

Greece Country Report



About ENISA

The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. ENISA is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard of information for good practices. Moreover, the agency facilitates contacts between the European institutions, the Member States and private business and industry actors.

Contact details

For contacting ENISA or for general enquiries on the Country Reports:

Mr. Giorgos Dimitriou

ENISA External Relations Expert

Giorgos.Dimitriou@enisa.europa.eu

Internet: <http://www.enisa.europa.eu>



Acknowledgments:

ENISA would like to express its gratitude to the National Liaison Officers that provided input to the individual country reports. Our appreciation is also extended to the ENISA experts and Steering Committee members who contributed throughout this activity.

ENISA would also like to recognise the contribution of the Deloitte team members that prepared this country report on behalf of ENISA: **Dan Cimpean, Johan Meire, Nicolas Roosens, Ioannis Diveris and Alexandros Charvalias.**

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be an action of ENISA or the ENISA bodies unless adopted pursuant to the ENISA Regulation (EC) No 460/2004 as amended by Regulation (EC) No 1007/2008. This publication does not necessarily represent state-of-the-art and it might be updated from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication. Member States are not responsible for the outcomes of the study.

This publication is intended for educational and information purposes only. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication. Reproduction is authorised provided the source is acknowledged.

© European Network and Information Security Agency (ENISA) 2011

Table of Contents

GREECE	4
THE STRUCTURE OF THE INDIVIDUAL COUNTRY REPORTS	4
NIS NATIONAL STRATEGY, REGULATORY FRAMEWORK AND KEY POLICY MEASURES	5
OVERVIEW OF THE NIS NATIONAL STRATEGY	5
THE REGULATORY FRAMEWORK	6
NIS GOVERNANCE	10
OVERVIEW OF THE KEY STAKEHOLDERS	10
INTERACTION BETWEEN KEY STAKEHOLDERS, INFORMATION EXCHANGE MECHANISMS IN PLACE, CO-OPERATION & DIALOGUE PLATFORMS AROUND NIS	11
FOSTERING A PROACTIVE NIS COMMUNITY	13
COUNTRY-SPECIFIC NIS FACTS, TRENDS, GOOD PRACTICES AND INSPIRING CASES....	14
SECURITY INCIDENT MANAGEMENT	14
EMERGING NIS RISKS	14
RESILIENCE ASPECTS	15
PRIVACY AND TRUST	16
NIS AWARENESS AT THE COUNTRY LEVEL	17
RELEVANT STATISTICS FOR THE COUNTRY	19
INTERNET ACCESS OF POPULATION AND ENTERPRISES	19
STATISTICS ON USE OF INTERNET BY INDIVIDUALS AND RELATED SECURITY ASPECTS	20
STATISTICS ON USE OF INTERNET BY ENTERPRISES AND RELATED SECURITY ASPECTS	21
OTHER STATISTICS	22
APPENDIX	23
NATIONAL AUTHORITIES IN NETWORK AND INFORMATION SECURITY: ROLE AND RESPONSIBILITIES	23
COMPUTER EMERGENCY RESPONSE TEAMS (CERTs)	26
INDUSTRY ORGANISATIONS ACTIVE IN NETWORK AND INFORMATION SECURITY	26
ACADEMIC ORGANISATIONS ACTIVE IN NETWORK AND INFORMATION SECURITY BODIES	27
OTHER BODIES AND ORGANISATIONS ACTIVE IN NETWORK AND INFORMATION SECURITY	28
REFERENCES	29

Greece

The structure of the individual country reports

The individual country reports (i.e. country-specific) present the information by following a structure that is complementary to ENISA's "Who-is-who" publication and is intended to provide additional value-added to the reader:

- *NIS national strategy, regulatory framework and key policy measures*
- *Overview of the NIS governance model at country level:*
 - *Key stakeholders, their mandate, role and responsibilities, and an overview of their substantial activities in the area of NIS:*
 - *Interaction between key stakeholders, information exchange mechanisms in place, co-operation & dialogue platforms around NIS*
 - *Fostering a proactive NIS community*
- *Country specific NIS facts, trends, good practices and inspiring cases:*
 - *Security incident management*
 - *Emerging NIS risks*
 - *Resilience aspects*
 - *Privacy and trust*
 - *NIS awareness at the country level*
 - *Country-specific activities for identifying and promoting economically efficient approaches to information security*
 - *Interdependencies, interconnection and improving critical information infrastructure protection*
- *Relevant statistics for the country.*

This report is based on information which was publicly available when research was carried out, as well as comments received from National Liaison Officers and ENISA experts. As such, the country report presents a high-level snapshot of NIS at the turn of the year.

NIS national strategy, regulatory framework and key policy measures

Overview of the NIS national strategy

Digital Strategy 2006-2013

As stated in the previous issue of this report, the goals and main objectives of Greece in NIS are tackled in the 'Digital Strategy 2006-2013'. The fundamental aim of the strategy is to use information technologies for achieving higher productivity in the economy and for improving citizens' quality of life, so as to materialize a "Digital leap".

The essential difference compared to previous practices is that the new strategy is not focused on specific projects per organisation but on prescriptions of services to be offered.

There are six basic orientations for the strategy – four of them focus on productivity and two on the quality of life:

- Promotion of ICT in enterprises;
- Supply of digital services to enterprises and restructuring of the public sector;
- Strengthening of the ICT sector;
- Promotion of entrepreneurship in ICT related activities;
- Improvement of daily life through ICT; and
- Design of digital services for the citizen.

The common denominator for all of the above is fast broadband Internet connectivity.

The path to the 'Digital Leap', i.e. the realization of a new digital strategy for Greece, involves 65 new actions. Emphasis is placed on significant broadband improvements, on the development of systems for electronic procurements, on information campaigns and the sensitization of the citizens to new technologies. A most practical priority of this strategy is to support enterprises towards the effective and efficient provision of the top 20 services to the citizens.

These actions are critical for taking the digital leap. In regards to the period following 2008, the design contemplates the establishment of one-stop electronic points with the aim to further accelerate services to enterprises. Also, the restructuring of the public sector will automate procedures and new technologies will be better integrated into the educational system.

An Operational Programme, called 'Digital Convergence', specifies strategy and actions aimed at the efficient utilization of Information and Communication Technologies (ICT) in the period 2007-2013. Amongst the main axes of this programme figure:

- The improvement of digital/online services to enterprises and re-engineering of relevant public administration processes;
- The promotion of Internet and ICT usage by enterprises;
- The development of digital/online services for Citizens.

The programme has a strong regional character, as major part of the described actions and interventions concerns all of the 13 regions of Greece.

The regulatory framework

No changes were noticed since the 2009 ENISA Country Report on Greece. The Greek national regulations having relevance and applicability in the domain of network and information security are the following:

eGovernment Legislation

A dedicated e-Government law has been drafted, scrutinized through a public consultation and is currently in the finalization process.

Data Protection/Privacy Legislation

Law on the Protection of Individuals with regard to the Processing of Personal Data, as amended

Based on the Law 2225/1994, the National Committee of Privacy of Communications was founded.

Law 2472/1997 on the Protection of Individuals with regard to the Processing of Personal Data was adopted in April 1997. It establishes the core principles and rules under which the processing of personal data is to be carried out so as to protect the fundamental rights and freedoms of natural persons and in particular their right to privacy. It also allows any person to obtain their personal information held by government departments or private entities.

The law, which was amended in 2000 and 2001, is enforced by the Hellenic Data Protection Authority. It is complemented by Law 2774/1999 on the Protection of Personal Data in Telecommunications, and by Law 3115/2003 that establishes the Hellenic Authority for the Information and Communication Security and Privacy in order to protect the secrecy of mailing, the free correspondence or communication in any possible way as well as the security of networks and information. The law has been revised by the Law 3471/2006 in June 2006.

