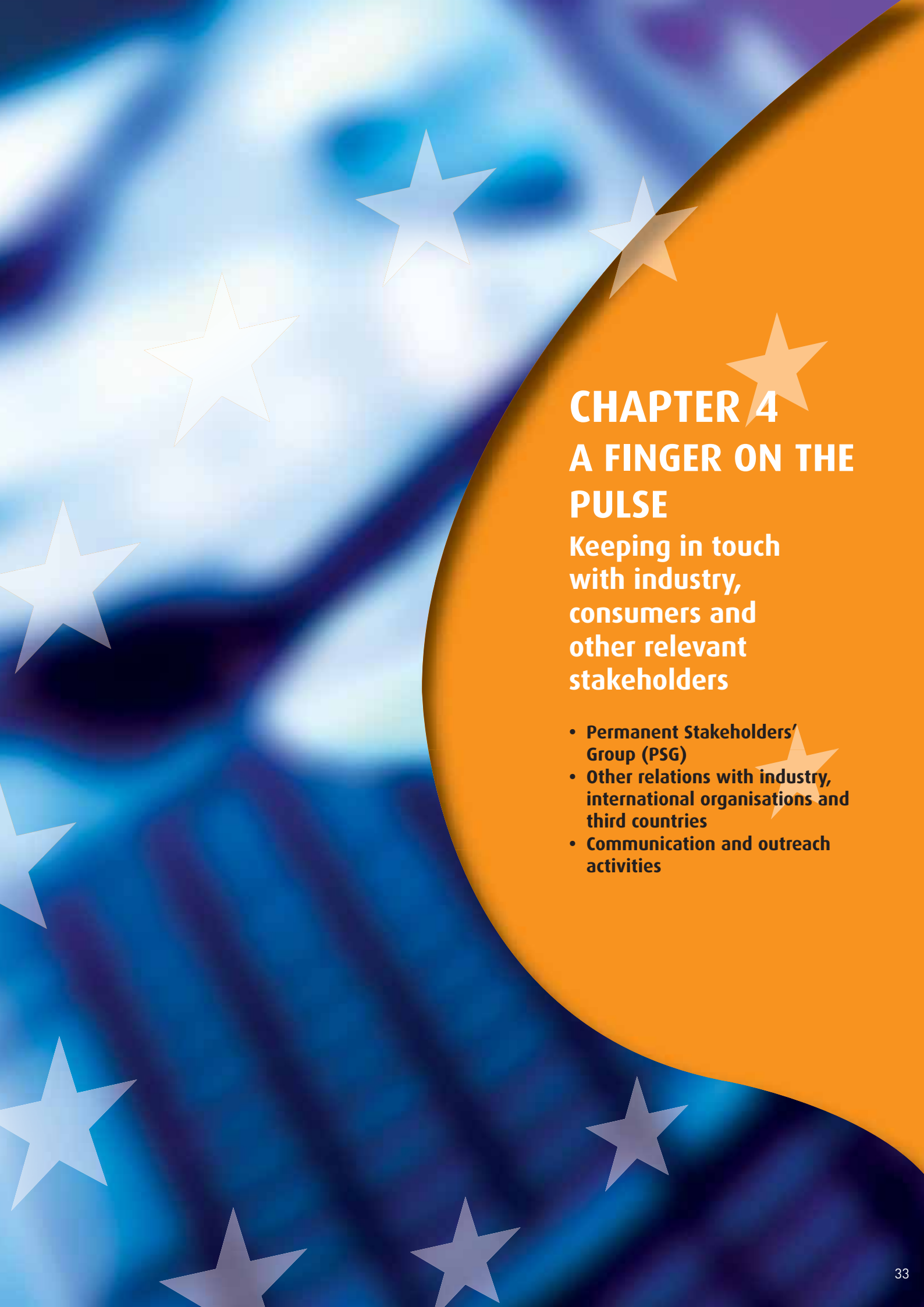
The event attracted more than 40 European experts from all over Europe and provided an opportunity to present ENISA's Risk Management results of 2006.

Highlights of the RA/RM Workshop

- ENISA should play a catalytic role in the field of Risk Management concerning best practice. Similarly ENISA should participate in the dialogue for a balanced regulatory activity within Europe in this field.
- Besides the technical details of Risk Management and Risk Assessment, business must pay more attention to organisational integration for increased profits, by applying more effective methods and simpler procedures.
- ENISA should provide guidance for SMEs based on size considerations and on the level of the required confidentiality of processed information.
- ENISA should research into Risk Management and collect data on Risk Assessment. This will help both non-experts and experts in applying Risk Management/Risk Assessment in their daily businesses.
- In co-operation with other initiatives and relevant bodies, ENISA should participate in the identification of new issues in Risk Management/Risk Assessment for potential European research and development.
- Emerging Risks issues also need to be stressed in ENISA's future initiatives.

Additional information and all the presentations given at the workshop are publicly available on the Risk Management web site:

www.enisa.europa.eu/rmra/events.html



CHAPTER 4

A FINGER ON THE PULSE

Keeping in touch with industry, consumers and other relevant stakeholders

- **Permanent Stakeholders' Group (PSG)**
- **Other relations with industry, international organisations and third countries**
- **Communication and outreach activities**

The Permanent Stakeholders' Group

As electronic communication and information systems are mainly privately owned and developed, industry is a very important stakeholder for ENISA. The Permanent Stakeholders' Group (PSG) maintains a regular dialogue with the private sector, consumer organisations and other relevant stakeholders. The Group comprises 30 independent 'ad personam' appointed experts, each with proven abilities in fields relevant to the PSG mandate and with the capacity to contribute to ENISA's activities. PSG Members represent a broad range of sectors, including the Information and Communication Technology industry, research and academia in the field of Network and Information Security (NIS), as well as representatives from Small and Medium-sized Enterprises (SMEs) and other industrial sectors.

In 2006, PSG Members formally met three times, in February, May and October, in addition to having electronic communication. Main items on the agenda of these meetings included defining the Group's vision and expectations from ENISA for forthcoming years. PSG Members also provided valuable input to the ENISA Work Programme for 2007. They offered views and advice on the drafting of the Terms of Reference for Ad hoc Working Groups established by ENISA and directly to the Executive Director on future challenges, and they provided insights into future and emerging issues in NIS.

The PSG Vision for ENISA

The PSG Vision document (www.enisa.europa.eu/pages/03_03.htm) comprehensively analyses current and future network security threats as well as risks of both a technical and non-technical character. Thus, the PSG Vision is a valuable input to the ENISA Strategy 2007-2011. Moreover, the PSG Vision provided crucial input and advice from NIS stakeholders to ENISA's Executive Director, thus enhancing ENISA's role in its relations with industry and other stakeholders.

As regards the future role of ENISA, the PSG's Vision for ENISA came to the conclusion that the Agency should become:

- The recognised spokesperson for European NIS interests in global co-operation, seeking to develop the relationships needed to advance European interests at the global level and based on a clearly defined role in relation to the European Commission and individual Member States.
- A widely acknowledged European centre of excellence in Network and Information Security, and a trusted expert body whose opinion is sought on key projects within both public and private sectors.
- The major driving force behind the creation, development and dissemination of trusted, secure Information Security technology, thus enabling

consumers in both public and private sectors to use digital technology without undue security risks.

- A recognised consultation centre for European Union bodies and Member States as well as other international standardisation and legislative bodies.

As regards current and foreseen security issues, the PSG undertook a detailed analysis of a number of risks and threats of both a technical (e.g. malware, worms, rootkits, botnets, DDoS, identity theft, attacks on mobile and wireless networks, spam and SPIT) and a non-technical character (such as lack of security awareness, professionalism of cyber criminals, and increased reliance on the Internet and networked resources). Their findings are very valuable and will be utilised in the continuing discussions on ENISA's strategy for the coming years.

The PSG, Management Board and the ENISA Strategy 2008-2011

To elaborate the strategic orientation of future ENISA activities, PSG Members and Members of the Management Board, together with ENISA staff, met for an informal workshop in London (UK) in early June 2006. This was a unique, first joint meeting of two ENISA bodies that have clearly defined, distinct roles within the overall ENISA structure. The Permanent Stakeholders' Group is the source of input and advice to ENISA's Executive Director, while the Members of the Management Board are the decision-making body of ENISA.

The event proved extremely useful both in achieving a common understanding and providing strategic orientation for ENISA. Both groups agreed to continue these informal workshops in the future. The Stakeholders of ENISA agreed to finalise the ENISA Strategy in further discussions during 2007, in order to integrate the findings of the evaluation of the Agency, stipulated by regulation, which is due in early 2007.

For a list of the members of the PSG, see Annex 4.



The joint meeting of the Management Board with the PSG in London.

Other relations with industry, international organisations and third countries

In addition to the baseline relations with industry via the Members of the Permanent Stakeholders' Group, ENISA initiated a number of activities with relevant industrial associations around Europe.

