

Slovenia 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 and Bogdan G. Petre.**

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.

Table of Contents

SLOVENIA	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	7
NIS GOVERNANCE	12
OVERVIEW OF THE KEY STAKEHOLDERS	12
INTERACTION BETWEEN KEY STAKEHOLDERS, INFORMATION EXCHANGE MECHANISMS IN PLACE, CO-OPERATION & DIALOGUE PLATFORMS AROUND NIS	13
FOSTERING A PROACTIVE NIS COMMUNITY	16
COUNTRY-SPECIFIC NIS FACTS, TRENDS, GOOD PRACTICES AND INSPIRING CASES....	18
SECURITY INCIDENT MANAGEMENT	18
EMERGING NIS RISKS	18
RESILIENCE ASPECTS	19
PRIVACY AND TRUST	20
NIS AWARENESS AT THE COUNTRY LEVEL	22
COUNTRY-SPECIFIC ACTIVITIES FOR IDENTIFYING AND PROMOTING ECONOMICALLY EFFICIENT APPROACHES TO INFORMATION SECURITY	24
INTERDEPENDENCIES, INTERCONNECTION AND IMPROVING CRITICAL INFORMATION INFRASTRUCTURE PROTECTION	24
RELEVANT STATISTICS FOR THE COUNTRY	25
INTERNET ACCESS OF POPULATION AND ENTERPRISES	25
STATISTICS ON USE OF INTERNET BY INDIVIDUALS AND RELATED SECURITY ASPECTS	26
STATISTICS ON USE OF INTERNET BY ENTERPRISES AND RELATED SECURITY ASPECTS	27
OTHER STATISTICS	28
APPENDIX	29
NATIONAL AUTHORITIES IN NETWORK AND INFORMATION SECURITY: ROLE AND RESPONSIBILITIES	29
COMPUTER EMERGENCY RESPONSE TEAMS (CERTs)	30
INDUSTRY ORGANISATIONS ACTIVE IN NETWORK AND INFORMATION SECURITY	31
ACADEMIC ORGANISATIONS ACTIVE IN NETWORK AND INFORMATION SECURITY BODIES	31
OTHER BODIES AND ORGANISATIONS ACTIVE IN NETWORK AND INFORMATION SECURITY	32
REFERENCES	33

Slovenia

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

On 23 July 2010, the Representation Office of the European Commission in Slovenia organised a conference in cooperation with the European Commission's Directorate General for the Information Society on the Digital Agenda, one of the initiatives under the European Commission's Europe 2020 Strategy. The representant of Slovenia's ICT sector, outlined the following measures and future goals:

- Improve digital literacy, knowledge and involvement;
- Develop ICT solutions to promote digital literacy amongst disadvantaged groups;
- Spread awareness of the importance and usefulness of ICT skills and competencies;
- Implement training of digital literacy skills and competencies for the elderly;
- Incorporate eLearning in a national policy.

The current strategic framework for the development of eGovernment in Slovenia comprises following key documents:

- Slovenia's Development Strategy, adopted on 23 June 2005;
- eGovernment Strategy of the Republic of Slovenia for the period 2006 to 2010 (SEP-2010 "eGovernment for effective Public Administration"), adopted on 20 April 2006;
- Action Plan for eGovernment for the period 2006 to 2010, adopted in February 2007;
- Strategy on IT and electronic services development and connection of official records (SREP).

Slovenia's Development Strategy (2006-2013)

One of the key national development objectives of the Slovenia's Development Strategy 2006-2013¹ (*Strategija razvoja Slovenije*) is to improve the quality of living and welfare of all citizens through inclusion, and access to education and training by using ICT-supported regional/local centres of lifelong learning. Among the measures introduced were to increase the use of ICT and related services in households with the launch of the pilot scheme Home Computer Initiative.

eGovernment Strategy for the period 2006 to 2010 (SEP-2010)

Entitled 'eGovernment for effective Public Administration', the Slovene eGovernment strategy (hereafter 'SEP-2010')² presents a strategic vision for the development of eGovernment in Slovenia and outlines the main actions to be taken in this area in the period 2006 to 2010.

This document was prepared for the Slovenian Government by an inter-agency project group working within the Ministry of Public Administration. In developing the strategy, the group drew on experiences from other national eGovernment plans, as well as from EU strategies and guidelines.

The purpose of SEP-2010 is to determine a framework and goals leading to the further realisation of new and already established eGovernment activities, laying emphasis on user satisfaction,

¹ The Slovenia's Development Strategy 2006-2013 available at http://www.slovenijajutri.gov.si/fileadmin/urednik/dokumenti/Slovenia_s_Development_Strategy.pdf

² The eGovernment Strategy of the Republic of Slovenia for the period 2006 to 2010 available at http://www.mju.gov.si/fileadmin/mju.gov.si/pageuploads/mju_dokumenti/english/SEP2010_english_final.doc

rationalisation of administrative operations and modern electronic services, so as to enable a higher quality of life and give administration a friendlier face when in contact with users.

Action Plan for eGovernment for the period 2006 to 2010

A central element of the SEP-2010 strategy is the Action Plan adopted in February 2007³. Its primary aim is to give concrete form to the implementation and monitoring of the SEP-2010 eGovernment strategy in Slovenia. It describes in a more detailed manner the actions announced in the strategy for reaching the targets set for 2010.

Covering all eGovernment projects and eServices put forward in SEP-2010, the Action Plan also provides detailed updates on the progress made so far. It also includes instances of good practice and a general overview of the advancement of eGovernment in Slovenia, comparing it with progress made in other parts of the European Union.

To ensure transparency, particular care was taken in selecting the most appropriate processes, organisational and technological solutions and tools to be used throughout the plan. These are essential for the successful development of eGovernment in the future. They also allow for mistakes which occur while developing new eServices to be corrected along the way, taking account of European and international standards.

Another goal of the Action Plan is to give a new impetus to the development of eServices that are considered necessary but which so far have been delayed; special focus is to be placed on services based on joint EU projects -using a shared architecture and common European standards- as well as those necessary for the internal functioning of the Slovenian Government.

Strategy on IT and electronic services development and connection of official records (SREP)

This strategy is enabling the balanced development of the IT public administration and electronic services, and the integration of solutions and best practices from eAdministration into other spheres of civil service work.

The strategy aims to lay down a framework and steps for the further development of IT and electronic services in Public Administration, introducing advanced approaches and a crucial shift in understanding the importance of eServices, with a view to overcoming current issues that hinder their development.

Strategy for the development of the Information Society in the Republic of Slovenia until 2010 (si2010)

The "Development strategy for the information society in the Republic of Slovenia - si2010" is only a development strategy. Although it certainly calls attention to most of the relevant NIS related problems it does not provide immediate solutions at the same time.

The structure of the si2010 strategy complies with the i2010 guidelines, enabling a clear connection between EU and national priority tasks. The strategy comprises three basic areas of implementing measures (verticals) which relate to the basic i2010 priority tasks, and six operating principles – each from the aspect of an individual challenge – (horizontal).

³ The Action Plan for eGovernment for the period 2006 to 2010 available at http://e-uprava.gov.si/eud/e-uprava/akcijski_nacr_e-uprave_2010.doc

With regard to the strategy, the common strategic goals of the si2010 strategy have been determined:

- **Single European Information space and Slovenia:** broadband accessibility to allow the population access to the broadband electronic communications network; transition from analogue to digital broadcasting carry out the transition from analogue to digital broadcasting; e-business provide the infrastructure to allow the introduction and use of e-business in all companies and institutions in Slovenia.
- **Innovations and Investments in ICT:** Scientific research infrastructure establish the research and educational infrastructure for high-capacity connections; technological platforms establish an efficient research environment which fosters collaboration between research institutions, the economy and users of ICT; R&D and implementation projects support for R&D activities in ICT aimed at developing globally competitive innovative products and services; Supporting the development of solutions based on open code provide adequate development and introduction of solutions based on the open source principle, in all spheres of public interest; European programmes support successful collaboration of Slovenian partners in European programmes.