The institutional framework of telecommunication privacy protection is further enhanced with Law 3674/2008, requiring a number of additional protection measures to be adopted by telecommunication providers, to ensure a better level of security in the provision of telephone services, and to enforce strict criminal and administrative penalties.

Article 13 of Law 3674/2008 defines the implementation of a National Framework for Communications Security (NFCS, ESAE in Greek) for public institutions, public legal entities, and telecommunication providers. The purpose of the NFCS is to provide a common security baseline for all nation-wide communication capabilities that serve the public sector and the citizens. Exceptions include classified networks where the National Security Regulation (EKA) is applied and other special-purpose, classified networks (e.g. Army). The NFCS is in progress at the time of this writing and is expected to be finalized in the summer of 2011.

Law on the Protection of Personal Data and Private Life with regard to Electronic Telecommunications and revision of Law 2472/1997

Law 3471/2006 was adopted on 28.06.2006 and intends to the enactment of preconditions with regard to the personal data processing and for the assurance of the confidentiality in telecommunications.

eCommerce Legislation

Presidential Decree 131/2003 on eCommerce

Adopted on 16 May 2003, this presidential decree transposes the Directive 2000/31 of the European Parliament and the Council on certain legal aspects of Information Society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce).

eCommunications Legislation

The full transposition of the new EU Regulatory Framework for Electronic Communications has not taken place in Greece yet. eCommunications are governed by the Telecommunications Law 3431/2006 that substituted Law 2867/2000.

The European Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, has been published in the official Gazette of the Government (February 2011), with a general provision of a 12 months data retention period for communication data. .

The European Directive 2002/58/EC on privacy and electronic communications (ePrivacy Directive) has been already implemented into national law by the Law on the Protection of Personal Data and Private Life with regard to Electronic Telecommunications (3471/06)

The transposition of the European Directives 2009/136/EC and 2009/140/EC is currently under the early stages of processing.

The European Directive 2009/136/EC amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No. 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws. Regarding the implementation of certain articles of the Directive 2009/136/EC, the following apply:

- Article 5(3) – Cookies: the respective Greek law (3471/2006, currently active) provides already for the explicit consent of the user (Article 4, par. 5);
- Article 4(3) – Personal data breach notification obligations: not yet fully implemented; however, ADAE regulations address (partially) this issue by establishing an inventory of security incidents which vendors are obliged to update when such an incident occurs;
- Article 13 – Unsolicited communications (spam) and direct marketing: not yet implemented – however, there is a HDPa Decision, regarding political spam in the period of elections.

The European Directive 2009/140/EC, amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorization of electronic communications networks and services.

The European Directive 1997/67/EC as amended by 2002/39/EC and 2008/6/EC with regard to the full accomplishment of the internal market of Community postal services is under final review. Based on the draft law, a new department is established under the General Secretariat of Communications, with responsibilities including among others, network security.

eSignatures Legislation

Presidential Decree 150/2001

This presidential decree came into effect on 25 June 2001 and implements the European Directive 1999/93/EC of 13 December 1999 on a Community framework for electronic signatures. It defines electronic signatures and advanced electronic signatures. It also deals with the legal consequences of electronic signatures, liability of suppliers of certification, obligation to protect personal information, terms in effect for recognized certificates and suppliers, assurance of the liability of the creation of a signature and recommendations for the verification of the signature. EETT performed a comprehensive compliance audit regarding the three major vendors of qualified digital certificates in Greece, issuing recommendations reports (2007 – 2009).

Other relevant regulations issued by the Hellenic Authority for Communication Security and Privacy (ADAE)

Secrecy Assurance Regulations for Telecommunication Services

This regulation concerns all telecommunication providers of mobile, fixed and wireless networks, providing telecommunication services

Secrecy Assurance Regulations for Internet Telecommunications

The following decisions have been published in FEK 88/2005:

- Internet Communications, Services and Applications Privacy Assurance Regulation;
- Internet Applications and Internet Users Privacy Assurance Regulation;
- Internet Telecommunication Infrastructures Privacy Assurance Regulation.

Other relevant regulations issued by the EETT – Greek National Telecommunications and Post Commission

EETT has issued a Code of Practice concerning the Provision of Electronic Communication Services to the Consumer, which defines a series of obligations and recommendations to the providers aiming at dealing with problems which had previously been identified in the context of EETT activity as well as in the processing of consumer complaints.

This Code lays out the general guidelines, clarifies procedures and clearly defines the behaviour and obligations of telecommunication service providers toward the consumer. Furthermore, it regulates issues related to the pre-contractual and contractual transactions between the consumer and the provider, putting emphasis on the detailed and clear flow of information to the consumer.

National Authority Against Electronic Attacks (NAAEA) – National CERT

The mission of the National Authority Against Electronic Attacks is to attend to the prevention as well as the passive and active encounter of electronic attacks against communication networks, data storage facilities and IT systems. In addition, the Authority is responsible for processing the data and notifying the competent authorities.

Responsibilities of the National CERT:

- The National Authority Against Electronic Attacks is the agency responsible for encountering-protecting mainly the Public Sector along with the Critical National Infrastructures as established by Law 3469/2008 and Presidential Decree 126/2009.

- The Authority utilizes the appropriate equipment and is staffed by the scientific personnel necessary for its operation, the implementation of the strategic policy decisions pertaining to the encountering of threats and/or attacks and finally the collection, processing and dissemination of the relevant information.
- In order to fulfil its mission more effectively the National Authority Against Electronic Attacks cooperates with foreign national or other CERT authorities and relevant agencies but with in-country government services, as well.

Self-regulations

Self-regulatory Code of Conduct for Value Added Services Provided through Mobile Phones and for the Protection of Minor Users + Annex A' Memorandum for Safer Mobile Use by Children and Younger Teenagers

The Greek mobile telecom operators have adopted a code of conduct that describes duties of the signatory members in ensuring minimum protective measures for safer use of the content provided on the mobile phone. The code has been tailored to the needs of the Greek mobile electronic telecommunications market and complies with applicable European and national legislation.

eIdentity

Greece uses a paper national ID card for its citizens.

This country offers one PKI based system, Syzefxis (the "National Public Administration Network"), which is managed by contractors. Additionally, it has two non PKI systems: TAXISnet (used by tax authorities), based on on-line identification using the tax number and the ID card number; and the E-KEP platform (citizen service centre), based on on-line identification.

NIS Governance

Overview of the key stakeholders

We included below a high-level overview of the key actors with relevant involvement, roles and responsibilities in NIS matters.

National Authorities	<ul style="list-style-type: none"> • Ministry of Infrastructure, Transport and Networks (government) • General Secretariat for Public Administration and Electronic Governance • Ministry of Interiors, Decentralisation and Electronic Governance (government) • General Secretariat for Information Systems, Ministry of Finance (government) • General Secretariat for Research and Technology – Ministry of Education, Lifelong Learning and Religious Affairs (government) • EETT – Hellenic National Telecommunications and Post Commission • ADAE (Hellenic Authority for Communication Privacy) • Hellenic Data Protection Authority (HDPA) • National Intelligence Service (EYP) • National Authority Against Electronic Attacks – National CERT • Hellenic Police - Electronic Crime Department
CERTs	<ul style="list-style-type: none"> • AUTH-CERT - Aristotle University of Thessaloniki CERT • GRNET-CERT - Greek Research and Technology Network Computer Emergency Response Team (it is operated and staffed by the University of the Aegean) • FORTH CERT - Foundation for Research and Technology CERT
Industry Organisations	<ul style="list-style-type: none"> • SEPE (Federation of Hellenic Information Technology & Communications Enterprises) • SEPVE (Association of Information Technology Companies of Northern Greece) • SATPE (Greek Licensed Telecommunication Providers Association) • The Southeast Institute for Computer Science – Foundation for Research and Technology (INA Institute)
Academic Organisations	<ul style="list-style-type: none"> • ICS-FORTH (Institute for Computer Science – Foundation For Research and Technology) • GRNET (Greek Research and Technology Network) • Research Academic Computer Technology Institute (RA-CTI) • Research Centre Demokritos (N.S.C.R Demokritos) • Laboratory of Information & Communication Systems Security – University of the Aegean (UoA) • Information Security and Critical Infrastructure Protection Research Group – Athens University of Economics and Business (AUEB) • Telecommunication Networks and Integrated Services Laboratory, Department of Digital Systems – University of Piraeus (UniPi)

For contact details of the above-indicated stakeholders we refer to the ENISA “Who is Who”¹ – 2010 Directory on Network and Information Security and for the CERTs we refer to the ENISA CERT Inventory².