For example, ENISA representatives met with representatives from the Business Software Alliance (BSA), the European Information & Communications Technology Industry Association (EICTA), the European Internet Service Providers Association (EuroISPA), the Association of European Chambers of Commerce and Industry (EUROCHAMBRES), and CENTR, the association of Internet Country Code Top-Level Domain Registries.

In addition, ENISA has an 'open door' policy to all the relevant stakeholder groups and held a number of bilateral discussions with stakeholders at its headquarters in Heraklion. During 2006, ENISA extended relationships with these organisations particularly through questionnaires distributed to the communities they represent. This work will continue in 2007.

The Organisation for the Economic Co-operation and Development (OECD) Working Party on Information

Security and Privacy (WPISP) is the originator of the 'OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security' (www.oecd.org/site/0,2865,en_21571361_36139259_1_1_1_1_1,00.html).

These Guidelines were one of the cornerstones for the creation of ENISA. In May 2006, at the invitation of the OECD WPISP secretariat, ENISA participated for the first time in the WPISP meeting in Seoul (Korea). ENISA introduced its activities, focusing on awareness raising. WPISP members showed great interest in actively involving ENISA in their future activities. In discussions with the European Commission, this has led to ENISA being appointed as an independent representative at the OECD. In October 2006, ENISA was invited again to participate in the OECD WPISP meeting, this time in Budapest (Hungary). Further collaboration with the OECD is expected to continue in 2007.

Finally, in 2006, ENISA met with representatives from third countries, such as China and Japan. In 2007, the Agency will build on these preliminary contacts with the aim of establishing a more structured approach to relations with countries outside the European Union.

During the year, ENISA played host to a number of visiting delegations from Member States, including...



DG Joint Research Centre



On 7 July 2006, a delegation from the newly established Austrian initiative, 'Secure Business Austria', visited ENISA. Pictured from left to right, front: Dr. Louis Marinos (ENISA), Prof. Dr. A Min Tjoa, Dr. Edgar Weippl, Markus Klemen, Dr. Olivier Hance (ENISA), Dr. Alain Esterle (ENISA). back: Tim Mertens and Marco Thorbruegge both of ENISA, Prof. Dimitris Karagiannis.



Senior Expert Louis Marinos of ENISA with Jean-Louis Roule, a representative of CLUSIF (Club de la Sécurité de l'Information Français)

Communication and Outreach Activities

Speaking of the European Agencies, European Commission (EC) President, José Manuel Barroso said:

"The Agencies are our satellites – picking up signals on the ground, processing them and beaming them back and forth. Through their activities, they bring Europe closer to its people and make Europe itself easier to understand, and I consider this of utmost importance."



Public information and knowledge spreading

The foundation for ENISA's outreach principles and policies was laid down in the Communication Strategy, finalised at the end of 2005. The importance the EU attaches to communications has been reinforced repeatedly since then at the highest level. President Barroso has announced his vision of a 'Europe of Results'. Being situated in the Member States, working with concrete matters, communication of the 28 European Agencies' activities is important to clarify the benefits of Europe for its citizens.

It is vitally important that ENISA is able to perform this essential role as a 'switchboard' of information, gathering and disseminating information, and communicating its activities, reports, studies, workshops, events etc. in a coherent, co-ordinated and consistent way. Consequently, staffing in this area has been reinforced with the appointment of a Press and Communications Assistant to support the ENISA Press and Communications Officer.

To gain best practices in communication, further contacts were made with governments, stakeholders and the EU institutions' Press Officers. In particular, closer contacts with DG INFSO, DG Communication, the EUROPA-web server, and a number of other Agencies were established in 2006. This lays the foundation for a network of contacts with media and communication professionals in Network and Information Security (NIS).

The main communication tool for ENISA is its web site. To enhance the web site as a communication channel and to ensure constant and secure management of the web site, at the end of 2006 preparations were made to launch several web positions including a Web Master. Considerable attention was also given to a web project launched in July 2005, for developing the initial

web site (the original ENISA web site was set up and cared for by the European Commission). The first phase of work focused on a 'look and feel' redesign. The new 'europa.eu' web domain was launched in conjunction with Europe Day (9 May) and the Agency's new web site flew soon after. To the same end, a web editorial policy was drafted, to clarify and codify the communication/publication practices and principles that were applied. The web site is continuously being improved with new content, sections and updates. Fact sheets on ENISA have been published, along with other features, photos, news of NIS and ENISA events, links and other NIS material in Europe. All in all, these actions to enhance the web site as a communication channel are helping make the site a 'hub' for NIS information in Europe.



Screenshot of the new web site design, displaying dynamism and transformation in the Information Society, with aspects of everyday life – emphasising the need for Information Security to be paramount in all sectors of society and its role in supporting the economy of a modern society.

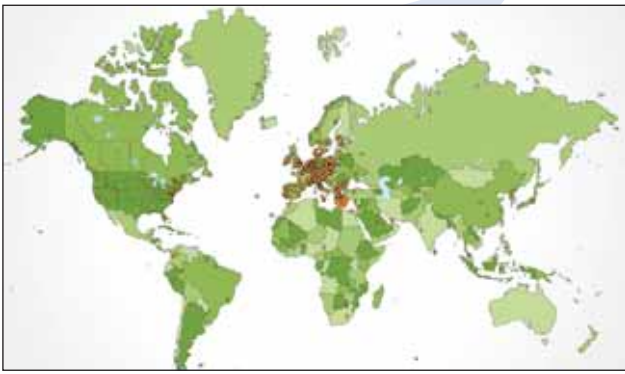
ENISA also reaches out to the general public through multipliers of information, such as the media, and through the assistance of the National Liaison Officers' (NLOs') stakeholders' media, press, communication and information managers at EU and national level, as well as the PSG. The media is targeted with press releases published on the web and then sent out by e-mail to a list of media contacts. During 2006, ENISA produced around 30 press releases, similar to other EU Agencies. Other news items of interest to those involved in NIS or who follow the activities of the Agency are regularly posted on the web site too.



Ulf Bergström, Press and Communications Officer



Sarah Capogrossi, Press and Communications Assistant



Sample of the geographic distribution of web site visitors, portraying visitors from all continents, and with a clear outreach concentration to Europe.

New media register software was purchased to develop the analysis of the web as a communication tool. The Agency used two different software tools to analyse statistics about visitors to the web site to help it develop its content and structure it in a logical and effective manner.

Considerable time was also dedicated to preparing and launching procurements in 2006, for example, to further develop the web site, for publications, ENISA marketing and brand building material and future media monitoring services.

Media, interviews and articles



The Executive Director during a television interview

ENISA and other key figures in the Agency figured in the media numerous times during 2006. Television and radio appearances by the Executive Director and others occurred on several occasions both in Greece and elsewhere. Thanks to media alerts, press cuttings have been identified and archived from NIS, European, national and regional press. The media list of contacts includes European journalists, NIS/ICT, general and other relevant media. In addition, the database of Press Officers in EU Representations and other Agencies was updated and extended. Preparations for Media Training for staff early in 2007 were made, to increase the understanding of media relations and the need for communicating our activities. Ever closer relations with DG INFSO's communication team, the DG Joint Research

Centre's European Media Monitoring, the European Centre for Journalism and the EUROPA server staff were also developed.

ENISA Quarterly

In 2005, ENISA launched the ENISA Quarterly magazine, as a way to reach information security professionals in Europe (www.enisa.europa.eu/pages/02_02.htm). In order to professionalise its visual identity and branding, a logo was developed for the publication. Using the new web site platform, additional information on the scope of the magazine, timelines and style guidelines for contributors were made readily accessible in a new dedicated section of the web site.



From its inception in 2005, the ENISA Quarterly quickly established itself as one of the leading independent, EU information security publications in Europe. It has attracted high quality professional contributions from across the European Union and the USA. At the end of 2006, there were about 4000 direct electronic subscribers from all over the world, from locations as diverse as the Vatican, Singapore and Venezuela. ENISA also contributed to other Information Security publications throughout the year.



Conferences and Workshops



The Executive Director speaking at GovCert in The Hague (above), and during the Finnish EU presidency, at the i2010 conference in Helsinki (below).

During 2006, ENISA participated in or co-organised about 40 events and speaking engagements, and staff attended numerous conferences to share knowledge and for networking. In this way, ENISA contributed to the European NIS discussion and took the Agency's message and promoted its achievements to an audience of approximately 7000 conference attendees.



For the second consecutive year, ENISA successfully co-organised its flagship conference, ISSE 2006 (Information Security Solutions Europe). This year the conference took place in Rome. ISSE 2006 attracted about 350 leading NIS experts, academics, business, industry and government players from over 35 countries all over the world. At the venue, delegates participated in around 70 workshops, debates and seminars, discussed opportunities and challenges, and exchanged examples of best practice. The conference was co-organised in close co-operation with key organisations such as ISCOM, TeleTrust and eema, (the independent European association for e-business), underlining ENISA's role in bridging between governments and industry in the setting up of the conference.