Slovenia has under preparation a National Development Programme of the Information Society 2011-2015. Six priorities of the programme areas are:

- Information Society in support of sustainable development
- Strengthening the research, innovation and business potential
- NGNs for cohesive society
- Inclusion of all in a creative society
- User-friendly public services
- Security, privacy and trust

The regulatory framework

eGovernment Legislation

Since the beginning of 2010 there is currently no overall eGovernment legislation in Slovenia. The General Administrative Procedure Act (Official Gazette of the Republic of Slovenia, no. 24/2006-ZUPUB2), adopted in 1999 and several times amended, with its last amendment dating in 2006, provides the general legal basis for all administrative proceedings and relations.

Among the main provisions of the act is one allowing for a two-way and full electronic communication between public administration and citizens. Prior to entering this text into force, citizens could post their eDocuments through the eServices of the eGovernment state portal by using the web application and digital signature; the answer from the administration could be expressed by regular mail only. In 2004 and in later amendments, this Act legalised what is qualified as "eDelivery".

eCommunications Legislation

Electronic Communications Act

The Electronic Communications Act was adopted in March 2004 and came into force on 1 May 2004. It was lastly amended in 2009. The Act aims to establish effective competition in the electronic communications market, maintain effective use of the radio frequency spectrum and of the number space, ensure universal services and protect the user's rights.

This Act encompasses all relevant issues that are separately dealt with by the EU directives forming the so-called EU Regulatory Framework for Electronic Communications, namely: Directive

2002/21/EC (Framework Directive); 2002/20/EC (Authorisation Directive); 2002/19/EC (Access and interconnection Directive); 2002/22/EC (Universal service and user's rights Directive); and 2002/58/EC (ePrivacy Directive). Also through the Act the Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communication services or of public communication networks is transposed.

Reports on Electronic Communications Act violations are handled by the Agency for Post and Electronic Communications (*Agencija za pošto in elektronske komunikacije - APEK*).

For SPAM the Article 109 (3) States: *§1 Electronic Communications Act: Use of electronic mail for the purpose of direct marketing is only allowed if the subscribers have given their prior consent. Sanction: A fine between EUR 50,000 and EUR 400,000 for legal entities (defined in Article 152)*

eCommerce Legislation

Act amending the Electronic Commerce and Electronic Signature Act ⁴

The initial version of the Electronic Commerce and Electronic Signature Act (ZEPEP) was adopted by the Slovenian Parliament on 13 June 2000 and came into force on 22 August 2000. It provides the legal basis for using eSignatures and developing eServices in Slovenia. This Act amending the Electronic Commerce and Electronic Signature Act, adopted in April 2004, defines more precisely the responsibilities of providers of Information Society services and sets the conditions for the realisation of the electronic identity card project.

Being a horizontal bill regulating eCommerce in a broader sense, this Act also applies to administrative, judicial and other similar procedures unless otherwise provided by a different law. The Electronic Commerce Market Act (ECMA) was adopted in 2006 and amended in 2009, and is in line with the Directive 2000/31/EC. ECMA regulates issues regarding establishment of service providers, commercial communication, contracts concluded by electronic means, responsibility of service providers, codes of conduct, dispute settlement, court actions and cooperation among member states. ECMA also derogated some provision regarding issues that had been regulated in the Electronic Commerce and Electronic Signature Act till enforcement of ECMA.

Cybercrime legislation

Slovenian criminal law identifies the following conduct related to cybercrime:

- abuse of personal data acquired by breaking into a computerised data bank;
- unauthorised entry or intrusion into a computer system and;
- development and implementation of tools intended for such intrusions.

The substantive criminal law is mostly in line with provisions of the Council of Europe Cybercrime Convention. However, there are problems especially regarding the illogical use of some provisions of the Criminal code due to the special nature of cybercrime.

Several articles of the Slovenian Criminal Code are of relevance for the NIS. Some regulations were introduced like for example:

- *Malicious code* - Article 309, §3 Criminal Code: Possession, manufacturing, selling, making available for use, importing, exporting or in any other way providing devices for breaking

⁴ The Act amending the Electronic Commerce and Electronic Signature Act available at <http://www.uradni-list.si/1/objava.jsp?urlid=200425&stevilka=1066>

into or unlawfully entering an information system with intent to commit a criminal offence. Sanction: imprisonment of up to 1 year;

- *Denial of service* - Article 225, § 2 Criminal Code: Obstructing transfer of data or operation of an information system without authorisation. Sanction: imprisonment of up to 2 years. If the offence resulted in a large loss of property, the penalty is raised to imprisonment from 3 months up to 5 years;
- *Denial of service* - Article 242, § 1 Criminal Code: Obstructing transfer of data or operation of an information system (in the course of business operations and without authorization) in order to obtain unlawful pecuniary benefit, or to cause pecuniary damage to another. Sanction: Imprisonment of up to 3 years. If the offence resulted in a large loss of property or a large property benefit (or if such was the perpetrators intent), the penalty is raised to imprisonment of up to 5 years;
- *Intrusion attempt* - Article 225, §3 Criminal Code: Attempt to perform a criminal offence as defined in Article 225, §2. Sanction: imprisonment of up to 2 years. If the offence resulted in a large loss of property, the penalty is raised to imprisonment from 3 months up to 5 years;
- *Unauthorised access to information* - Article 154, § 2 Criminal Code: Breaking into a computer database in order to acquire personal data. Sanction: A fine or imprisonment of up to 1 year;
- *Unauthorised access to information* - Article 225, §2 Criminal Code: Use without authorisation of data held in an information system. Sanction: imprisonment of up to 2 years. If the offence resulted in a large loss of property, the penalty is raised to imprisonment from 3 months up to 5 years.

eSignatures Legislation

Since the beginning of 2010 no significant changes were recorded regarding the eSignature Legislation.

Electronic Commerce and Electronic Signature Act

The initial version of the Electronic Commerce and Electronic Signature Act (ZEPEP) was adopted by the Slovenian Parliament on 13 June 2000 and it provides the legal basis for using eSignatures and developing eServices in Slovenia.

This Act amending the Electronic Commerce and Electronic Signature Act, adopted in April 2004, more precisely defines the responsibilities of providers of Information Society services and sets the conditions for the realisation of the electronic identity card project.

The Slovenian legislation literally translated the definitions of "advanced" and "qualified" electronic signature of the Directive 1999/93/EC of 13 December 1999 on a Community framework for electronic signatures. However, the word "secure" is used for referring to an advanced signature. As defined in the Act, the devices for secure electronic signing should comply with special conditions regarding security and reliability.

In accordance with the Directive, electronic signatures for internal government applications must be secured by qualified certificates issued by one of the Certification Authorities at the Ministry of Public Administration.

Decree on Administrative Operations

This decree was adopted in 2005 and has been amended several times since then, lastly in 2008. It forms the legal basis for the introduction of eSignatures in eGovernment services and applications (administrative operations). According to this decree, the eGovernment services

operations for citizens and businesses can be performed by any qualified certificates issued by registered Certificate Service Providers (CSPs), governmental CAs and other commercial certification authorities.

eIdentification

The use of electronic identification management (eIDM) systems in the context of eGovernment in Slovenia until 2010 is coordinated reasonably well.