NOTE: only activities with at least a component of the following eight ENISA focus points have been taken into account when the stakeholders and their interaction were highlighted: CERT, Resilience, Awareness Raising, Emerging Risks/Current Risks, Micro-enterprises, e-ID, Development of Security, Technology and Standards Policy; Implementation of Security, Technology and Standards.

¹ The ENISA Who-is-Who Directory on Network and Information Security (NIS) contains information on NIS stakeholders (such as national and European authorities and NIS organisations), contact details, websites, and areas of responsibilities or activities. Ref. code: ISBN 978-92-9204-003-1 - Publication date: May 12, 2010

² <http://www.enisa.europa.eu/act/cert/background/inv/certs-by-country/>

Interaction between key stakeholders, information exchange mechanisms in place, co-operation & dialogue platforms around NIS

Co-operation between public authority bodies

The following interaction mechanisms were observed:

- Government driven: through different initiatives and programs (e.g. Program “Information Society”), the government calls private sector to submit proposals of projects for funding;
- The majority of the public initiatives in the area of information society (National Strategic Reference Framework, see www.espa.gr) tackle information security at a horizontal level; thus, the information society projects funded by the European structural funds in the framework of information society are subject to security risk analysis and risk assessment and the definition of a security policy;
- Public consultations (often initiated by the Greek electronic communications regulator – EETT): the Government officially supports initiatives and consultation fora with industry. One of these fora through which the government promotes the market dialogue on a wide range of topics relevant to information society, including NIS, is the E-Business forum (<http://www.ebusinessforum.gr>). The forum is funded with resources of the Programme “Information Society” and, since its set-up (year 2000), it has supported the formation of 54 working groups to look into different thematic areas of e-business. A number of these working groups have been focused on subject matters related to electronic communication services and security of data exchanges, such as: FTTx (Fiber to the Home – Fiber to the Building), Interactive Digital Television, Broadband penetration, unified communications, PKI and electronic signatures, etc.

Co-operation and dialogue platforms around NIS

Dialogue and consultation between regulators, government and market stakeholders take place through the set-up of a few formal consultation platforms, such as the E-Business forum³. Yet, this forum deals with topics from the broad thematic area of information society and e-business. It should however be pointed out that the accent of many working groups has often been put on NIS topics.

The design of the Greek Digital Strategy (see below, Section “NIS Strategy”) was a collaborative effort between the ICT Commission and of more than 20 managing directors and high ranking officers from the sectors of IT and Communications. In this effort contributed also information users (e.g. banks, commerce players, etc.), agencies of the public sector, staff from the Ad-hoc Secretariat of the Information Society, experts and associations (e.g. the Federation of Hellenic Information Technology & Communication Enterprises [SEPE] and the Federation of Greek Industries, etc).

Recognizing the issue of digital security as of particular importance to citizens, and aiming to enhance user’s confidence to the new media, the Special Secretariat for Digital Planning proceeded to the establishment of the ‘Task Force on Digital Security’ with the name DART (Digital Awareness & Responses to Threats). The immediate objective of the team is to inform citizens, prevent and address risks associated with the new technologies and electronic communications. The team includes all agencies, organisations and NGOs that work on Internet security matters; through a systematic plan, the team updates citizens and small businesses across the country.

³ See: <http://www.ebusinessforum.gr>

In the framework of the Operational Programme for the Information Society (OPIS) the phone line 1020 was activated for the Digital Greece, aiming to serve the citizens in matters relating to the use of new technologies and the Internet, the ongoing actions and the issues raised around digital security.

Co-operation and initiatives on security incidents

- Reporting to ADAE of security incidents according to its responsibilities (not mandatory);
- Reporting to National Authority Against Electronic Attacks (NAAEA) – National CERT of security incidents;
- Submission to ADAE by electronic communications service providers of their security policies ensuring the secrecy and confidentiality of communications (mandatory);
- Exchanges with the electronic communications regulator (EETT) take place on an “ad-hoc” basis, in case in which the authority communicates a request or query for clarification to market operators. Other means of communication with EETT is the organization of public surveys to obtain providers’ feedback and take stock of market experiences before the adoption of new regulatory approaches or regulatory measures;
- Digital Awareness and Response to Threats (DART): Set-up under the auspices of the Special Secretariat of Digital Design (Ministry of Regional Development and Competitiveness), DART has as main objective to enhance user confidence in electronic communications tools, as well as to contribute to the prevention of threats and incidents relating to new technologies. The awareness campaigns of DART aim at coordinate the efforts of the competent public authorities, as well as to reinforce users’ reliance on the fast Internet.

Co-operation on information security at an international level

The Southeast Institute for Computer Science – Foundation for Research and Technology (INA Institute) publishes the “SEE ICT Monitoring Review” - a series of reports that provides a detailed overview of the developments that shape the Information and Communication Technology (ICT) Sector in the countries of South-East Europe (SEE).

Each publication comprises 10 issues that are focused on Albania, Bosnia-Herzegovina, Bulgaria, Croatia, FYROM, Moldova, Montenegro, Romania, Serbia and Turkey. Each issue contains detailed analysis and data on the country's Economic, Political and Regulatory Environment, the most up-to-date information on its Competitive ICT Environment, which includes telecom statistics based on Fixed, Mobile and Internet Market indicators, and the profiles of the Market's Key Players. INA currently proceeded with the second publication of the “SEE ICT Monitoring Review”.

- Updated Statistical Data;
- Intelligent Sector Analysis;
- Country Data Comparisons;
- Info on collaboration with regional Telecom Regulators, ITU and Telecom Operators.

A Regional Electronic Security Forum: Telecommunications Networks and Systems Security is also organised by the South Eastern Europe Telecommunication & Informatics Research Institute (INA). The most recent one took place in 2008: “4th Regional Electronic Security Forum: Telecommunications Networks and Systems Security, 6 & 7 November 2008, Thessaloniki, Greece”.

Finally, a project coming under European programme FP7 Security 2009 titled “SecureCHAINS - Integration of Security Technology Supply Chains and Identification of weaknesses and untapped potential” has commenced from May 2010.

Fostering a proactive NIS community

International cooperation through the TERENA initiative

It is interesting to mention that the Greek Research and Technology Network Computer Emergency Response Team (GRNET-CERT) participates in international forums and exchanges organized by TERENA, ⁴Trans-European Research and Education Networking Association.

⁴ Source: www.terena.org/activities/tf-csirt/meetings.html

Country-specific NIS facts, trends, good practices and inspiring cases

Security incident management

The National Authority Against Electronic Attacks (NAAEA) – National CERT, attends to the prevention as well as the passive and active encounter of electronic attacks against communication networks, data storage facilities and IT systems. In addition, the Authority is responsible for processing the data and notifying the competent authorities.

No particular NIS incident report is published by the National CERT or any other relevant authority.

Cyber Defence initiatives

The Ministry of Infrastructure, Transport and Networks participated as full member in the “**CYBER EUROPE 2010**” – the first pan European exercise on CIIP (Critical Information Infrastructure Protection) which took place on Nov. 4, 2010 and organized by ENISA.