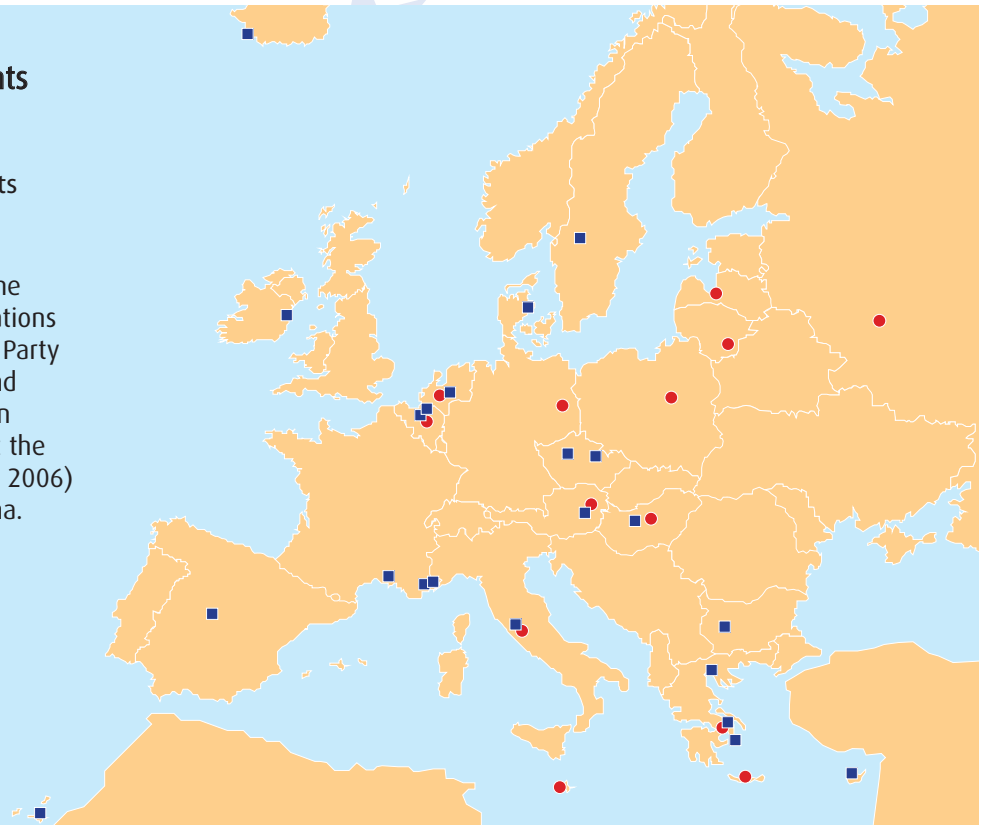
Internal Communication

Good internal communication underpins coherent and professional external communication. During 2006, ENISA therefore took steps to increase and improve its internal communication. With the arrival of the new Press and Communications Assistant and other measures, more resources were dedicated to internal communication in the Agency. A new internal newsletter called 'Inside ENISA' is now being produced on a monthly basis, and staff are encouraged to participate in its content, as well as in the weekly internal staff meetings.

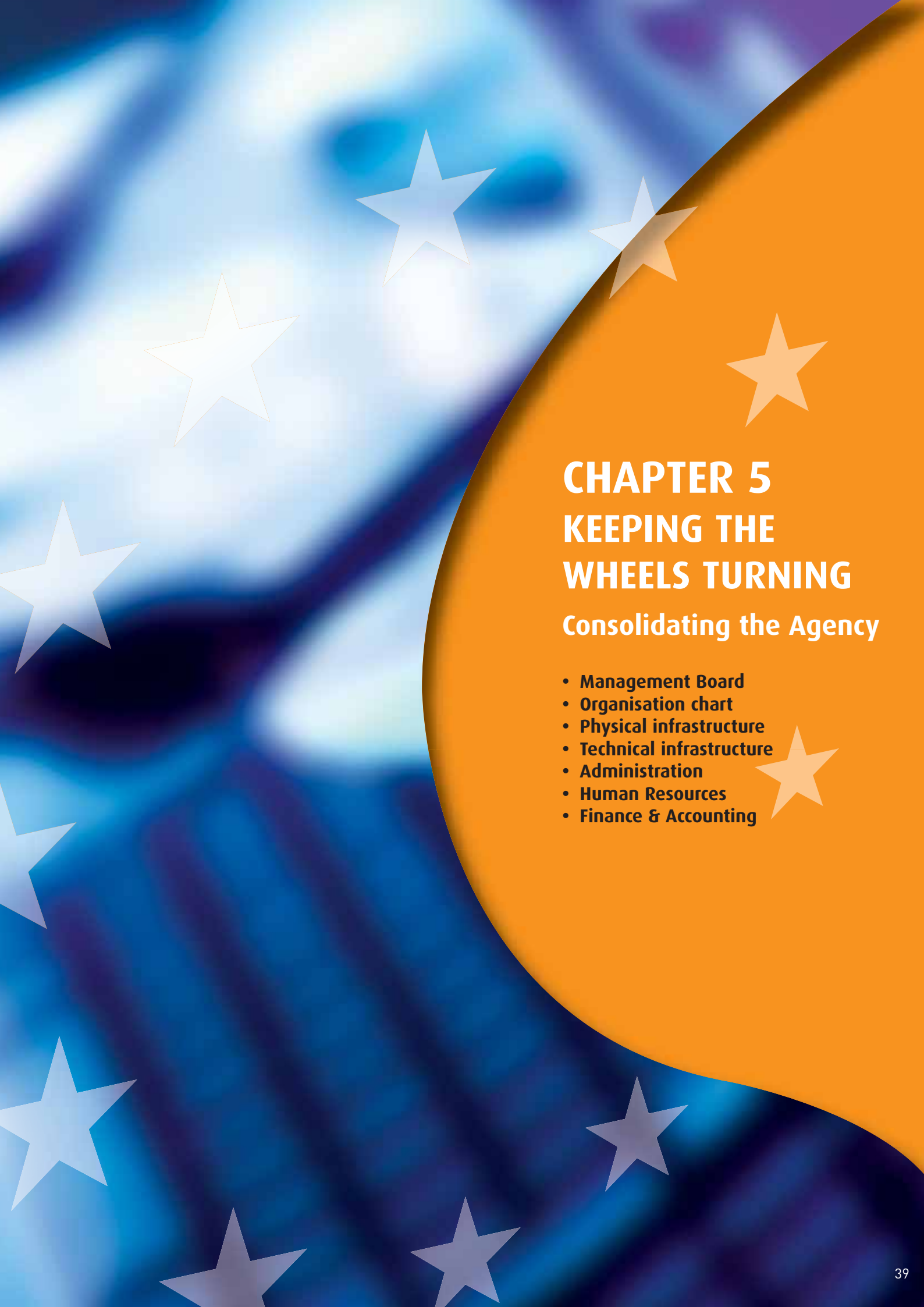
ENISA events and speaking engagements

- ENISA events
- Speaking engagements

In addition, members of the ENISA staff made presentations to the 20th OECD Working Party on Information Security and Privacy (WPISP) meeting in Seoul, South Korea, and at the Asian Pacific CERT (APCERT 2006) conference in Beijing, China.



During 2006, ENISA participated in or co-ordinated about 40 events and speaking engagements throughout Europe and further afield. In addition, staff attended numerous conferences and other events to fulfil ENISA's role in gathering and disseminating information about Network and Information Security.



CHAPTER 5

KEEPING THE WHEELS TURNING

Consolidating the Agency

- **Management Board**
- **Organisation chart**
- **Physical infrastructure**
- **Technical infrastructure**
- **Administration**
- **Human Resources**
- **Finance & Accounting**

Consolidating the Agency

Since its creation, ENISA has developed fast. 2006 was dominated by the appointment and integration of new staff and intense efforts to establish and develop the infrastructure of the Agency. ENISA's premises were extended as the Agency moved into additional offices in the newly constructed second wing of the building, and there was significant progress in IT, including the introduction of a new domain.



2004

March 2004

Founding regulation 460/2004 for ENISA, which governs the mission of ENISA

6 October 2004

The Executive Director is nominated by the ENISA Management Board and makes a statement before the European Parliament

2005

1 May 2005

ENISA gains financial independence

1 September 2005

ENISA begins operations from new headquarters in Crete

2006

2 May 2006

The European Court of Justice confirms the legal basis of ENISA

31 May 2006

Communication Strategy of the Commission on Information Security envisages an increased role for ENISA in the field of data collection to handle security incidents and measured levels of consumer confidence from all over Europe by developing a trusted partnership with Member States and stakeholders, and to examine the feasibility of a multilingual information sharing and alert system.