Steps are being taken towards the provisions needed for the development for central information and telecommunications infrastructure for eGovernment including the usage of horizontal integration for authentication processes based on certificates and their implementation or username/passwords (One-Stop-Shop concept).

The use of this infrastructure will enable to achieve lower costs of development and operation of eGovernment, increased quality and uniformity of solutions and interoperability. The main legal framework for the eID systems is laid down in:

- Electronic Commerce and Electronic Signature Act of 13 June 2000, coming into force on 22 August 2000. It provides the legal basis for using e-signatures and developing e-services in Slovenia (Official Gazette of the RS, No. 57/2000, 25/04),
- the Decree on Conditions for Electronic Commerce and Electronic Signing (Official Gazette of the Republic of Slovenia, No. 77/2000 and 2/2001)
- Rules on official registration procedure for certification authorities register of the Republic of Slovenia (Official Gazette of the RS, No. 99-4859/2001)
- Access to Public Information Act (Official Gazette of the RS, No. 51/2006), law on access to information and documents produced by public institutions;
- Personal Data Protection Act (Official Gazette of the RS, No. 86/2004, 113/2005-ZInfP), regulating rights, obligations, principles and measurements to prevent illegal encroachment upon someone's rights with regards to her/his personal data. The databases of the certificates and personal data of their holder are regulated by this act;
- The Central Population Register Act (Official Gazette of the RS, No. 1/1999, 54/2002, 39/2006): Law on central population register and personal number

Regarding the authentication is not especially emphasized by law. There is no regulation with respect to interoperability with other identity management systems (including through international interoperability agreements).

eArchiving Legislation

The Protection of Documents and Archives and Archival Institutions Act and the Regulation on Documentary and Archival Material Custody were both passed in 2006 with the aim to regulate the electronic content management.

All electronic records, including digitalised documents have full legal effect provided they comply with technical conditions. The regulation governs the activities and internal rules for individuals to keep documents and/or archives, the storage of such materials in physical and digital forms, the general conditions, registration and accreditation of digital storage equipment and services, the selection and transfer of archives to public archival institutions, the processing and the keeping of registers of archives, the protection of film and private archives, the use of archives in archival institutions and the work of the Archival Commission. Both acts also contain provisions regarding the long term validity of eSignature.

Self-regulations

Self-regulatory Code of Conduct for Public Mobile Electronic Communications Operators concerning Safer Mobile Use by Younger Teenagers and Children⁵

The Post and Electronic Communications Agency of the Republic of Slovenia, the Association for Information Technology and Telecommunications of the Slovenian Chamber of Commerce and a number of six mobile telecom operators have adopted a code of conduct that describes duties of the signatory members in ensuring minimum protective measures for safer mobile use by children and the under-18s. The Code has been tailored to the needs of the Slovenian mobile electronic telecommunications market and complies with applicable European and national legislation.

Self-regulatory Memorandum of understanding for regulation of hate speech on web media portals

Slovenian hotline Spletno oko and six web media portals have adopted a Memorandum of understanding that describes minimum measures for regulating hate speech on web portals. The Memorandum has also established cooperation between hotline Spletno oko, web portals and other relevant organizations with the aim of tackling the issue of hate speech on internet systematically. Thus, the Memorandum is not only one time event, but presents the start of an on-going process in the field of hate speech regulation. The Memorandum complies with applicable national legislation.

⁵ http://www.gsmeurope.org/documents/eu_codes/Slovenian_code_of_conduct.pdf

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 Higher Education, Science and Technology, Directorate of Information Society • Ministry of Foreign Affairs - Section for Information System Development and Information Security • Ministry of Public Administration, Directorate for e-Government and Administrative Processes • Post and Electronic Communications Agency of the Republic of Slovenia / Agencija za pošto in elektronske komunikacije (APEK) • Slovenian Governmental Certification Authority (SIGOV-CA) • Slovenian General Certification Authority (SIGEN-CA) • The Slovenian Time Stamping Authority (SI-TSA) • Slovene Intelligence and Security Agency (SOVA) • Office for the Protection of Classified Information / Urad Vlade RS za varovanje tajnih podatkov (UVTP) • Information Commissioner / Informacijski Pooblaščenec • Ministry of Interior, Criminal Police Directorate, Computer Crime Section
CERTs	<ul style="list-style-type: none"> • SI-CERT - Slovenian CERT(SI-CERT also provides the role of the Government CERT)
Industry Organisations	<ul style="list-style-type: none"> • Chamber of Commerce and Industry / Gospodarska zbornica Slovenije (GZS) – Association of Informatics and Telecommunications (ZIT) • Slovene Internet Service Provider Association / Sekcija ponudnikov Internet storitev Slovenije (SISPA)
Academic Organisations	<ul style="list-style-type: none"> • Academic and Research Network of Slovenia (ARNES), Ljubljana • Faculty of Social Sciences, University of Ljubljana • Institute of Informatics/ Faculty of Electrical Engineering and Computer Science, University of Maribor • Laboratory for system research and information technologies, Faculty of Computer and Information Science, University of Ljubljana • Laboratory of E-media, Faculty of Computer and Information Science, University of Ljubljana, • Laboratory for Telecommunications, Faculty of Electrical Engineering, University of Ljubljana • Laboratory for Open System and Networks, Jozef Stefan Institute, Ljubljana • Faculty of Organisational Sciences/ University of Maribor • Centre for Legal Informatics (CEPRIS)
Others	<ul style="list-style-type: none"> • Slovene Consumers Association (ZPS) • Spletno-Oko • SAFE-SI • SETCCE (Security Technology Competence Centre), Ljubljana • Cepris (Centre for Legal Informatics), Maribor • IFIT – Institute for forensics of Information Technology, Ljubljana

For contact details of the above-indicated stakeholders we refer to the ENISA "Who is Who"⁶ – 2010 Directory on Network and Information Security and for the CERTs we refer to the ENISA CERT Inventory⁷.

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.

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

Slovenia strategy is to have an interoperability governance and methodology to guide product developments and propagate the use of horizontal services. Within horizontal projects, data is stored in registers and the exact specifications will be defined by the owners of the registers, which publish their own standard.

The application this strategic objective is essential to ensure interoperability between all the institutions of public administration. An action plan was ready at end January 2010 and has an activity scope until 2015, and will be continued after this period. The European interoperability framework (EIF) is seen as an important input.

The Slovenian interoperability Portal is called NIO (National Interoperability Framework) and currently is in the testing phase. NIO will be used for publishing a set of standards and guidelines on interoperability, interoperability information, and systematic Context presentation and display products and interoperability assets. Next to this the portal is supporting the work flow for interoperability assets certification process (support the implementation of the notification procedures, public consultation and commenting on the decision-making on interoperability of products).

Co-operation via the Directorate for the Information Society of the Ministry of Higher Education, Science and Technology

Since the beginning of 2010, The Ministry of Higher Education, Science and Technology, through its Directorate for the Information Society is still the key driver in coordinating the development and implementations activities and programs in the field of the information society, which includes aspects relating to information security, at the national level of Slovenia.

The Directorate is active in the national co-operation in drafting other strategic development documents and monitoring their implementation from the standpoint of the information society:

- National Development Programme for 2004-2006;
- National Development Programme for 2007-2013;
- Development Strategy for Slovenia 2007-2013;
- Monitoring and Evaluation of Regional Development Programmes in terms of the Introduction of Regional Integrated Strategies;

⁶ 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

⁷ <http://www.enisa.europa.eu/act/cert/background/inv/certs-by-country/>

- National Research Programme;
 - Under preparation: the National Development Programme of the Information Society 2011-2015. One of six priority areas is dedicated to Security, Privacy and Trust.