The Greek Army (Division of Cyber Defence) organized the first National Cyber Defence exercise (**PANOPTIS 2010**), which was held on May 17-19, 2010. The exercise, which was fully supported by the Ministry of Infrastructure, Transport and Networks, tested the cooperation and response to realistic cyber threat scenarios with a number of participants from military bodies, public sector organizations and academia; this national cyber defence exercise will take place in a yearly manner, with the sequel (PANOPTIS 2011), to be held on September 2011 with an extended scope of scenarios and actors (i.e. communication vendors from the private sector and national critical infrastructures operators).

Emerging NIS risks

No specific details were noted on emerging NIS risks that are officially considered by the Greek authorities.

The Institute of Computer Science (ICS), Foundation for Research and Technology – Hellas (FORTH) is active⁵ in the collaboration and partnership initiatives focused on emerging NIS risks, like initiatives i-CODE⁶, FORWARD⁷, SYSSEC⁸ and WOMBAT⁹, detailed below:

- The i-CODE project is an effort to create an integrated forensics console for real-time malicious code identification which will be easy to use by the broader community. The developed toolset will include capabilities for detection, identification and categorization of malicious code spreading through current and next-generation networks;
- The FORWARD initiative aims at identifying, networking, and coordinating the multiple research efforts that are underway in the area of cyber-threats defences, and leveraging these efforts with other activities to build secure and trusted ICT systems and infrastructures. The initiative concluded in the first quarter of 2010 with the issuance of a whitepaper containing detailed and concrete scenarios of how adversaries can leverage the emerging threats identified by the FORWARD project working groups to carry out their

⁵ See the presentation: www.ict-forward.eu/media/publications/fidis2008-presentation-forward.pdf

⁶ See: www.icode-project.eu

⁷ See: www.ict-forward.eu

⁸ See: <http://syssec-project.eu/>

⁹ See: <http://wombat-project.eu/>

malicious actions. These scenarios illustrate future dangers and provide arguments to policy makers that are needed to support research in critical areas;

- The SYSSEC project relates to creating a Network of Excellence in the field of Systems Security for Europe to play a leading role in changing the rules of the game. Capitalizing on the results of the recent FORWARD initiative and building on strong synergies with Industry and Policy makers, SysSec will work towards:
 - Creating a virtual centre of excellence, to consolidate the Systems Security research community in Europe;
 - Promoting cybersecurity education;
 - Engaging a think-tank in discovering the threats and vulnerabilities of the *Current and Future Internet*;
 - Creating an active research roadmap in the area, and
 - Developing a joint working plan to conduct State-of-the-Art collaborative research;
- The Worldwide Observatory of Malicious Behaviours and Attack Threats (WOMBAT)¹⁰ project has an interface for data exchange, administered by FORTH in Greece, and is expected to conclude within 2011.

Resilience aspects

In Greece, EETT submitted to public consultations a set of regulations that contain network resilience aspects, including minimum requirements to ensure integrity and availability of certain eCommunications services.

Also, EETT submitted a Recommendation to the Greek Minister of the Interiors, Decentralization & Electronic Governance and to the Minister of Infrastructure, Transport & Networks for the issue of a Joint Ministerial Decision which shall define the minimum requirements of telecommunication providers for the integrity of public telephone networks at fixed locations. The determination of these minimum obligations to which fixed public telephone network providers must comply, aims at ensuring the provision of fixed telephony services to citizens under any circumstances, even in the case of emergency conditions which may arise following a catastrophic event or an event due to force majeure.

The recommendation comprises a series of obligations which must be fulfilled by providers operating public telephone networks at fixed positions. Indicatively, some of these obligations are stated here below:

- Implementation of Risk Assessment and Business Impact Analysis;
- Drafting of Business Continuity Plans;
- Drafting of Recovery Plan from Catastrophic Events;
- Strengthening network reliability through various measures such as equipment and power supply redundancy physical safety, maintenance, and restoration of network operation;
- Ensuring the integrity and availability of the information necessary for the provision of services;
- Ensuring uninterrupted access to emergency services.

In addition, the recommendation comprises issues related to provision of timely and effective information to consumers regarding the events which may threaten or affect the operation of the network and the provision of services. According to Law 3431/2006 on Electronic Communications, EETT will monitor the compliance of providers with the minimum obligations included in the recommendation.

¹⁰ See: <http://www.wombat-project.eu/>

No other particular/specific network resilience enforcement rules were noted for Greece, therefore neither specific enforcement action were taken towards operators who infringed resilience rules. These aspects will be taken into account in the forthcoming National Framework for Communications Security.

Privacy and trust

Status of implementation of the Data Protection Directive

The Data Protection Directive has been implemented in Greece by the Data Protection Act (Law 2472/1997) amended by the Law 3471/2006 – G.G. 133A'/28.06.06 (collectively named the "DPA").

The competent national regulatory authority on this matter is the Hellenic Data Protection Authority (the "Authority").

Personal Data and Sensitive Personal Data

The definition of personal data in the Greek DPA is closely based on the standard definition of personal data. However, it can also apply to legal persons, since companies are constituted of natural persons entitled to apply for the protection of the corporate data. Companies may also be entitled to apply for their data protection based on Article 9 of the Greek Constitution and Articles 57 and 59 of the Greek Civil Code.

Under the DPA, sensitive personal data includes: (i) the standard types of sensitive personal data (i.e. personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.); (ii) information about criminal offences and alleged criminal offences; and (iii) participation in syndicates, social groups.

Sensitive personal data may be processed if the standard conditions for processing sensitive personal data are met. Compliance with a legal obligation imposed in connection with employment is a condition for personal data processing but not sensitive data processing. In addition, processing is permitted for medical treatment, national security, crime-prevention, research or scientific purposes or journalistic purposes.

The processing of sensitive personal data also requires a license from the Greek Data Protection Authority.

Information Security aspects in the local implementation of the Data Protection Directive

Data controllers must comply with the general data security obligations. Specific regulations have been issued with regard to security measures and use of technological measures for the protection of personal data. These measures should protect personal data and maintain its quality. For this reason, data controllers should take all appropriate technical, physical and organisational measures to protect personal data against unauthorised access, unlawful processing, accidental loss or damage or unauthorised destruction (e.g. physical access control, CCTV, biometrical techniques, secure information system firewalls, security patching and threat analysis).

Enforcement

The Hellenic Data Protection Authority has the power to take direct enforcement action in Greece. It has the authority to issue enforcement notices, as well as the ability to fine organisations itself. Prosecutions for criminal offences are brought before the Greek Criminal Courts who can impose fines. There is no requirement to notify the Authority of a breach of the DPA.

DNSSEC: DNS Security Extensions

Since 15th of December 2010 the [.gr] zone file as well as the zone files for the secondary level domains are digitally signed by making use of the DNSSEC technology. As the authoritative RRsets of the [.gr] zone are signed, DNS resolvers can use the public key that signed those records and thus authenticate them, which greatly improves the security and authenticity of the information returned from DNS name servers, eliminating DNS spoofing.

To take advantage of the increased security offered by DNSSEC, domain names currently registered in [.gr] must gradually make use of DNSSEC, which will soon be made available via the [.gr] registrars. The use of DNSSEC technology is optional.

The Registry of [.gr] Domain Names, a department of the Institute of Computer Science of the Foundation of Research and Technology Hellas, is responsible for the operation and technical coordination of the [.gr] top-level domain name space. This role has been assigned to the Registry by the Hellenic Telecommunications and Post Commission (EETT).

NIS awareness at the country level

In Greece, several NIS awareness raising measures are undertaken by both competent authorities as well as by private companies, academic bodies and NGOs.

Awareness initiatives between providers and public authorities

ADAE has organized a conference in 2005 dealing with the general principles of national strategy for the privacy and security of networks and information. The aim of this conference was to establish a continuous forum for discussing security and e-communication networks. Similar conferences were held in 2007 and 2008. As far as EETT is concerned, there are no such initiatives between providers and public authorities. Similar initiatives among providers are not known. ADAE's conference findings are so far shared with those attending only.