2 June 2006

Permanent Stakeholders' Group (PSG) produces its Vision for ENISA, together with future risk and threats analysis

16 June 2006

First informal PSG/Management Board Strategy workshop in London

November 2006

Visit of the European Commission's evaluation panel as part of their scheduled mid-term review of ENISA. Their report was delivered to the Commission in January 2007.

Management Board



From the left: Vice Chairman Ferenc Suba, Chairperson Kristiina Pietikäinen and Executive Director Andrea Pirotti in Crete, March 2006.



The Management Board

In brief, the Management Board's task is to define the general strategic orientation for the operation of ENISA, to ensure the consistency of the Agency's work with activities conducted by Member States as well as at Community level. The Management Board also approves the ENISA Work Programme, ensuring it 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. It also establishes and oversees the budget.

A key pillar of ENISA, along with the Executive Director and the Permanent Stakeholders' Group, the Management Board includes one representative of each EU Member State, and three representatives appointed by the European Commission. There are also three members, proposed by the Commission and appointed by the Council, without the right to vote, who represent respectively:

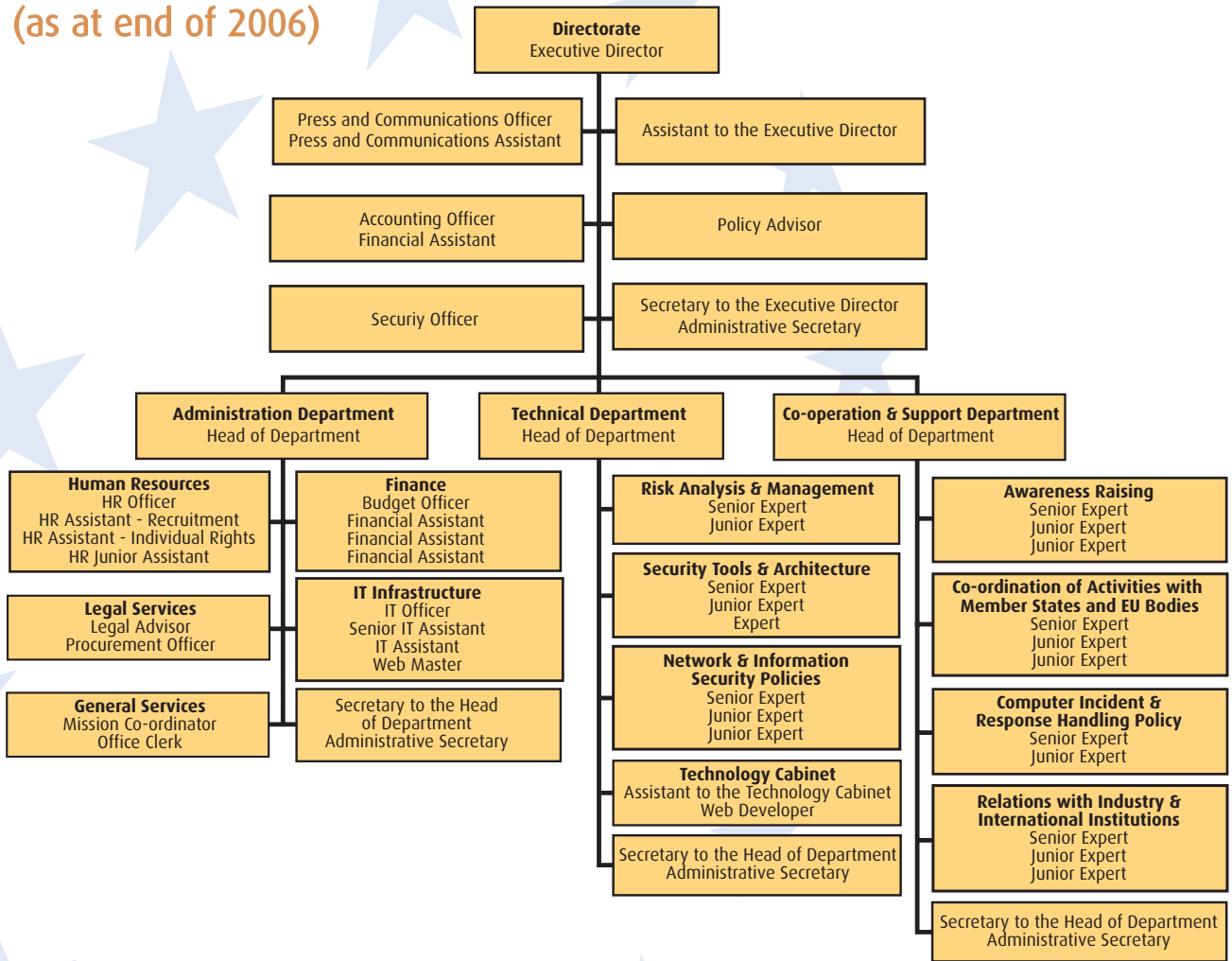
- the information and communication technologies industry
- consumer groups
- academic experts in network and information security.

Finally, there are also three observers from the EEA Member States, Lichtenstein, Norway and Iceland.

In 2006, the full Management Board met twice: in Crete and in Helsinki. Numerous bilateral contacts and other discussions between the Chair and the Executive Director also took place. The preparation and subsequent adoption of the Work Programme for 2007 and the (amended 2006) and 2007 budgets dominated activities. Together with the PSG, the Management Board also made significant contributions to discussions concerning the ENISA Strategy. Some key Management Board decisions were taken, for example, on public access to ENISA documents, and the related topic of transparency and confidentiality rules, as well as proceeding with the Request Handling Procedures. The Management Board also gave direction on the National Liaison Officers network, and future ENISA Working Groups, amending the internal rules for the Working Groups. The Management Board contributed to the Terms of Reference for the EC's mid-term evaluation of the Agency. All minutes and decisions by the Management Board are available on the ENISA web site.

For a list of members of the Management Board, see Annex 3.

Organisation Chart (as at end of 2006)



Physical Infrastructure

Following a request for additional accommodation, made to the Board of Directors of FORTH (the Foundation of Research and Technology) as the host institute, in December 2006 ENISA rented offices in the newly constructed second wing of the building.

The Agency's request was welcomed and accepted by FORTH. Given the scarcity of free office space, this once again demonstrated FORTH's continuing support for ENISA. During a short ceremonial meeting for the signature of a contact between ENISA and FORTH, Executive Director Andrea Pirotti expressed appreciation for FORTH's ongoing support of ENISA and welcomed the possibility of further opportunities for co-operation between the two organisations.

The additional office space will provide accommodation for new staff members, the Technological Cabinet of ENISA, meeting rooms and teaching rooms for staff training.

Technical Infrastructure

Following the start-up phase of the agency, IT efforts have been concentrated on fine-tuning the ICT infrastructure, especially with regard to security, with the installation of industry-standard firewall and gateway scanning solutions to protect ENISA from the ever growing number of threats. In addition, comprehensive data backup solutions have been installed.

In the middle of 2006, the new domain, europa.eu, went 'live' for all EU institutions, and ENISA was one of the first to start to use it, switching over smoothly within a few days of the launch date. Soon after this, the new ENISA web site went live, giving ENISA a new face to the outside world. Once again the transition went smoothly.



A video conferencing service has also been set up, reducing travel expenditure and increasing efficiency while allowing liaison with many players in Europe.

Planning for the installation of a Listserv service for automatic distribution of ENISA press releases and the ENISA Quarterly, as well as an Intranet for better internal communication, was completed. Both projects are planned for launch early in 2007.



Administration



organisation of events and 4 contracts for the provision of various services (e.g. rental) were prepared. In addition, in 2006, 31 restricted procedures and 2 open procedures were launched.



General Administration

In addition to day-to-day responsibilities, in 2006 ENISA's Administration dealt successfully with two audits by the Court of Auditors and one by the Internal Audit Service of the European Commission.

General Services

Highlights of 2006 for General Services included dealing with about 300 missions, managing office equipment during the move to the new wing that took place in December 2006 and, in co-operation with Human Resources, the procurement of ergonomic chairs in line with guidelines about the working environment.

Legal Services

As the Agency gathered speed during the year, 25 service contracts (e.g. consultancy services) or supply contracts (e.g. ergonomic chairs) covered by procurement rules, 7 co-operation agreements for the

In addition to its regular activities in relation to contracts, procurement and other routine legal matters in 2006, the Legal Unit helped conclude several Co-operation Agreements with regard to the organisation of events such as conferences and training. The Legal Unit led ENISA's responses to Requests for assistance from the European Commission on eIDM and the Czech Republic. Other activities included co-ordinating the Working Group on Regulatory Aspects of Network and Information Security (WG-RANIS), which delivered its final report as planned at the end of 2006. Presentations were also made at several conferences and events, and 4 book chapters and an article in an academic journal were published.