The Directorate for the Information Society is also active in a series of major projects relevant for the NIS domain:

- Information Society Indicators;
- Network of Public Internet Access Points (PIAP): e-schools, e-libraries, MultiMedia Centres (MMC);
- publication of e-government content on public Internet access points, and maintenance of e-point Web site;
- Promotion of the Information Society Development;
- Support to the Introduction of e-Business, promotion of the ICT Sector Development;
- Promotion of e-Content Development in the Republic of Slovenia;
- Distance learning of the Slovenian language;
- Slovenian Intervention Centre for Internet Incidents;
- Prevention of Illegal Use of Software, Web Site Identity of State Administration Authorities;
- Research Programme in the Field of the Information Society – Target Research Programme – Focus 9;
- Slovenia’s Strategy in the Information Society;
- eGOV Pilot (Vinova) – Programme Implementation for Slovenia, etc.
- Co-financing the SAFE-SI project (<http://www.safe.si/>).
- Financing the “Varni na internetu” project (<http://www.varninainternetu.si/>)

In terms of international co-operation, the Directorate is active in participation in working groups of international organisations: eAccessibility (EU), High Level Group on Internet Governance (UN/WSIS), e-Governance (OECD), Membership of and Activities within ERISA on behalf of Slovenian Regional Development Agencies, Council of Europe Working Group on Telecommunications and the Information Society, Council of Europe Working Group on Structural Policy and Regional Development, Participation in Activities for Preparation of WSIS, Group on Safe and Intelligent Transport Systems (EU-DG INFOS e-Safety).

Cooperation of the Post and Electronic Communications Agency of the Republic of Slovenia (APEK) with other competent authorities in the Republic of Slovenia

Within the scope of analysing relevant markets the Post and Electronic Communications Agency of the Republic of Slovenia (APEK) cooperates with the Competition Protection Office, with the Office pursuant to Article 124 of the Electronic Communications Act (ZEKom) regularly providing APEK with opinions on the analyses conducted. Also, APEK provides the Competition Protection Office with professional support during several procedures of establishing abuse of the dominant position in the field of electronic communications.

APEK also cooperates with the Ministry of Higher Education Science and Technology, Directorate for the Information Society in the process of amending the EU electronic communications Regulatory Framework by providing the Directorate with direct professional support. This support was reflected in the cooperation with the working group of the Ministry of Economy, Directorate for Electronic Communications.

The Agency forwarded to the Ministry certain initiatives for legislative amendments (initiatives to amend ZEKom, the initiative to amend the Rules on the Quality of Service for the Single European Emergency Call Number “112”) and assisted the Ministry in the collection of data for the needs of

the annual "112" emergency number implementation questionnaire by processing and forwarding the answers of operators legally obliged in the period in question to report to APEK.

Also APEK forwarded to the Ministry broadband access data for the needs of drafting the document describing the broadband network development strategy in Slovenia.

As part the working group tasked with making available to the hearing-impaired end users the access to the single European emergency number "112", the police telephone number "113" and to certain other public services numbers generally in use, APEK also cooperated with the Ministry of Labour, Family and Social Affairs, Directorate for Disabled.

APEK is cooperating with the Statistical Office of the Republic of Slovenia in the collecting of postal services data and data on the development of the electronic communications market. In accordance with the agreement on providing information adopted in 2006 and due to a change in the method of data collection and retention technically amended in 2008, APEK provides the Statistical Office with operator data in a desire to reduce the administrative burden of operators. APEK also makes use of the data collected by the Statistical Office in its statistical research of households and end users of services.

Additionally, APEK participated in the preparation of answers to the OECD questionnaire on the Slovenian service market regulation and the RCC questionnaire on electronic communications.

APEK attended a Eurostat working group meeting dedicated to the harmonization of definitions and other amendments of the questionnaire used to collect electronic communications data.

For some years now APEK has been also successfully cooperating with the Bank of Slovenia in the collection on international roaming data for the needs of monitoring tourist and transit movements. For this purpose monthly data on daily-active users that are roaming in mobile networks of individual countries is collected from mobile telephony operators, both in the case of users of domestic operators roaming in the networks of foreign countries as in the case of foreign users roaming in the networks of domestic mobile operators. Data aggregated by individual country is forwarded to the Bank of Slovenia for the needs of further population migration and balance of payments analyses.

Co-operation via the Information Commissioner

In compliance with the provisions of Article 48 of the Personal Data Protection Act, the Information Commissioner gives preliminary opinions to ministries, the National Assembly (parliament), self-governing local communities (municipal authorities), as well as other state institutions and bearers of public authority, as to the compliance of statutory provisions and other regulations with extant legislative regulation determining the processing of personal data. The Information Commissioner participates in the preparation of the acts of parliament and other legislative regulations.

Other co-operation of NIS stakeholders to combat spam and malware

No specific formal cooperation agreements appear to exist. There is however a non-formalised principle of (obligatory) administrative assistance. In practice this would mean that any competent authority must, when a case of spam is presented, inform the other competent authorities.

Co-operation via SI-CERT

In the course of 2010, similar with the previous year, Slovenia has as a computer emergency response team the SI-CERT which operates within the Academic and Research Network of Slovenia (ARNES); hence it is often referred to as the ARNES SI-CERT.

The constituency is extended to all computer networks in Slovenia, both academic and commercial. By agreement with Slovenian government, SI-CERT provides the role of the Government CERT. SI-CERT's main services include coordination of security incidents involving networks or systems in Slovenia, distribution of security-related information to the constituency, and providing technical expertise on network security related issues. The team can also provide contact information of appropriate law-enforcement agencies in Slovenia. As part of the national research and education network, SI-CERT has strong ties with the academic community.

ARNES SI-CERT is also member of the TERENA-TF-FIRST and the Forum of Incident Response and Security Teams (FIRST) forums. In the event of a state of emergency chapter IX of the Slovenian Law on Electronic Communications become applicable which stipulates the obligation of the operators to provide access to public communications networks and publicly available communications services, and to implement appropriate technical and organisational measures, e.g. by facilitating the exchange of information, to minimise the disruption to their activities in the event of catastrophic network breakdown, war or state of emergency and natural and other disasters.

Information exchange mechanisms in place on network resilience aspects

Information exchange on network resilience issues is not regulated for the time being, in Slovenia. Most of the co-ordination is done in a more informal way, either by personal contacts between the relevant players or in working groups which focus more on technical standards and interoperability issues.

Fostering a proactive NIS community

In terms of international cooperation Slovenia is active in participation in working groups of international organizations OECD – WPISP (Working Party on Information Security and Privacy), EFMS - European Forum for Member States (follow-up to the policy initiative on Critical Information Infrastructure Protection (CIIP) adopted by the European Commission on 30 March 2009).

Cyber Europe 2010

During 2010 Slovenia, as an observer, took part in the first pan-European exercise on critical information infrastructure protection, Cyber Europe 2010, organised by EU Member States and jointly supported by the European Network Security Agency (ENISA) and the EU's Joint Research Centre (JRC).

This exercise is part of the measures stipulated by the Digital Agenda for Europe (strategy launched by the European Commission) in order to increase confidence in the Internet and improve network security.

The exercise scenario called "Cyber Europe 2010 foresaw the gradual loss or considerable reduction of Internet connections between European countries and in the worst case, the effective cancellation of the main cross-border connections in Europe. The objectives of the exercise were:

- To establish trust in between actors within the Member State, and between the Member States (MS)
- To increase understanding of how management of incidents is done in different MS across Europe.
- To test the communication channels, communication points and procedures in the MS/between MS.
- To highlight interdependencies between MS across Europe.
- To increase mutual support procedures during incidents or massive cyber attacks

Participants in CYBER EUROPE 2010 were only public authorities of EU Member States. The players involved include ministries, national regulatory agencies, CIIP and information security related organisations, national computer security incident response teams (CSIRTs).