Awareness actions against harmful content distributed through the Internet and other New Media

The Greek awareness node **SafeNetHome**, www.saferinternet.gr, is the Greek node for public awareness against harmful content distributed through the Internet and other New Media. **SafeNetHome** is a member of Insafe¹¹.

The goal of **SafeNetHome** is the design and implementation of a hard-hitting awareness campaign in Greece for different target groups about the potential dangers lying in illegal and harmful content on the Internet but also in mobile and emerging technologies. The campaign has been implemented based on the slogan '**Saferinternet ... together**', inviting every member of the society to contribute in making the Internet and all new technologies safe for all consumers, but especially for kids and youngsters. The campaign focuses on parents, educators and kids, but is also addressing public authorities, the government and the media.

¹¹ See : www.saferinternet.org

Awareness actions against spam

The website of the Hellenic Data Protection Authority (HDP, which is the responsible authority for dealing with unsolicited communication) contains awareness information on spam, including advice on how to protect against spam and on how to file a complaint in case they are victims of spamming. Currently the HDP is considering the adoption of guidelines/recommendations for the ISPs in four main directions:

- General policy and customer awareness measures;
- Measures against outgoing spam;
- Measures against ingoing spam and;
- Cooperation measures among ISPs.

The HDP has organised a consultation with major Greek Internet service providers to discuss the problems caused to their service by spam emails. As a result the HDP is preparing a recommendation.

Awareness actions undertaken by the Greek service providers and banking sector

The Greek service providers have a code of conduct for online advertising. Several service providers have awareness information on their website and offer spam filters, use black lists, etc. One service provider actually offers a personalised anti-spamming service, which can be activated/deactivated according to the wishes of the service and offers the creation of personal white and black lists.

The mobile provider Vodafone Greece published a mobile telephony guide for parents with a part on spam, in which customers are urged to contact the service centre to allow spot the spammer.

The Hellenic Bank Association web page maintains a specific section¹² on Internet banking usage risks.

Awareness actions targeting the consumers/citizens

The objectives of the Greek Awareness Centre are to:

- Raise awareness about all kinds of unsuitable, harmful or illegal content and activities;
- Promote the positive aspects of the online technologies as means of enhancing the quality of our daily life;
- Educate parents and teachers about the safe use of the Internet, ensuring that they are aware of both benefits and risks;
- Encourage dialogue between minors and parents on media use and safety issues, promote media literacy and critical thinking;
- Support (grand-) parents and educators to help children in becoming responsible users of the new technologies;
- Closely work with the government, industry, law enforcement, and NGOs to make online worlds safer places;
- Establish the Greek helpline.

One of the main objectives of the Greek node is to use the Internet in order to promote safety advice, and thus conduct awareness about the medium through the medium.

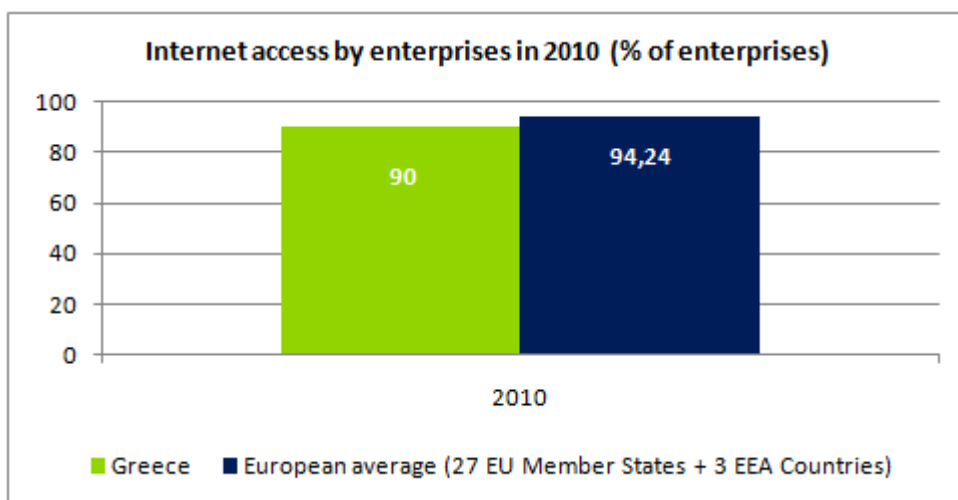
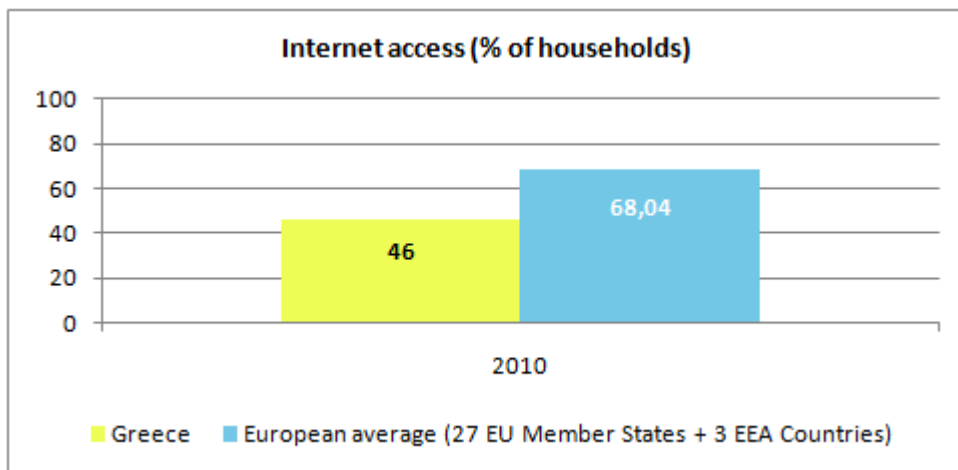
¹² See: <http://www.hba.gr/e-banking2005/index.htm>

Relevant statistics for the country

In order to provide the reader with additional information about the relative stage of NIS development in Greece, a series of relevant statistics are included in this section. Some of them indicate that the information society in Greece still needs some improvement, while others show progress and interesting trends.

Internet access of population and enterprises

The following graphs, based on Eurostat information, provide an overview of the situation¹³ of Internet access in Greece for enterprises and respectively households, relative to the European average.

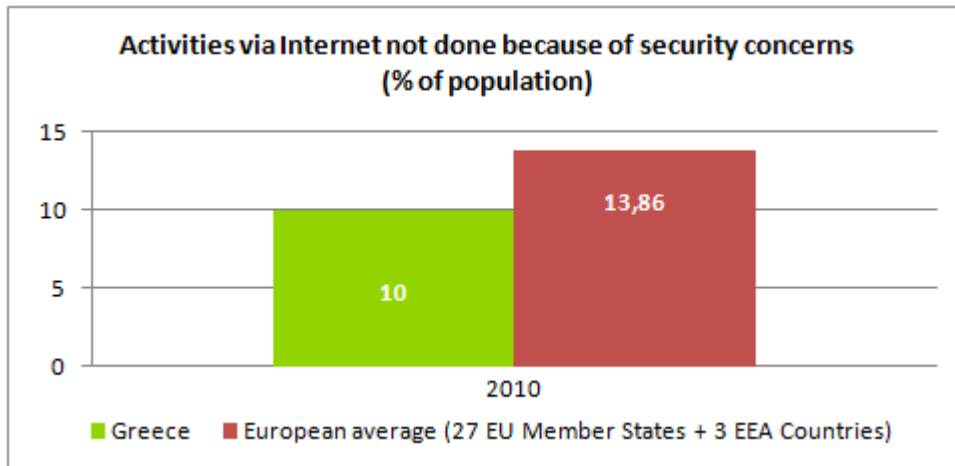


In 2010, the statistics indicate that the enterprises in Greece have almost the same level of Internet access as the European average, while more effort is required to close the gap on the households.