Human Resources

Recruitment

In 2006 the Human Resources (HR) Section focused its activities on the recruitment of staff in order to reach the total number of 44 'Temporary Agents' and 12 'Contract Agents' positions. In view of the Agency's tasks, most of the statutory positions were at administrators' level. A total of 892 applications were received for 18 posts advertised during 2006. Candidates from all over Europe showed their interest in working for ENISA, not only in the operational positions, but also in the administrative posts. The majority of the candidates were aged between 30 and 40 years old, while the female applicants were slightly more numerous than the male candidates.

All recruitment procedures were carried out in accordance with the EU Staff Regulations, strictly respecting the principles of transparency, objectivity and equal treatment. The Agency promoted the equal opportunity policy and considered all applicants without any distinction on the grounds of age, race, political, philosophical or religious conviction, gender or sexual orientation, disabilities, marital status or family situation.

Further to the successful recruitment process, 15 new staff members were appointed in 2006. With the support of the HR Section, the settlement and relocation of these new colleagues and their families in a new country and new working environment went smoothly.

In addition to the recruitment of statutory staff, HR finalised the selection of National Experts seconded to the operational departments. Thanks to excellent co-operation with the national administrations, the Agency will now benefit from the high level of professional knowledge and experience of these experts.

In 2006 ENISA launched its first traineeship programme which offered a 5-month period of 'work experience in a dynamic international environment for young university graduates in the field of network and information security'. This new programme aims to provide an understanding of the Agency's objectives and activities, enabling trainees to acquire practical knowledge and experience of the day-to-day work of the organisation. The scheme represents a contribution to the integration of all citizens in Europe. The Agency could also benefit from the fresh point of view and up-to-date academic knowledge which these trainees bring. ENISA welcomed its first trainee from Latvia in November 2006.

Agency's Staff Members (as at 31 December 2006)

Following successful selection procedures, by the end of 2006 the Agency's staff comprised 44 staff members, 1 trainee and 1 seconded national expert.

ENISA staffing at 31 December 2006 – Some key facts

- **Gender:**
The division between males and females remains balanced, as in 2005, with a slight majority of male staff members.
- **Nationality:**
14 out of 25 nationalities of the European Union are represented, with a high percentage from the 'old' Member States. 14% of the total staff has dual nationality.
- **Age:**
The majority of staff continues to be aged between 31 and 40 years.
- **Function group:**
the majority of staff members occupy posts at administrator's level.

Training

One of the main activities of the HR Section in 2006 was the management of training, aimed at achieving and maintaining the highest quality standards and reflecting the Agency's core values of excellence, professionalism and service. Courses were introduced in Greek, French and German at beginners' level and in English at advanced level, and training in teambuilding and individual professional development was provided.

Health & Safety at Work

In 2006 HR launched the Agency's first health and safety programme. Training in health and safety at work was provided to the staff. The successful selection of a medical adviser enabled the Agency to offer its staff a regular consultation service on medical issues on its premises.

For a full report of the HR Section's activities in 2006 see Annex 7.

Finance and Accounting

The Finance and Accounting Sections carry out functions associated with the management of the Agency's Budget, the preparation of the Financial Statements in line with its Financial Regulation and the Audits conducted by the Court of Auditors.

Specific activities of the two sections include:

- Implementation of the approved budget
- Establishment of Internal Controls, as appropriate, in order to address possible financial risks
- Reporting on the Annual Budget, including budget status reports and providing an analysis of key aspects
- Budget revision and execution of budgetary transfers
- Planning of the Budget 2007 and presentation to the Management Board and the Budgetary Authority for adoption, as appropriate
- Ensuring adherence to the accounting rules
- Validation of the new systems put in place and continuous checking of existing ones
- Keeping the Accounts
- Preparation of the Annual Financial Statements
- Preparation of the Reporting Package for consolidation purposes with the European Commission's Accounts
- Regular financial reporting to the European Commission and the Court of Auditors

Budget Execution

The overall Budget 2006 was committed at a rate of 90%, with payments reaching a level of 77% of the total appropriations managed. This is a positive result, given that 2006 was the first year of full activity for the Agency.

The Agency's budget is divided into three parts or 'titles':

Title 1 – Staff expenditure: Staff expenditure was as foreseen, with 94% of appropriations committed at the end of the year. The respective rate of payments is 88%. The management of Title 1 funds improved when compared with 2005 (the first year of ENISA operations), where the respective rates demonstrated commitments of 74% and payments of 63% on appropriations.

Title 2 – Administrative expenditure (Functioning of the Agency): The funds allocated to administrative expenditure were used as planned, with 91% of appropriations being committed by the end of the year, and 76% paid. The respective figures on Budget 2005 execution were 59% and 18%.

Title 3 – Operating expenditure: 83% of the funds allocated to the operating expenditure of the Agency, i.e. the funds directed to the core business of the Agency according to the 2006 Work Programme, were committed, with the total rate of paid appropriations reaching 54%.



Financial Reporting

According to Article 82 of the Financial Regulation, the Agency's Accounting Officer sent to the Commission's Accounting Officer the Provisional Accounts, together with the Report on Budgetary and Financial Management. Subsequently the Commission sent the Provisional Accounts to the Court of Auditors.

Based on the observations of the Court of Auditors, the Executive Director sent the Final Accounts to the Management Board which gave its opinion on them. Finally the Executive Director submitted Final Accounts along with the opinion of the Management Board to the Commission, the Budgetary Authority and the Court of Auditors.

The Final Annual Accounts will be published in the Official Journal of the European Communities together with the statement of assurance which will be given by the Court of Auditors.

The Financial Statements included in the Annual Accounts are the following:

Balance Sheet

	31.12.2006	31.12.2005
I. Non Current Assets	344.932	344.168
Intangible fixed assets	32.564	11.971
Tangible fixed assets	312.368	332.197
II. Current Assets	2.575.036	2.523.326
Short-term receivables	55.843	13.276
Cash and cash equivalents	2.519.193	2.510.050
Total Assets	2.919.968	2.867.494
III. Non Current Liabilities		
IV. Current Liabilities	2.289.543	1.769.242
EC pre-financing received	1.124.138	149.144
EC interest payable	88.829	31.143
Accounts payable	432.531	756.833
Accrued liabilities	578.173	787.295
Provisions	65.872	44.827
Total Liabilities	2.289.543	1.769.242
V. Net Assets	630.425	1.098.252
Accumulated result	630.425	1.098.252
Total Net Assets	630.425	1.098.252

Economic Out-turn Account

	2006	2005
Revenue from the Community Subsidy	5.475.862	4.250.856
Other revenue	12.309	0
Total Operating Revenue	5.488.171	4.250.856
Administrative expenses	-4.717.893	-2.634.169
Staff expenses	-3.100.024	-1.039.738
Fixed asset related expenses	-103.279	-31.273
Other administrative expenses	-1.514.590	-1.563.158
Operational expenses	-1.236.173	-517.973
Total Operating Expenses	-5.954.066	-3.152.143
Surplus/(deficit) from operating activities	-465.895	1.098.713
Financial expenses	-1.932	-460
Surplus/(deficit) from ordinary activities	-467.827	1.098.252
Economic Result for the Year	-467.827	1.098.252

Cash Flow Statement

	2006	2005
Surplus/(deficit) from ordinary activities	-467.827	1.098.252
Operating activities		
Amortisation (intangible fixed assets)	9.392	2.257
Depreciation (tangible fixed assets)	93.887	29.016
Increase in short term receivables	-42.566	-13.276
Decrease in accounts payable	-606.436	1.588.024
Increase in liabilities to consolidated entities	1.126.736	181.217
Net cash flow from operating activities	113.186	2.885.491
Cash flows from investing activities		
Purchase of tangible and intangible fixed assets	-104.043	-375.441
Net cash flow from investing activities	-104.043	-375.441
Net increase in cash and cash equivalents	9.143	2.510.050
Cash at the beginning of the period	2.510.050	0
Cash at the end of the period	2.519.193	2.510.050

Statement of Changes in Capital

	Reserves	Accumulated Surplus/Deficit	Economic result of the year	Capital
Balance as of 1 January 2006	0	0	1.098.252	1.098.252
Allocation of the Economic Result of Previous Year		1.098.252	-1.098.252	0
Economic result of the year			-467.827	-467.827
Balance as of 31 December 2006	0	1.098.252	-467.827	630.425



ANNEXES

- **Glossary**
- **ENISA 2006 Work Programme Excerpts**
- **Management Board members**
- **Permanent Stakeholders' Group (PSG) members**
- **Ad hoc Working Group members**
- **National Liaison Officers**
- **Human Resources**

Annex 1 Glossary

CERT	Computer Emergency Response Teams. 'CERT' is an organisation 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 preventative services such as alerting, advisory and security management. Therefore, the term 'CERT' was not considered to be sufficient. As a result, the new term 'CSIRT' was established at the end of the '90s. Currently, 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 <i>not</i> included in the list of posts appended to the section of the budget relating to each EU institution (see Temporary Agent)
DG INFSO	Directorate General for Information Society
DIGIT	Directorate General for Informatics
eIDM	Electronic IDentity Management
FIRST	Forum of Incident Response and Security Teams – a global CERT organisation
FORTH	Foundation for Research and Technology - Hellas
ICT	Information and Communication Technology
NIS	Network and Information Security
NLO	National Liaison Officer
PSG	Permanent Stakeholders' Group of ENISA
RIPE	Réseaux IP Européens
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
TRANSITS	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

ENISA 2006 Work Programme Excerpts

The following tasks were stipulated in the Work Programme for 2006 and have been delivered by the Agency:

Work Package (WP) Recruitment and Financing

Deliverables	Budget
Finalised recruitment of temporary staff	not applicable
Implementation of career development and training	not applicable
Budget execution and preparation of the accounts	not applicable
Financial reports; budget and accounting	not applicable

WP Equipment and Premises including Information and Communication Systems

Deliverables	Budget
Fully functional Agency information system	not applicable
Implementation of office and building arrangements	not applicable
Implementation of security policies	not applicable

WP Operational Tasks: General

'Communication Implementation Plan', improvement of the ENISA web site, high level European conference, smaller events, workshops, identifying developments in NIS to reach out with ENISA's findings to a broad audience, a newsletter in electronic form, important technical and policy developments, responding to requests for advice and assistance from the European Parliament, the European Commission or competent bodies in the Member States.