EU Convention on Cybercrime⁸

Slovenia joined the Convention on Cybercrime CETS No. 185 on 2005. The Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception.

Its main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation.

The Convention is the product of four years of work by Council of Europe experts, but also by the United States, Canada, Japan and other countries which are not members of the Organisation. It has been supplemented by an Additional Protocol making any publication of racist and xenophobic propaganda via computer networks a criminal offence.

⁸More details about the Convention on Cybercrime available at <http://www.conventions.coe.int/Treaty/en/Treaties/Html/185.htm>

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

Security incident management

During the course of 2010, similar as in previous year, most of the information security incidents reported in Slovenia, are handled via the Slovenian Computer Emergency Response Team (SI-CERT), which is the authorized body to address all types of computer security incidents which occur, or threaten to occur, in its constituency and which require cross-organizational coordination. Past incidents are analysed for large-scale problems and when identifying new trends. Currently it is not clear when, how and what kind of incidents must be reported by an infrastructure owner - reporting of incidents to SI-CERT is voluntary.

The SI-CERT can also provide assistance and advice on reporting criminal activity to the appropriate Slovenian law-enforcement body. Another role that SI-CERT performs is the issuing of warnings to the general public on security issues via public bulletins and advisories.

Emerging NIS risks

The national risk management process

Slovenia has a national risk management process in place, but it does not specifically cover NIS-related risks. The Administration of the Republic of Slovenia for Civil Protection and Disaster Relief, Ministry of Defence put in place a disaster risk information management system but this is not specifically address the NIS-related risks.

Relevant emerging NIS risks

The information or cyber blockades are specifically identified as emerging sources of threats to the National Security of Republic of Slovenia⁹. The National Security Strategy recognises that as a developed computerised society, the Republic of Slovenia is becoming vulnerable also in the field of data processing security. The transport infrastructure, telecommunication network, health and social welfare system, financial system, and supply are identified fields whose functioning can be thwarted or completely disrupted with computer measures.

No recent relevant information was identified on the participation of the Slovenian CERT, ISPs, etc in other European-wide projects aiming at identifying emerging NIS risks, like for example in the Worldwide Observatory of Malicious Behaviours and Attack Threats (WOMBAT)¹⁰ or in the FORWARD¹¹ initiative of the European Commission.

Computer crime incidents

With reference to the computer crime incidents, according with the Slovenian Police's last published reports¹² which was from 2008 at the time of this report, there was a major upward trend in computer crime rates with 310 cases in 2008, representing a 176.8 % increase. Suspect

⁹ See the resolution on the National Security Strategy of the Republic of Slovenia

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

¹¹ See: <http://www.ict-forward.eu/home>

¹² See the latest published annual report on the work of the Slovenian Police, available at: http://www.policija.si/portal_en/statistika/lp/pdf/report2008.pdf

numbers went up from 96 to 304 (a 216.7 % increase). Information system attacks rates rose most significantly, which is due to expanding cyber crime and also people's increased awareness of Internet hazards and their readiness to report such violations.

The following categories of computer crime incidents are reported:

- Abuse of personal data in the Internet
- Violation of material copyright related to the Internet
- Attack against information systems
- Intrusion into a commercial information system
- Manufacture and acquisition of weapons and instruments intended for intrusion into or attack on information system

Resilience aspects

Comparing with the previous year, during the course of 2010 there were no significant changes related to the NIS resilience aspects. In line with the provisions of the Slovenian Electronic Communications Act (*Zakon o elektronskih komunikacijah – ZEKom*), the telecom operators providing access to the Slovenian public telephone network and publicly available telephone services are obliged to implement appropriate technical and organisational measures to minimise the disruption to their activities in the event of catastrophic network breakdown, war or state of emergency and natural and other disasters. They are also obliged to coordinate such measures with the bodies responsible for the security and defence system and the civil protection and rescue system.

These measures must ensure that the integrity of the public telephone network and the availability of the public telephone network and publicly available telephone services are restored in the shortest possible time. These measures must also enable uninterrupted access to and use of emergency call numbers and in particular the standard European emergency call number 112 and 113 for police, even in the event of partial failure of the public telephone network.

In line with the same act, operators must prioritise ensuring the operation of those parts of the network that are essential for the uninterrupted operation of the networks of the security and defence systems and the civil protection and rescue system.

Privacy and trust

Status of implementation of the Data Protection Directive¹³

The new Slovenian Personal Data Protection Act (*Zakon o varstvu osebnih podatkov, UL RS No. 86/2004 et seq, ZVOP-1*) replaced the previous Personal Data Protection Act (*UL RS No. 59/1999, Old ZVOP*) and implemented the Data Protection Directive.

The Personal Data Protection Act was adopted by the National Assembly of the Republic of Slovenia on 15th July 2004, and has been in force since 1st January 2005. Adoption of this Act was for the most part a consequence of the accession of Slovenia to the European Union, and the resultant obligations to harmonize personal data protection with the provisions of Directive 95/46/EC of the European Parliament and the Council for the Protection of Individuals regarding Personal Data Processing and the Free Movement of Such Data¹⁴.

The Slovenian competent national regulatory authority on this matter is the Information Commissioner (*Informacijski pooblaščenec or the Commissioner*).

During 2009, the Information Commissioner received 624 applications and complaints as to suspected violations of the provisions of the Personal Data Protection Act; namely 219 in the public sector and 405 in the private sector. Statistical data indicates that the number of applications as to alleged violations of Slovenia's Personal Data Protection Act remained at almost the same level as in 2008.

Personal Data and Sensitive Personal Data

According to the ZVOP-1 personal data is any data relating to an individual (an identified or identifiable natural person to whom personal data relates), irrespective of the form in which it is expressed.

Under the ZVOP-1, sensitive personal data includes: (i) the standard types of sensitive personal data; (ii) information about criminal records and minor offences; and (iii) biometric information if it can be used to identify sensitive personal data about a data subject.

The ZVOP-1 also has a range of additional restrictions that apply to video surveillance, biometric information, access control information and connecting systems.

Sensitive personal data may be processed if the standard conditions for processing sensitive personal data are met. In addition, when processing sensitive data the data must be labeled and protected so as to prevent unauthorised access. Transfer of sensitive data is deemed adequately secure if the data are encrypted so they are illegible and un-recognisable during transfer. Furthermore, any consent from a data subject must be given in writing.

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

Data controllers must comply with the general data security obligation, for example in Article 24 of the Data Protection Act by enabling subsequent determination of when individual personal data were entered into a filing system, used or otherwise processed, and who did so, for the period covered by statutory protection of the rights of an individual due to unauthorised supply or

¹³ Source: the annual report 2009 of the Slovenian Information Commissioner, available at http://www.ip-rs.si/fileadmin/user_upload/Pdf/poročila/Annual-report-2009.pdf

¹⁴ Official Journal of the European Union, No. L 281, 23rd November 1995

processing of personal data¹⁵. In processing sensitive data, the data must be labeled and protected so as to prevent unauthorised access. Transfer of sensitive data is deemed adequately secure if the data are encrypted so they are illegible and unrecognisable during transfer.

Data protection breaches

The ZVOP-1 does not contain any obligation to inform the Information Commissioner or data subjects of a security breach. According to the latest information published¹⁶ by the Information Commissioner, in 2009, the insufficient security measures to ensure adequate protection of personal data represent the second most encountered reason of the suspected violations of the personal data protection act (i.e. a number of 54 reported cases in 2009 comparing with 31 in 2008).