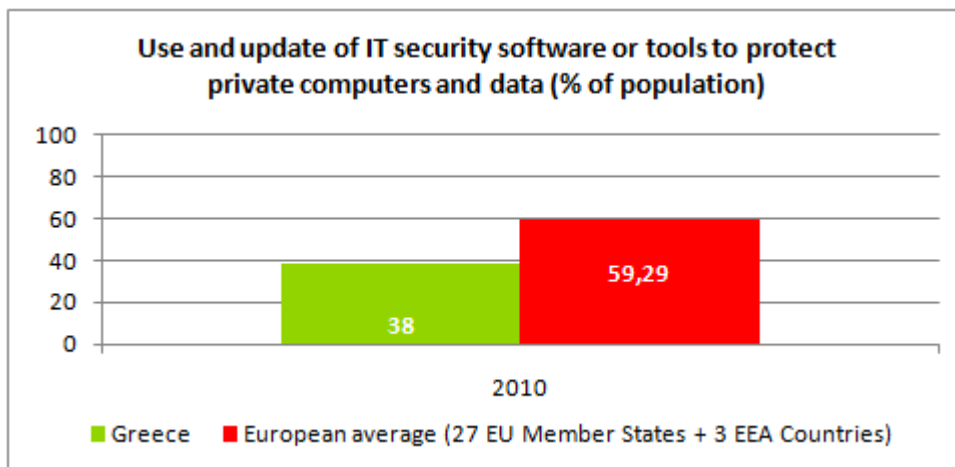
¹³ Source: Eurostat

Statistics on use of Internet by individuals and related security aspects

The percentage of population in Greece that is reluctant in performing activities via Internet (e.g. e-banking, purchases of goods and services over Internet, etc.) because of security concerns is slightly below the European average:



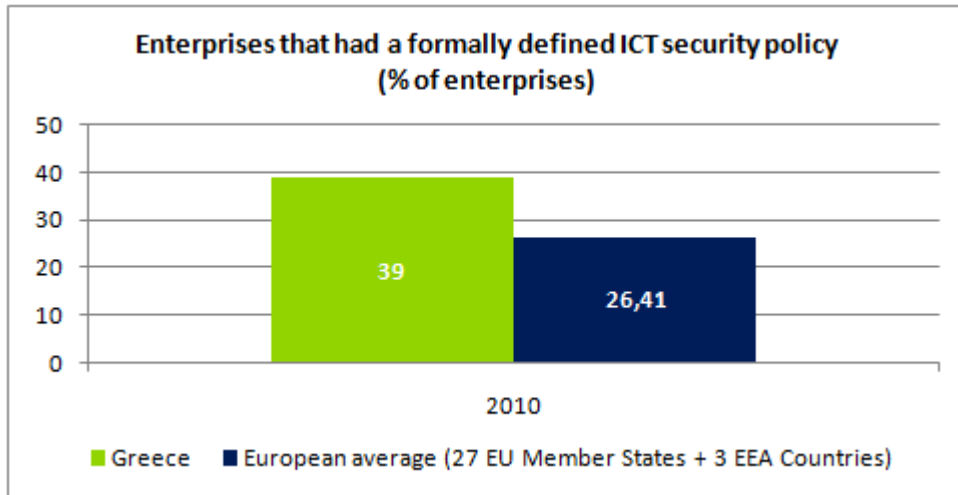
This can be an indication of either more confidence in web-based transactions or of less awareness of the general public regarding IT threats.



Meanwhile, it appears that the use of security tools to protect private computers and data is below the European average.

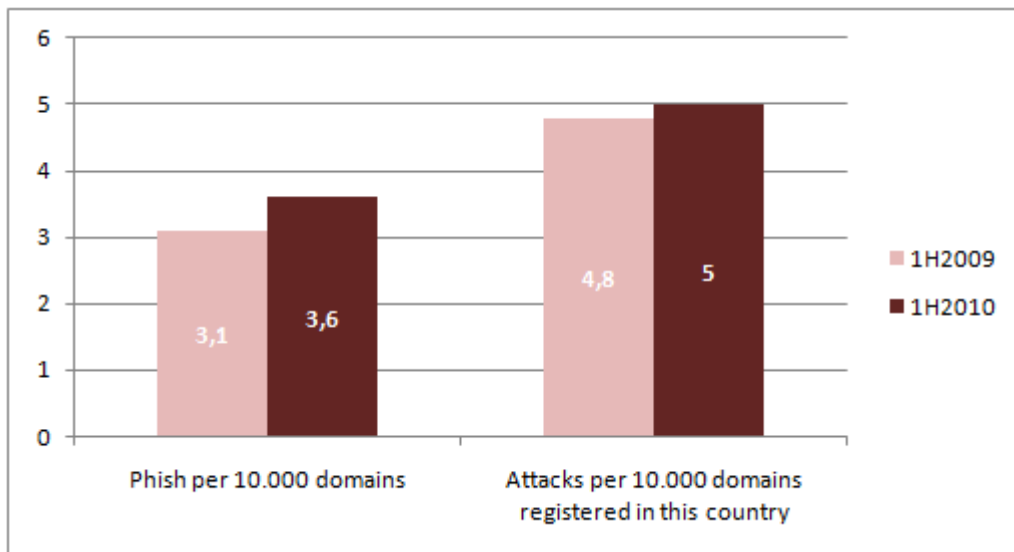
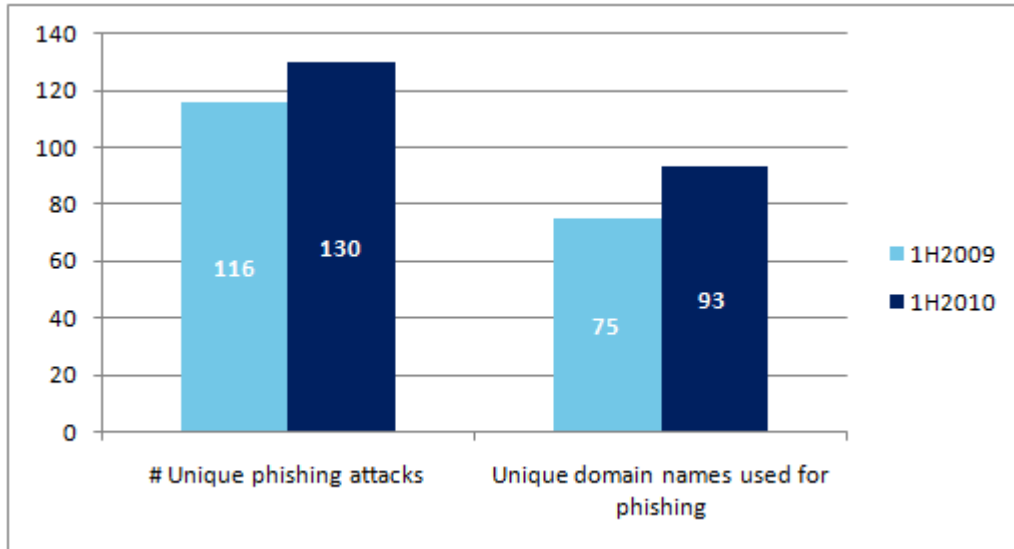
Statistics on use of Internet by enterprises and related security aspects

More enterprises in Greece have a formally defined ICT security policy, compared with their European peers. See below:



Other Statistics

It is interesting to also mention that during the 1st half of 2010, and respectively for the 1st half of 2009, Greece was mentioned in the global report¹⁴ published by the Anti-Phishing Working Group (APWG) with the following relevant statistics:



¹⁴ See: *Global Phishing Survey: Trends and Domain Name Use 1H2010*, available at: http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_1H2010.pdf