Deliverables
Plan for building up 'library'.
Communication Implementation Plan 2006
Updated web site
Draft communication action plan 2007
Conference
4-5 Workshops
4 issues of the newsletter
Response to requests

WP Operational Tasks: Technical – Risk Management

Deliverables	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.	102,000
Information package for SMEs.	

WP Technical and Procedural – Security Policies

Deliverables	Budget €
Knowledgebase of Best Practices: data, figures, advice, knowledge accessible via an IT tool through the Internet. The SME-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.	102,000
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.	
Begin an assessment of the need to facilitate the functioning and accessibility of accreditation and certification schemes.	
Plan how to create a common language between Member States to identify the levels of security that can be met by various authentication methods.	

WP Network and Information Security Technologies

Deliverables	Budget €
Analysis of the major technical developments in the field of network and information security technologies in relation to standardisation with a view to producing report on information gathered from technical fora, consisting partially in updating already existing reports and publications (e.g. CEN, ETSI)	102,000
Presence of ENISA in various fora. Establishment of a network of contacts in the technical, development, standardisation and research community in order for ENISA to contribute to the promotion of research activities in the area of NIS	

WP Operational Tasks: Co-operation and Support – Computer Incident and Response Handling

Deliverables	Budget €
Written report on step-by-step approach on how to set up a CERT or similar facilities, including examples	102,000
Excerpt of roadmap in itemised form allowing an easy application of the roadmap in practice	
Written plan on how co-operation between CERTs or similar facilities can be facilitated by relevant stakeholders	

WP Awareness Raising

Deliverables	Budget €
Written report on Member States' best practices in awareness raising for particular target groups, including examples	177,000
Written report on how awareness raising with various target groups can be facilitated within Europe	
CD-ROM with information on best practices customised to various target groups, including examples	
Written plan on how the customised information packages could be disseminated within Europe	

WP Relations with EU Bodies and Member States

Deliverables	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	117,000
Document listing relevant EU institutions and bodies in Europe, including name of authority, area of responsibility and contact information	
Country pages on ENISA web site, including national authorities, other bodies and organisations, activities and events, developments and best practices/case studies (update)	
Well established and functioning network of national liaison officers ensuring rapid information exchange between Member States and ENISA	

WP Relations with Industry and International Institutions

Deliverables	Budget €
Well established and functioning PSG ensuring adequate advice on Work Programme and establishment of Working Groups to the Executive Director of ENISA	42,000
Well established and functioning Working Groups ensuring independent advice on scientific matters to the Executive Director of ENISA	
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	

Annex 3 Members of the Management Board

European Commission representatives

Representative	Alternate
Fabio COLASANTI Director General – Information Society and Media DG	Michael NIEBEL Head of Unit, Information Society and Media DG – ‘Internet: Network and Information Security’
Francisco GARCIA MORÁN Director General – Informatics DG	Marcel JORTAY Head of Unit, Informatics DG – ‘Telecommunications and Networks’
Gregory PAULGER Director, Information Society and Media DG – ‘Audiovisual, Media, Internet’	Fabio MARINI Acting Head of Unit, Fight against Economic, Financial and Cyber Crime, DG Justice, Liberty and Security

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 Director of the Commissioner’s Office for the Control of the Telecommunications and Postal Services	Director Antonis ANTONIADES Senior Officer of the Commissioner’s Office for the Control of the Telecommunications and Postal Services
Czech Republic	David KOTRIS Acting Deputy Minister of the eGovernment Section, Ministry of Informatics of the Czech Republic	Vit LIDINSKY PAIS Conception and Co-ordination Department, Ministry of Informatics of the Czech Republic
Denmark	Flemming FABER Head of the IT-Security 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) Deputy Director-General, Communications Department	Juhapekka RISTOLA Ministerial Adviser, E-Commerce and Data Security, Ministry of Transport and Communications, Finland

Member States representatives (cont.)

Member State	Representative	Alternate
France	Patrick PAILLOUX Central Director of Information Systems' Security, Office of Prime Minister/General Secretariat of National Defence/DCSSI	Isabelle VALENTINI Central Directorate of Information Systems' Security, Office of Prime Minister/General Secretariat of National Defence/DCSSI
Germany	Christoph VERENKOTTE Head of Division, IT-Security Policy, Federal Ministry of the Interior	Anja DIEK IT-Directorate, IT-Security Policy, Federal Ministry of the Interior
Greece	Nikolaos VLAISOPOULOS Hellenic Telecommunications and Post Commission	Constantin STEPHANIDIS Director, Institute of Computer Science, Foundation of Research and Technology (FORTH)
Hungary	Ferenc SUBA (VICE-CHAIR OF ENISA MANAGEMENT BOARD) General Manager of CERT-Hungary	András GERENCSE 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 International Issues Division, Department of Communications, Ministry of Transport
Lithuania	Valdemaras SALAUŠKAS 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 Ministère de l'Économie et du Commerce extérieur, Direction des Communications CASES
Malta	Joseph N. TABONE Chairman, Malta Communications Authority	Colin CAMILLERI Chief Technical Officer, Malta Communications Authority
The Netherlands	Edgar R. DE LANGE Senior Policy Adviser, Ministry of Economic Affairs Director-General for Telecommunications and Post	Ronald M. VAN DER LUIT Senior Policy Adviser, Ministry of Economic Affairs
Poland	Krzysztof SILICKI Technical Director, Research and Academic Computer Network	Edward SELIGA Ministry of Interior and Administration
Portugal	Pedro Manuel BARBOSA VEIGA Presidente da Fundação para a Computação Científica Nacional (FCCN)	Manuel Filipe PEDROSA DE BARROS Director de Tecnologias e Equipamentos da Autoridade Nacional das Comunicações (ANACOM)

Member States representatives (cont.)

Member State	Representative	Alternate
Slovakia	Peter BIRO Information Society Division, Ministry of Finance	Ján HOCHMANN Information Society Division, Ministry of Finance
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 Näringsdepartementet	Pernilla SKANTZE Division for IT, Research and Development, Ministry of Industry, Employment and Communications
United Kingdom	Geoff SMITH Head of Information Security Policy, Information Security Policy Team	Peter BURNETT National Infrastructure Security Co-ordination 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 Secretary, Statistical Office of the Republic of Slovenia

EEA-country representatives (Observers)

Iceland	Björn GEIRSSON Legal Counsel, 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

Annex 4 Members of the Permanent Stakeholders' Group

Name	Nationality	Organisation
Jaap Akkerhuis	Dutch	NLnetLabs
Charles Brookson	British	Department of Trade and Industry, UK
Giuseppe Carducci Artensio	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
Wim Hafkamp	Dutch	Rabobank
Christian Hauser	German	University of Stuttgart
Urho Ilmonen	Finnish	Nokia
Andrzej Kaczmarek	Polish	Polish Data Protection Authority
Paul King	British	Cisco
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
Vincent Tilman	Belgian	EUROCHAMBRES
Giuseppe Verrini	Italian	Adobe Systems

Annex 5 Members of the ENISA Ad Hoc Working Groups

Ad hoc Working Group on CERTs

Gilles ANDRE, SGDN/DCSSI, FR
Henk BRONK, NL
Mirosław 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 Technical and Policy Aspects of Risk Assessment and Risk Management

Giuseppe CARDUCCI ARTENISIO, IT
Alain DE GREVE, Fortis Bank, BE
Aljosa PASIC, Athos, ES
Jeremy WARD, Symantec, UK
Serge LEBEL, Premier Ministre, Dir. Centrale de la Sécurité des Systèmes d'information, FR
Ingrid SCHAUMULLER-BICHL, Univ.-Doz. University of Applied Sciences, Hagenberg, AT
Juhani SILLANPAA, Ministry of Finance, SF
Marcel SPRUIT, Haagse Hogeschool, NL
Lydia TSINTSIFA, Federal Office for Information Security, DE