Enforcement

The Information Commissioner has the power to: (i) issue enforcement notices, such as to order the elimination of irregularities or deficiencies; (ii) order the prohibition of processing of personal data; and (iii) order the prohibition of the transfer of personal data to third countries or foreign recipients.

The Information Commissioner also has the power to fine the violators of the ZVOP-1. Prosecution for criminal offences are brought before the Slovenian courts which may impose higher fines than the Commissioner and may sentence violators to up to two years' imprisonment.

The Information Commissioner also has capabilities under the Act on Electronic communications in the field of data retention. One of the more relevant articles is Article 112, which states that the information commissioner shall undertake inspection supervision of the retention of traffic and location data acquired or processed in connection with providing public communications networks or services.

¹⁵ <http://www.ip-rs.si/index.php?id=339>

¹⁶Source: the annual report 2009 of the Slovenian Information Commissioner, available at http://www.ip-rs.si/fileadmin/user_upload/Pdf/porocila/Annual-report-2009.pdf

NIS awareness at the country level

Awareness actions targeting the consumers/citizens

In recent years, many successful projects have taken place in Slovenia in the field of safe use of Internet, namely the SAFE-SI awareness node and the Slovenian website hotline Spletno oko for receiving anonymous reports on child pornography and hate speech on the Internet. The two projects are operated in the framework of the EU Community programme Safer internet and are financed by the Directorate General for Information Society at the European Commission and Directorate for Information Society operating within the Ministry of Higher Education, Science and Technology.

The SAFE-SI (<http://www.safe.si>) is an awareness node on safer use of the Internet in Slovenia. The project is being implemented by the coordinator - University of Ljubljana, Faculty of Social Sciences in cooperation with the Academic and Research Network of Slovenia (ARNES) and the Slovene Consumers Association. This project is part of a wider European network of awareness nodes called INSAFE. The goal of the project is to raise awareness and digital literacy of selected target populations of children, minors, their parents and teachers.

One of most important SAFE-SI project objectives is to educate Slovenian teachers on the safe use of the Internet at schools. It is of key importance to include the syllabus covering the aspects of safe use of IT technologies at schools into the regular programme of IT education for teachers and into IT seminars organised by the Ministry of Education and Sport and by the National Education Institute. Accordingly, in 2008, 35 multipliers competent for primary school education performed 23 seminars with 297 participants.

The SPLETNO-OKO.SI hotline (<http://www.spletno-oko.si/>) collects anonymous reports of child pornography and hate speech on the Internet and forwards them to prosecuting authorities. The Spletno oko hotline checks the report and if it estimates that alleged illegal content is in question, it reports it to the police.

The project Spletno oko is being implemented by the coordinator - University of Ljubljana, Faculty of Social Sciences in cooperation with the Slovene Consumers Association and the Academic and Research Network of Slovenia (ARNES).

SPLETNO-OKO.SI operates in the context of communitarian programme Safer internet plus and INHOPE organization. The project's consultation body also includes the Office of the State Prosecutor of the Republic of Slovenia, the Police, media representatives, and representatives of other organizations active in the child rights protection field.

The project SIP-SI was a logical continuation of the projects Safe.si and Spletno oko. Besides the awareness node on safer use of the Internet and the hotline for children pornography and hate speech, an anonymous phone number 080 22 80 called Nasvet za net was launched in 2009 for assistance to young people in case of web problems at the website <http://www.nasvetzanet.si> coordinated by the Consumers Association of Slovenia.

Most recently the project SIP-SI was renamed to Safer Internet Centre Slovenia. The Centre integrates the Awareness Centre SAFE-SI (<http://www.safe.si>), the hotline Spletno oko (<https://www.spletno-oko.si>) and the helpline Nasvet za Net (<http://www.nasvetzanet.si/>)

Awareness actions related to personal data protection

Among the Slovenian Information Commissioner's awareness and prevention activities are the issues of guidelines which convey clear, comprehensive and useful practical instructions for controllers of personal data collections and hence provide answers to the most commonly asked

questions from the field of personal data protection, which are encountered by controllers of personal data collections. The Information Commissioner issued the following guidelines which are accessible via the Internet:

- Guidelines for the protection of personal data in hospital information systems
- Guidelines in the introduction of biometric measures
- Guidelines for personal data protection in employment relationships
- Guidelines for carrying out video surveillance.

The Information Commissioner maintains a web site containing awareness raising information on: phishing, pharming attacks, unsolicited e-mails (spam) and Slovenian legislation related to it, child pornography and hate speech report hotline.

"Varni na internetu" project

The project addresses a wide range of information security issues. Raising of awareness on safe Internet use is defined as a key objective of the project of the Slovenian public awareness.

Project activities are aimed at achieving the following objectives:

- raise awareness of target audiences about the different threats facing them on the web;
- safe use of online banking;
- inform about the types of fraud websites and offer practical solutions on how to stay;
- protection of personal identity in social networks.

Awareness actions targeting the industry

INFOSEK 2010

This three-day conference INFOSEK is an annual joint event in cooperation with ENISA and takes place in Nova Gorica, Slovenia. Traditionally organized at the end of November in Nova Gorica, Slovenia, INFOSEK is known as a unique expert conference and a Slovenian central event. Led by security experts from a variety of industries from Slovenia and foreign countries, the INFOSEK offers insight into how essential information security is key to organisation's success and survival.

RiSK 2010

The RiSK 2010 Conference was organised in February 2010 in Maribor, Slovenia and involved more than 400 people, mainly IT management and information security experts from 15 countries. RiSK 2010 is a continuation of the conference organised in 2009 and was a specialized two-day meeting on information security and business continuity and covered topics like for example:

- Professional expert overview of the state of security and risk management practice;
- Overview of new best practices and solutions in each area of the security segment;
- Specific recommendations for addressing security needs;
- One-on-one debate with representatives from leading IT security vendors;
- Information exchange between CIOs, CFOs, CTOs;
- Takeaway tools for assessing risk, drafting a plan, and testing solutions.

The International Information Society – IS multi-conference held in Ljubljana

This is an annual event in Ljubljana, Slovenia and provides an international forum for scientists, academicians and professionals to present their latest research findings in the various fields of information society. In 2010, the conference covered the following topics with relevance for NIS:

- intelligent systems;

- education in information society;
- data mining and data warehouses;
- collaboration, software and services in information society;
- cognitive sciences
- robotics.

Country-specific activities for identifying and promoting economically efficient approaches to information security

There was identified no relevant recent information regarding Country-specific activities for identifying and promoting economically efficient approaches to information security in Slovenia.

Interdependencies, Interconnection and Improving Critical Information Infrastructure Protection

At the moment the Republic of Slovenia has no formally accepted policy and strategy with regard to critical infrastructure protection. The government of the Republic of Slovenia has appointed an inter-ministerial coordination group in order to coordinate activities for the protection of critical infrastructure of the Republic of Slovenia, which is lead by the Ministry of Defence. The main task of the coordination group is to define which infrastructure should be considered as vital and to propose adequate measures and procedures as well as bodies and organizations to be in charge of the critical infrastructure protection.

At the governmental level there is no supervision assured over the actual protection of the critical information infrastructure for the time being. After the critical infrastructure of the Republic of Slovenia will be determined the government will appoint appropriate ministries and governmental offices that will have to carry out the supervision over the implementation of proper measures for the safeguarding and protection of critical infrastructure by relevant agencies, organizations, companies, private entities and others that actually have to deal with critical infrastructure through their daily businesses.