APPENDIX

National authorities in network and information security: role and responsibilities

National authorities	Role and responsibilities	Website
1. Ministry of Infrastructure, Transport and Networks (government)	<p>Its role is to define the policy guidelines, institutional and regulatory framework regarding the development of high-quality (transport) and electronic communications services in a competitive environment.</p> <p>Areas of responsibility in the electronic communications field:</p> <ul style="list-style-type: none"> • Definition of ICT strategy • Enactment of ICT technical regulations. <p>NIS is not dedicated on a special unit or department of this Ministry. However, a new legislation under development provisions for a separate Ministry department with NIS responsibilities; moreover, the Ministry is in principle competent for policy and regulation in areas such as FTTx (Fiber to the Home – Fiber to the Building), digital television, broadband penetration, unified communications as well as for technical regulations in relation to the establishment of electronic communications networks inside and outside of buildings, etc., either on its own or together with other Greek ministries. It should be noted that any proposal of EETT (the regulatory authority in the electronic communications area) has to be approved by the Ministry in order to be enacted as ministerial decision, presidential decree or regulation.</p>	www.yme.gov.gr
2. General Secretariat for Public Administration and Electronic Governance Ministry of Interiors, Decentralisation and Electronic Governance (government)	<p>Having as main goal the simplification of administration and governmental services offered to Greek citizens through the use of automated (internet-based) means, the GSPA defines the national e-government strategy within 3 main activity axes:</p> <ul style="list-style-type: none"> • Definition & follow-up of all initiatives, actions and projects of the national program "Information Society" that relate to the promotion of e-government services; • Management of the program "politeia": The main aim through this program is to develop and modernize the simplification of administrative procedures that delay the provision of public services to the citizen. 	www.gspa.gr
3. General Secretariat for Information Systems – Ministry of Finance (government)	<p>Design and implementation of information systems for tax offices. The General Secretariat is competent of the security issues in the implementation and functioning of Taxis (the digital on-line system for the submission of tax declarations on-line).</p>	www.qsis.gr
4. General Secretariat for Research and Technology – Ministry of Education, Lifelong Learning and Religious Affairs (government)	<p>The General Secretariat for Research and Technology of the Ministry of Education, Lifelong Learning and Religious Affairs:</p> <ul style="list-style-type: none"> • Supports through its programmes, the research activities of both the country's scientific research institutes and those of its productive industry, focussing on areas that are important for the national economy and for the improvement of the quality of life; • Promotes the transfer and dissemination of 	www.gsrt.gr

National authorities	Role and responsibilities	Website
	<p>advanced technologies throughout the country's productive sector, thus ensuring early utilisation of the results of research activity;</p> <ul style="list-style-type: none"> • Contributes to the reinforcement of the country's research manpower; • Represents Greece in relevant institutions of the European Union, thus bringing the country's research and technology activities into line with the requirements of the international community; • Promotes cooperation with other countries and international organisations on research and technology issues; • Establishes new institutes and technological centres in support of sectors of high priority for the development of the Greek economy; • Supervises underwrites the fixed costs of, and otherwise provides support for 21 of the country's best-known research and technological centres; • Supports the dissemination of research and technology information throughout the country and internationally by means of advanced IT systems and networks; • Encourages activities aimed at raising awareness of the general public about research and technology issues. 	
<p>5. EETT – Hellenic National Telecommunications and Post Commission</p>	<p>The EETT is the national regulatory authority, which regulates, supervises and monitors the electronic communications and postal services market in Greece.</p> <p>The role of EETT is to:</p> <ul style="list-style-type: none"> • Ensure the access of all in a great range of communication networks and services; • Safeguard the rights of the consumers of telecommunication and postal services; • Inform the consumers of their rights and obligations; • Secure the utilization of scarce national resources, such as the spectrum of radio frequencies and the numbering resources. • Ensure implementation of regulation by electronic communication operators through guidance, organisation of public consultations and market supervision. <p>They contribute to the development of the telecommunication and postal services markets by creating a regulatory environment according to the principles of competition</p>	<p>www.eett.gr</p>
<p>6. ADAE (Hellenic Authority for Communication Privacy)</p>	<p>The Hellenic Authority for Communication security and communications privacy is an authority with administrative independency responsible for ensuring network security and integrity through compliance controls and regulatory enforcement. Oversight authority for the implementation of security policies with the electronic communications operators to protect communications secrecy and confidentiality.</p>	<p>www.adae.gr</p>
<p>Hellenic Data Protection Authority (HDPA)</p>	<p>The primary goal of the HDPA is the protection of citizens from the unlawful processing of their personal data and their assistance in case it is established that their rights have been violated in any sector (financial, health, insurance, education, public administration, transport, mass media, etc).</p> <p>The second main goal of the HDPA is to offer</p>	<p>www.dpa.gr</p>

National authorities	Role and responsibilities	Website
	support and guidance to controllers in their effort to comply with their obligations vis-à-vis the Law, while taking into account the needs of the services in the Greek society, as well as the growing use of modern digital communications and networks. As a result of the above, the HDPA focuses, among others, on the identification and solution of problems which arise from the advancements of new technologies and their applications.	
7. National Intelligence Service (EYP)	The National Intelligence service is in charge of : <ul style="list-style-type: none"> • Collecting, processing and disclosure of intelligence to all competent authorities. • To serve as National Authority Against Electronic Attacks, competent for preventing and statically and actively dealing with electronic attacks against communication networks, information storage facilities and computer systems. • To serve as Information Security Technical Authority (INFOSEC) and procure, pursuant to the provisions of the security of national communications and information technology systems, as well as the certification of classified national communications material. The certification shall be given against the payment of a fee, the level of which shall be determined by joint resolution of the Ministers of Interiors, Decentralization & Electronic Governance and Ministry of Finance. 	www.nis.gr
8. National Authority Against Electronic Attacks (NAAEA) – National CERT	The National Authority Against Electronic Attacks is the agency responsible for encountering-protecting the Public Sector along with the Critical National Infrastructures as established by Law 3469/2008 and Presidential Decree 126/2009	http://www.cert.gov.gr
9. Hellenic Police - Electronic Crime Department	No specific description available.	http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=1763&Itemid=378
10. Digital Awareness & Responses to Threats (DART)	The Digital Awareness & Responses to Threats (DART) team is a task force on Digital Security. The immediate objective of the team is to inform citizens, prevent and address risks associated with the new technologies and electronic communications.	http://www.dart.gov.gr/
11. Centre for Security Studies (KEMEA)	The Centre for Security Studies is a consulting body, that aids, supports and fortifies competent state bodies in planning and implementing projects to best deal with today`s security threats as well as traditional forms of crime, through the provision of studies, analysis and investigations in these issues always including feasible solutions.	http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=1402&Itemid=416&lang=en

Computer Emergency Response Teams (CERTs)

CERT	Role and responsibilities	Website
	<ul style="list-style-type: none"> FIRST15 member TI16 listed 	
12. AUTH-CERT	<p>AUTH-CERT is the Aristotle University of Thessaloniki CERT.</p> <ul style="list-style-type: none"> Not FIRST member; TI listed 	http://cert.auth.gr/index.php?&newlang=eng
13. GRNET-CERT	<p>GRNET-CERT is the Greek Research and Technology Network Computer Emergency Response Team. It is operated and staffed by the University of the Aegean.</p> <ul style="list-style-type: none"> Not FIRST member; TI listed 	http://cert.grnet.gr/grnetcert_english.php
14. FORTH CERT	<p>FORTH-CERT is the Foundation for Research and Technology, Hellas, CERT.</p> <ul style="list-style-type: none"> FIRST member; TI listed 	www.forth.gr/forthcert/