Ad hoc Working Group on Regulatory Aspects of Network and Information Security (WG-RANIS)

David MARSH (Chair)
Antonio AMENDOLA (Vice-Chair)
Patrick VAN EECKE
Stefan ENGEL-FLECHSIG
Paivi HAUTAMAKI
Christopher KUNER

Annex 6 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 LIDINSKY
Denmark	Charlotte JACOBY
Estonia	Toomas VIIRA
Finland	Mari HERRANEN
France	Isabelle VALENTINI
Germany	Anja DIEK
Greece	Georgios DROSSOS
Hungary	Ferenc SUBA
Iceland	Björn GEIRSSON
Ireland	Aiden RYAN
Italy	Daniele PERUCCHINI
Latvia	Ingrida GAILUME
Liechtenstein	Kurt BUEHLER
Lithuania	Tomas LAMANAUSKAS
Luxembourg	Pascal STEICHEN
Malta	Joanna BORG
Norway	Heidi KARLSEN
Poland	Mirosław MAJ
Portugal	Paulo FERREIRA
Slovakia	Rastislav MACHEL
Slovenia	Radovan PAJNTAR
Spain	Salvador SORIANO MALDONADO
Sweden	Fredrik SAND
The Netherlands	Edgar DE LANGE
United Kingdom	Geoff SMITH

Annex 7 Human Resources

Recruitment

Recruitment is a key element in a growing organisation. In 2006 the Human Resources (HR) Section invested a considerable amount of time and resources in recruitment in order to fill the total number of 56 statutory positions anticipated in the Agency's budget. In comparison with 2005, the establishment plan for 2006 increased by 15% including 6 additional posts to make a total of 44 temporary agents (TA). In addition, 12 contract agents' (CA) positions not provided for by the establishment plan were created for 'non core tasks' to support the directorate, the administration and the technical department.

The target for 2006 of 56 statutory posts was distributed as follows:

Department	Total Temporary Agents	Total Contract Agents	Total
Directorate	7	3	10
Administration	13	6	19
Technical Department	10	3	13
Co-operation & Support Dept.	14	0	14
TOTAL STAFF	44	12	56

In view of the Agency's tasks, the majority of the positions was allocated to administrators' functions, mainly concentrated in the operational departments as demonstrated in the table below:

Department	Administrator (AD)	%	Assistant (AST)	%	Total
Directorate	5	17	5	18.5	10
Administration	5	17	14	52	19
Technical Department	8	28	5	18.5	13
Co-operation & Support Dept.	11	38	3	11	14
TOTAL STAFF	29	100	27	100	56

The HR Section carried out a total of 18 recruitment procedures for 'Temporary Agents' and 'Contract Agents'.

Recruitment procedures

The method of recruitment follows the rules described in the Staff Regulations of Officials of the European Communities and the Conditions of Employment of Other Servants of the European Communities. Following the publication of a position on the ENISA website, applicants are requested to send their CVs, application forms and covering letters explaining their motivation. A Selection Board is drawn up for each position, composed of three members appointed by the Executive Director and representing the Agency's administration and operational departments. When necessary, external experts from other EU organisations are invited to join the Selection Boards.

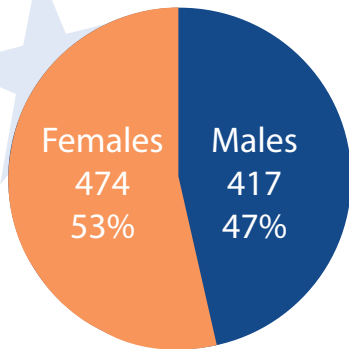
After the screening of the applications, the most eligible candidates are interviewed and tested on their knowledge of the EU and their specific field of interest. The most successful interviewees are put on the list of suitable applicants for the appointing authority who may hold a further interview to assess the candidates' suitability for the advertised position and the Agency's environment. Although this is quite a time-consuming process, it enables the Agency to select the best qualified candidates by ensuring the respect of the basic principles of transparency, objectivity and equal treatment. In all its recruitment procedures, ENISA applies the equal opportunity policy and considers the candidates without any distinction on the grounds of age, race, political, philosophical or religious conviction, gender or sexual orientation, and regardless of disabilities, marital status or family situation.

Including selection procedures for all statutory staff (TA and CA), the HR Section handled a total of 892 applications for 18 posts advertised during 2006. Candidates from all over Europe showed their interest in working for ENISA, not only in the operational positions, but also in the administrative posts.

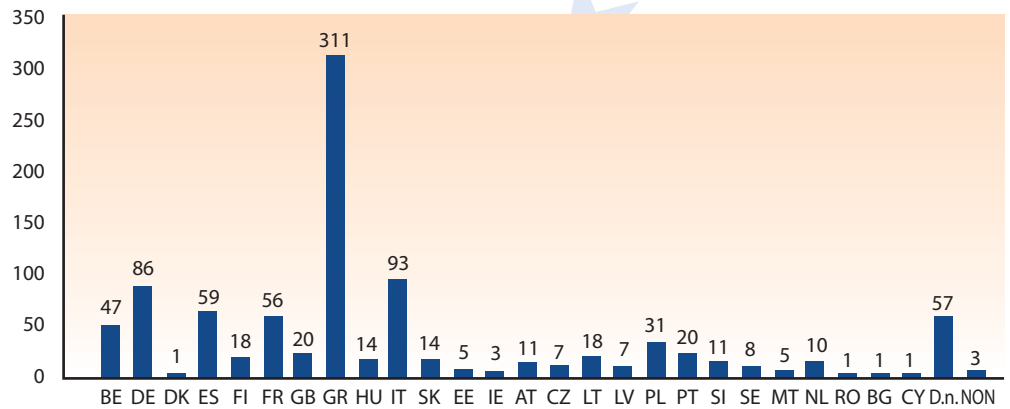
The following graphs depict some statistics about the applicants based on four indicators:

- Gender
- Nationality
- Age
- Function group (administrator/assistant).

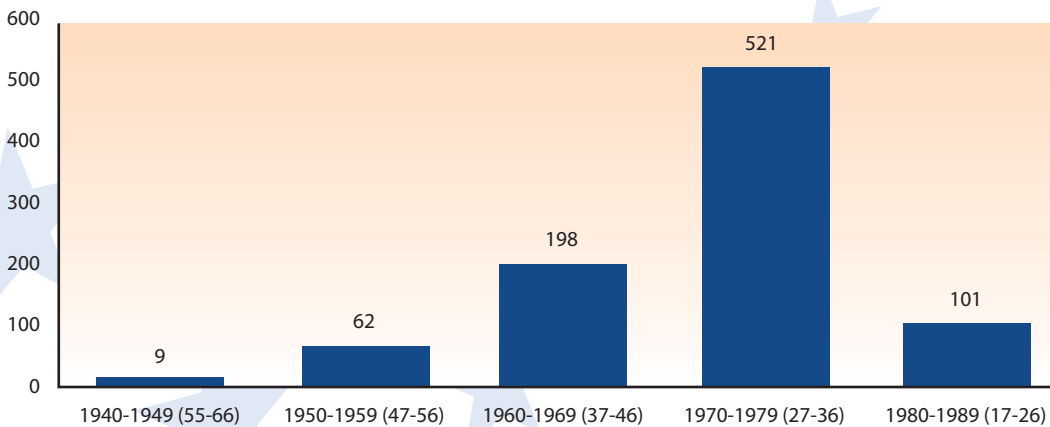
a. Applicants by gender



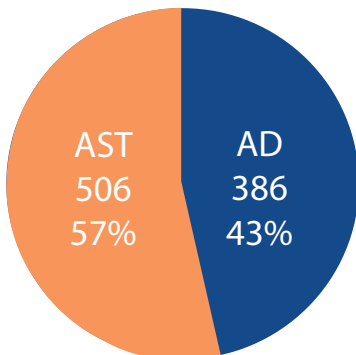
b. Applicants by nationality



c. Applicants by age



d. Applicants by function group



Note: For the sake of brevity, the function group AD (administrator) also includes the applicants for the CA posts in function group IV, while the function group AST (assistant) comprises the applicants for CA posts in function groups I, II and III. The male/female ratios were 37% to 63% for the AST level posts, and 59% to 41% for the AD level posts.

Further to the successful recruitment process, 15 new staff members were appointed in 2006.

General update figures on recruitment of 2006 positions

Category	2006 positions published	Interviews finalised	Posts filled
AD	8	8	7
AST	10	10	8
TOTAL	18	18	15

As soon as new staff members are appointed, the HR Section's administrative work increases. The typical activities related to new appointments are numerous and vary from the organisation of the compulsory pre-recruitment medical visits to providing assistance to new colleagues and their families. The HR Section provides whatever support it can to new staff in order to ensure their smooth and positive settlement in their new working and living environment.