There is also a project ongoing in Slovenia that is entitled "Public-private partnerships in the area of protection of the critical infrastructure: analysis of best practices and solutions". The research focuses on issues of reasonableness, possibilities, conditions and uses of public-private partnerships in the area of critical infrastructure protection. The main aim of the project is to identify common practices in the area in some reference countries, to analyze the operation and regulation of the PPP in the reference countries and to determine conditions and possible adjustments that may be necessary in order to be able to adopt the solutions that were developed in other countries. This holds true for the information and communication sector as well.

One of the goals of the inter-ministerial coordination group aimed to coordinate activities for the protection of critical infrastructure, is to propose a systemic solutions for protection of the critical information infrastructure in case of disastrous scenario. Within the frame of designing critical infrastructure protection it will be necessary to properly shape and identify appropriate instrument for early warning and informing about events jeopardizing critical infrastructure and exchange of information in support of harmonized and efficient response for protection of the critical infrastructure.

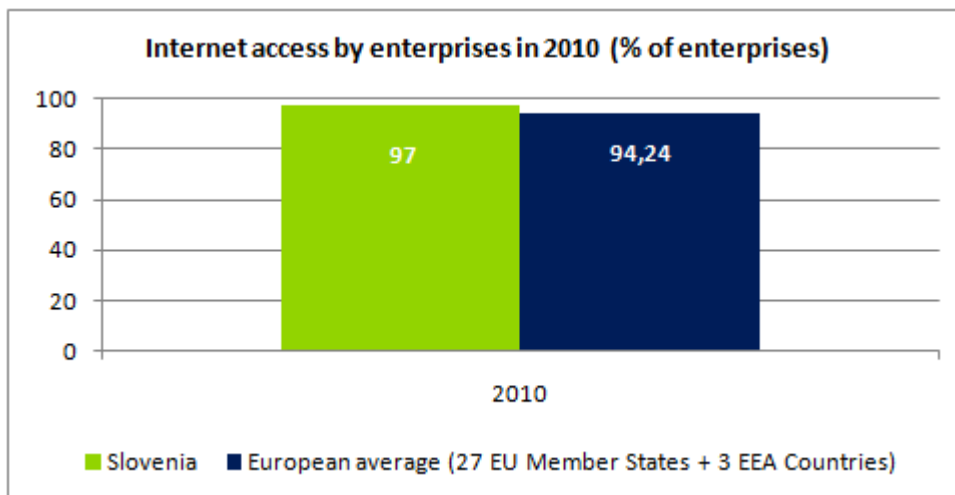
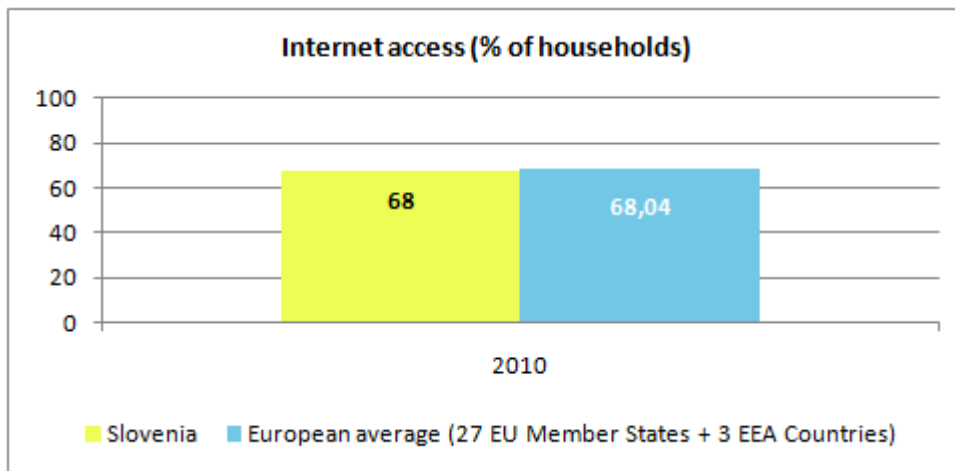
The Slovenian law on Electronic Communications uses neither the term "critical infrastructure protection" nor the term "critical information infrastructure protection".

Relevant statistics for the country

In order to provide the reader with additional information about the relative stage of NIS development in Slovenia, a series of relevant statistics are included in this section. Those statistics mainly show that Slovenia is on the European average in regards of Information Technology matters.

Internet access of population and enterprises

The following graphs provide an overview of the situation¹⁷ of Internet access in Slovenia for enterprises and respectively households, relative to the European average.

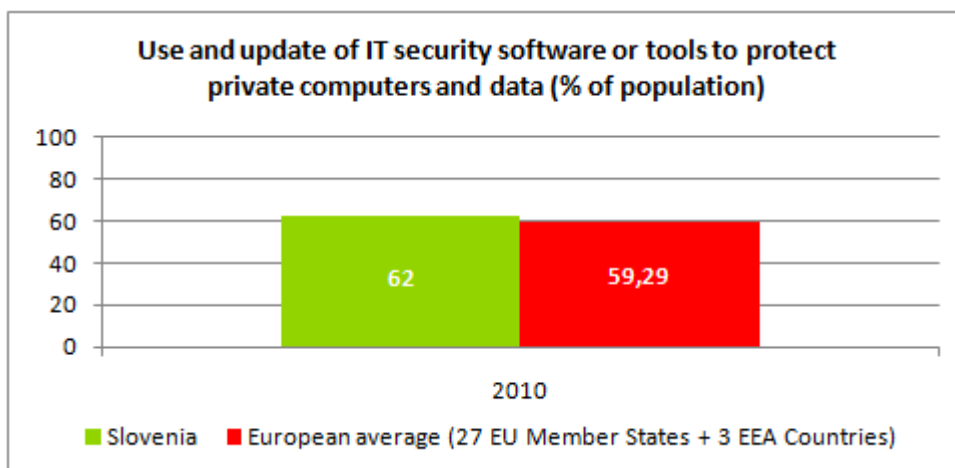
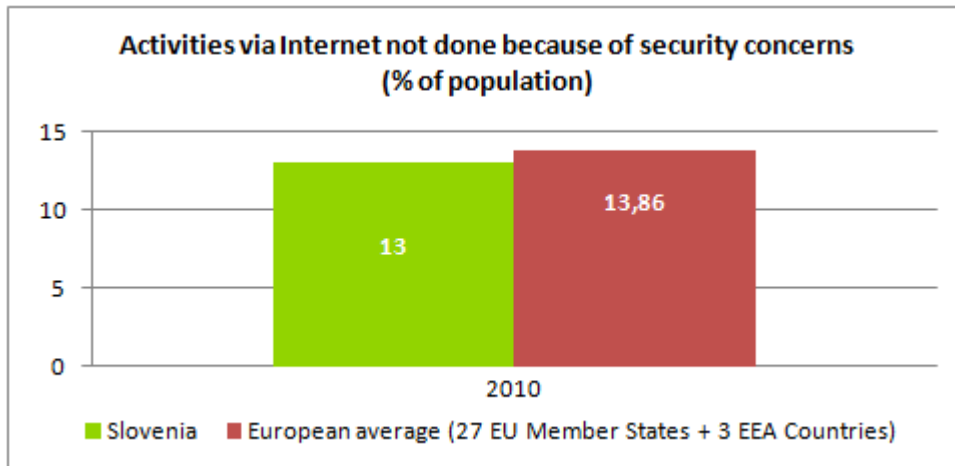


In 2010, the statistics indicate that the enterprises and the households in Slovenia have almost the same level of Internet access as the European average.