Industry organisations active in network and information security

Industry Organisations	Role and responsibilities	Website
15. SEPE (Federation of Hellenic Information Technology & Communications Enterprises)	<p>Over 400 companies are currently members of SEPE and collectively they hold more than 95 % of the country's turnover in the Information Technology and Telecommunication Industry. The main objectives of SEPE are to promote Information and Communications Technologies (ICT) in Greece and to enlarge ICT Industry's market.</p> <p>SEPE also represents the interests of the Greek ICT Enterprises vis-à-vis the Greek Government, the European Commission and other bodies of influence.</p>	www.sepe.gr
16. SEPVE (Association of Information Technology Companies of Northern Greece)	<p>SEPVE numbers more than 240 member enterprises. Over the 17 years since its foundation the association has organised a significant number of events, training seminars, conferences and forums, while taking part in an even larger number of such events organised by other associations and agencies. SEPVE has also focused on organising business delegations to countries in south-eastern Europe.</p>	www.sepve.org.gr
17. SATPE (Greek Licensed Telecommunication Providers Association)	<p>This Association aims at defending the interests of the major stakeholders of electronic communications networks and services of the Greek market as actively present in all fora and public initiatives in the area of electronic communications.</p>	www.satpe.gr
18. The South Eastern Europe Telecommunication & Informatics Research Institute	<p>Created as an initiative of the major telecommunications and informatics companies of Greece (OTE, Intracom, Hellascom, Nokia, etc.) , INA is an organization designed to facilitate investment in the region's telecom and informatics markets by analysing regional market trends, enhancing the exchange of technological expertise and helping to develop a regulatory framework for the regions telecom markets.</p>	www.inatelecom.org

¹⁵ <http://www.first.org/members/teams/>

¹⁶ <http://www.trusted-introducer.nl/>

Academic organisations active in network and information security bodies

Academic Organisations	Role and responsibilities	Website
19. ICS-FORTH (Institute for Computer Science — Foundation For Research and Technology)	The Institute of Computer Science (ICS) is one the seven institutes of the Foundation for Research and Technology - Hellas (FORTH), a major national research centre partly funded by the General Secretariat for Research and Technology of the Hellenic Ministry of Education, Lifelong Learning and Religious Affairs. The mission of FORTH-ICS is to perform high quality basic and applied research, to promote education and training, and to contribute to the development of the Information Society, at a regional, national, and European level. FORTH-ICS comprises laboratories, each of which conducts basic and applied research in thematic areas in the field of Information and Communication Technologies.	www.ics.forth.gr
20. GRNET (Greek Research and Technology Network)	Network development and NIS research.	www.grnet.gr
21. Research Academic Computer Technology Institute (RA-CTI)	The Research Academic Computer Technology Institute is mainly involved with fundamental and applied research activities. The principal areas of activity on which RA CTI concentrates its research efforts are: Algorithm Analysis and Design, Advanced Parallel Computer Architectures, Networks and Distributed Computing, Natural Language Processing, Signal Processing and Digital Image Processing, Software Technology, High Performance Computing, Educational Technology and Database Management. The applied research performed by RA CTI is focus mainly in areas such as Geographic Information Systems, Multimedia, User Environments, Telematics Services, Information and Communication Technologies in Education, Medical Informatics, Expert Systems Design and Optimisation of Industrial Production.	www.cti.gr
22. Research Centre Demokritos (N.S.C.R Demokritos)	The main mission of the Research Centre Demokritos remains: <ul style="list-style-type: none"> • The carrying out of high class, basic, applied, and developmental research aiming at the generation of new knowledge and technology; • The conveyance of new knowledge and technology to others and the formation of know-how for the resolution of specific financial and social development problems.; • The provision of specialized high technology services to both private and public institutions of the country. • The education and specialization of new scientists in new technologies and their familiarization with the generation of new knowledge; • The coordinated undertaking of research work of national importance. 	www.demokritos.gr
23. Laboratory of Information & Communication Systems Security - University of the Aegean	Research in Information & Communication Systems Security, participating in a number of national and international security projects	http://www.icsd.aegean.gr/group/index.php?group=L1

Academic Organisations	Role and responsibilities	Website
24. Information Security and Critical Infrastructure Protection Research Group – Athens University of Economics and Business (AUEB)	Research in Information Security & Critical Infrastructure Protection, participating in a number of national and international security projects	www.cis.aueb.gr/
25. Telecommunication Networks and Integrated Services Laboratory, Department of Digital Systems – University of Piraeus (UniPi)	Research in Telecommunications & related Services, and Information Security	http://tns.ted.unipi.gr/

Other bodies and organisations active in network and information security

Others	Role and responsibilities	Website
26. SafeNetHome	Part of the European 'Insafe' Internet safety network under the 'Safer Internet' programme which aims to promote safer use of the Internet and new online technologies, particularly for children, and to fight against illegal content and content unwanted by the end-user, as part of a coherent approach by the European Union	www.saferInternet.gr
27. SafeLine	SafeLine cooperates with Internet service providers, the national academic network 'GRNET' and the national school network, research and cultural Institutions, consumer organisations and the Greek Police, on restricting the flow of illegal content on the Internet. Co-funded by the European Union 'Safer Internet' action plan, SafeLine is managed by SAFENET, the collective body of ISPs in Greece	www.safeline.gr
28. Information Society in Greece	The Greek IS portal; includes the Information Technology Committee and the institutional bodies responsible for IS.	www.infosoc.gr
29. Observatory for the Greek Information Society	It aims at collecting and assessing quantitative and qualitative data on issues regarding the Information Society in Greece, diffusing best practices, as well as conducting relevant studies and contributing to the policy formulation processes to the Greek Government and any other party interested. The strategic objectives of the Observatory for the Greek Information Society are the following: <ul style="list-style-type: none"> • Reliable and on time validation of the quantitative and qualitative data as regards the progress made towards the IS; • Improvement of the level of information on which the national strategy and actions are based as regards the IS; • Transfer and diffusion of best practices and assistance in the exchange of experience, technical expertise and information among agencies in Greece and abroad. 	www.observatory.gr
30. ISACA Athens Chapter	ISACA is a worldwide association of IS professionals dedicated to the knowledge and good practices regarding audit, control, and security of information systems. The chapter in Greece organizes local events such as education and training, workshops, roundtables and other	www.isaca.gr

Others	Role and responsibilities	Website
	specific events.	
31. INKA (General Consumers' Federation of Greece)	A consumer organisation, its aim is to protect and educate consumers.	www.inka.gr
32. KEPKA (Consumers' Protection Centre)	A consumer organisation, its aim is to protect and educate consumers.	www.kepka.org
33. Athena- Research and innovation centre in information, Communication and knowledge Technologies	<p>The Research and Innovation Centre in Information, Communication and Knowledge Technologies ("Athena") is a research and technology body, which was founded under the auspices of the Ministry of Development in 2001. The objectives of the RC Athena are:</p> <ul style="list-style-type: none"> • The promotion of innovative information and communication technologies in the industrial and in the services sector; • The development of scientific and technological research and its implementation and exploitation of results in the sectors of information technology, knowledge, communication and automating production processes aiming at the production of laboratory prototype products and services; • The creation of development activities in the same sectors and in their applications; • Lifelong learning and training in the respective sectors; • The management of financing programmes supporting businesses that act in its sector and promote state research and technology policies. 	www.athena-innovation.gr

References

- An overview of the eGovernment and eInclusion situation in Europe, available at <http://www.epractice.eu/en/factsheets>
- ENISA, Information security awareness in financial organisations, November 2008, available at http://www.enisa.europa.eu/doc/pdf/deliverables/is_awareness_financial_organisations.pdf
- Greece - ENISA CERT Directory: <http://www.enisa.europa.eu/act/cert/background/inv/certs-by-country/greece>
- ICS-FORTH Presentation "Security and Privacy in a Networked and Mobile World" available at: <http://www.ict-forward.eu/media/publications/fidis2008-presentation-forward.pdf>