In addition to the recruitment of statutory staff, the HR Section finalised the selection procedure of two National Experts (from Poland and Italy) who were seconded to the Agency's operational departments for a period of six months. Thanks to successful co-operation with the National Administrations, the Agency will now benefit from these experts' high level of professional knowledge and experience. A new call for expressions of interest for seconded national experts was launched in Q3 of 2006. The selection process concluded with the nomination of two new experts from Austria and Italy who are expected to join the Agency at the beginning of 2007.

In 2006 ENISA launched its first traineeship programme which offered a 5-month period of 'work experience in a dynamic international environment for young university graduates in the field of network and information security'. This new programme aims to provide an understanding of the Agency's objectives and activities, enabling trainees to acquire practical knowledge and experience of the day-to-day work of the organisation. The scheme represents a contribution to the integration of all citizens in Europe. The Agency could also benefit from the fresh point of view and up-to-date academic knowledge which these trainees bring. ENISA welcomed its first trainee from Latvia in November 2006.

The HR Section continued to outsource the hiring of ad-interim staff to provide administrative support to the administration and the operational departments until the completion of the recruitment process for 'Temporary Agents' and 'Contract Agents'.

Agency's Staff Members (as at 31 December 2006)

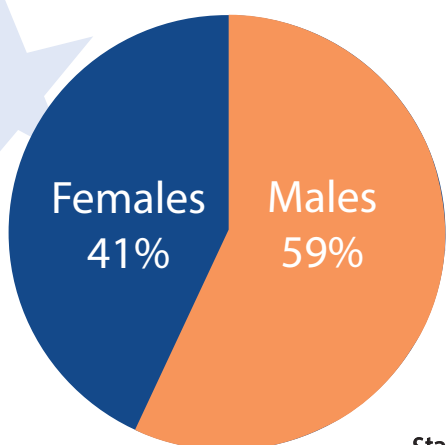
Further to the successful selection procedures, at the end of 2006 the Agency's staff comprised 44 staff members, 1 trainee and 1 seconded national expert. The following table depicts the appointment of the total workforce of the Agency chronologically:

	Total workers	Temporary agents	Contract agents	Interim staff	Seconded National Experts	Trainees
1 Dec 05	47	35	0	10	2	0
1 April 06	45	35	3	5	2	0
1 July 06	41	33	3	3	2	0
1 Sep 06	43	34	5	3	1	0
1 Dec 06	49	37	7	4	1	1

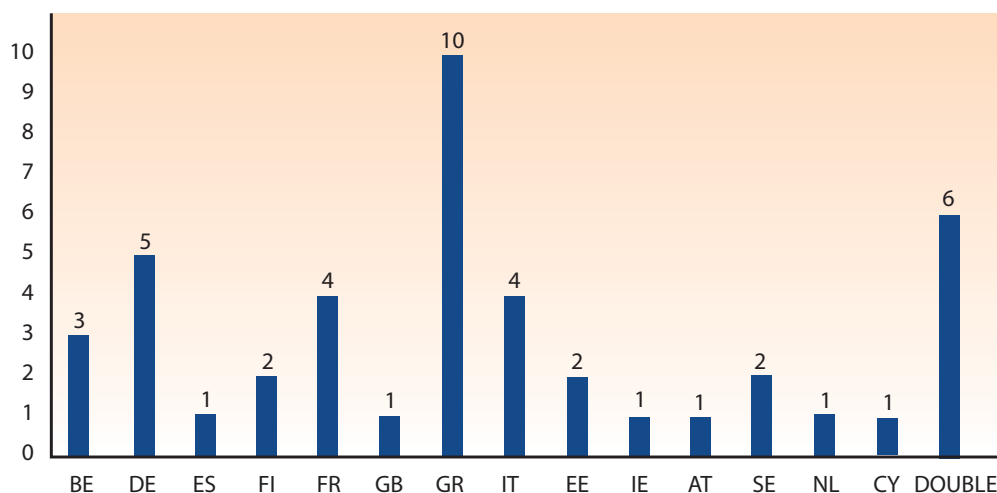
The following conclusions can be drawn from these statistics:

- **Gender:** The division between males and females remains balanced, as in 2005, with a slight majority of male staff members.
- **Nationality:** 14 out of 25 nationalities of the European Union are represented, with a high percentage from the 'old' Member States. 14% of the total staff has dual nationality, as indicated in the separate column in the graph below.
- **Age:** The majority of staff continues to be aged between 31 and 40 years.
- **Function group:** the majority of staff members occupy posts at administrator's level.

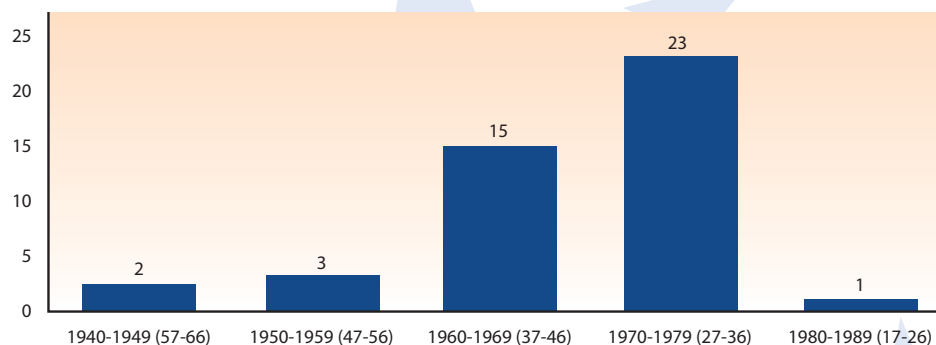
Staff members by gender



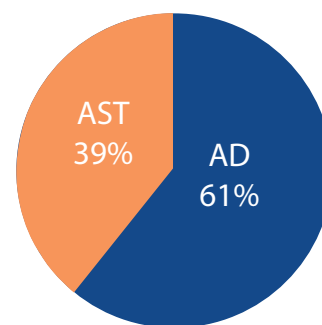
Staff members by nationality



Staff members by age



Staff members by function group



Training

One of the main activities of the HR Section in 2006 was the management of training. Training is an important tool in order to achieve and maintain the highest quality standards and reflect the Agency's core values of excellence, professionalism and service. The successful finalisation of the procurement procedure for the selection of training providers facilitated the organisation and implementation of language courses for the Agency's staff. The general objective was to develop the staff's language skills in Greek, French and German at beginners' level and in English at advanced level. With specific reference to the provision of Greek courses, the main scope of the language course has been to facilitate the integration of staff members and their families into the local Greek environment.

In addition, a Service Level Agreement with the European Commission on training was signed in Q2 of 2006 and came into force in Q3 of 2006. This facilitated the organisation of training courses targeted at the entire staff on Agency premises. Training in organisational and individual development was organised in Q3 of 2006 to facilitate a teambuilding spirit and increase the sense of mutual respect, support and community within the Agency. In particular, a participative workshop was organised on how to build a community at ENISA and how to work more effectively both as individuals and as a team.

The HR Section also supported staff in their individual training requests. Staff were able to participate in specific external training courses in order to enhance their professional performance.

Staff Evaluation and Performance

The performance of probationary staff recruited in 2005 was duly evaluated with the positive confirmation of all employment contracts. The overall appraisal evaluation confirmed the high level of ability, efficiency and integrity of the Agency's staff. In addition, the HR Section was involved in the preparatory work of the Grading Committee that met on a regular basis in order to assess the correct grade of individual employees.

Health & Safety at Work

In 2006 HR launched the Agency's first health and safety programme. Intensive activities were organised to improve the working environment within the organisation. Thanks to a successful procurement process, the Agency could purchase new ergonomic chairs for the entire staff and ensure higher standards of work units. Specific training on health and safety at work was also provided to the staff by a specialist company.

A medical adviser was contracted to interact with the management and the staff on medical aspects related to the Agency's activities, to advise the administration in the medical domain and to act as an interface with local medical services. A special office has been arranged in the Agency's premises in order to facilitate regular meetings between the medical adviser and staff members.

Other activities

HR had to carry out more regular tasks such as preparing salaries, calculating the allowances to which staff members are entitled, reimbursing costs related to interviewing candidates and medical expenses, processing payments, organising personal files and handling all requests for assistance and clarification submitted by the employed staff.

In addition to other routine duties, the HR Section also handled the Agency's requests for official translations of documents and contacts with the Translation Centre of the European Communities.

© European Network and Information Security Agency (ENISA), 2007

Published in July 2007

Produced by Kingston Public Relations Ltd, UK (+44 1482 876229) www.kingstonpr.com



PO Box 1309, 710 01, Heraklion, Crete, Greece
Tel: +30 2810 39 12 80, Fax: +30 2810 39 14 10
E-mail: info@enisa.europa.eu
www.enisa.europa.eu