¹⁷ Source: Eurostat

Statistics on use of Internet by individuals and related security aspects

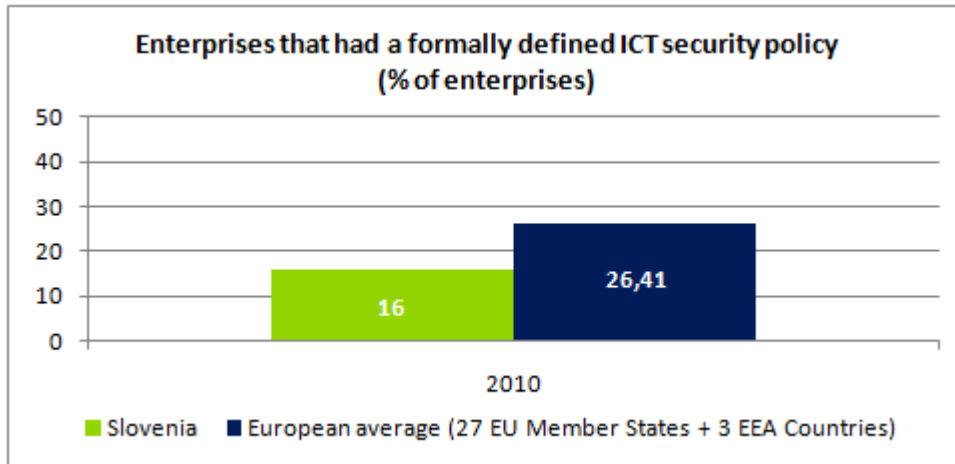
The percentage of population in Slovenia that is reluctant in performing activities via Internet (e.g. e-banking, purchases of goods and services over Internet, etc.) because of security concerns is almost the same as the European average:



Also, it appears that the use of security tools to protect private computers and data is slightly above the European average.

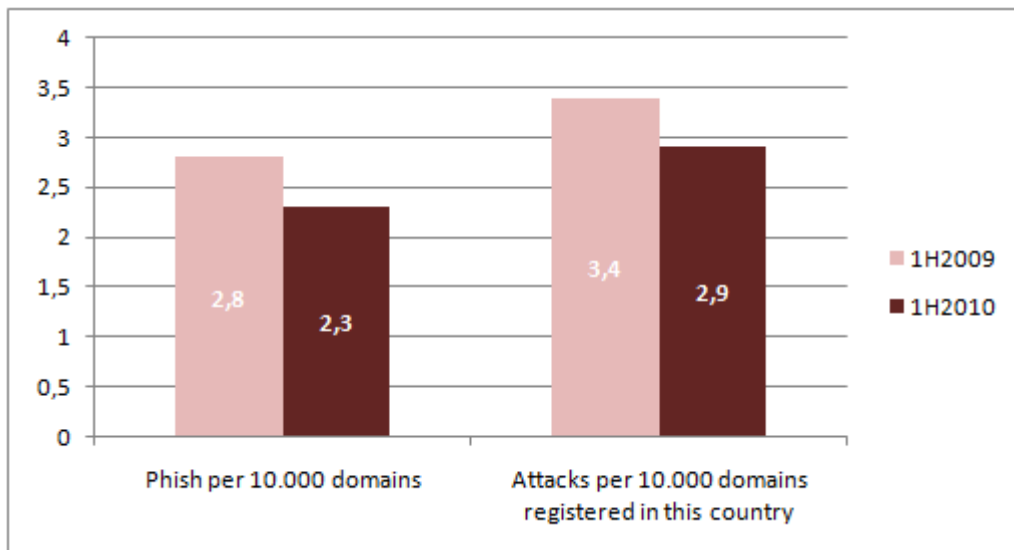
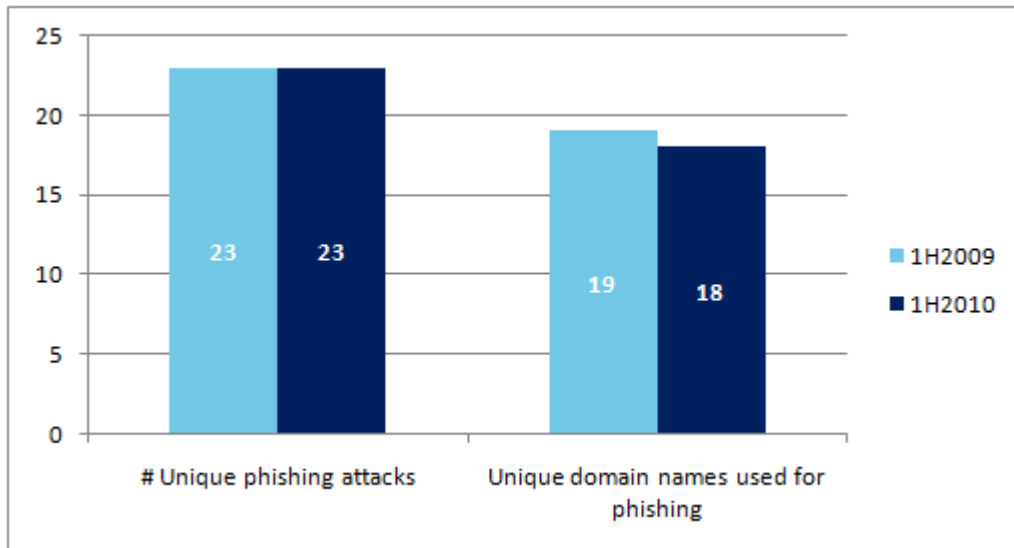
Statistics on use of Internet by enterprises and related security aspects

Fewer enterprises in Slovenia 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, Slovenia was mentioned in the global report¹⁸ published by the Anti-Phishing Working Group (APWG) with the following relevant statistics:



¹⁸ 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 Higher Education, Science and Technology - Directorate of Information Society	<p>Coordinates various thematic fields of the information society under the i2010 strategic framework including further development of digitally supported business, services, open code accessibility, and inclusion in the digital society for all new and innovative approaches in ICT.</p> <p>The coordination contributes towards general growth based on the information society, supporting the development of eServices, eContent and eBusiness within the framework of the national interoperability network</p>	www.mvzt.si
2. Ministry of Foreign Affairs - Section for Information System Development and Information Security / <i>Ministrstvo za zunanje zadeve (MZZ)</i>	<p>The Section for Information System Development and Information Security is responsible for the strategy and development of the Ministry's information system.</p> <p>It oversees information projects and the procurement of IT equipment and specifies standards for the IT equipment. It is also responsible for system and application development and system administration, setting up test and model installations, planning and proposing the adoption of rules on information technology, and assuring verification and control. The Section operates in the fields of data communications, data security and protection and defence preparations. It is also responsible for the development and operation of the Ministry's communications system, protected electronic mail, Internet connections and connections with other information systems.</p>	www.mzz.gov.si
3. Ministry of Public Administration, Directorate for e-Government and Administrative Processes / <i>Ministrstvo za javno upravo (MJU)</i>	In charge of development, smooth operation and maintenance of state authorities' applications systems on the information and communication infrastructure of state authorities.	www.mju.gov.si
4. Post and Electronic Communications Agency of the Republic of Slovenia / <i>Agencija za pošto in elektronske komunikacije (APEK)</i>	<p>The Post and Electronic Communications Agency of the Republic of Slovenia is an independent regulatory body that regulates the fields of electronic communications, postal services and radio and television programmes in the Republic of Slovenia.</p> <p>The Agency's mission is to stimulate competition, ensure equality for operators of communications networks and service providers and providers of postal services, to manage the radio-frequency spectrum and number range, to monitor the content of radio and television programmes and protect the rights of users in both the Republic of Slovenia and the European Union.</p>	www.apek.si
5. Slovenian Governmental Certification Authority / <i>Overitelj digitalnih potrdil (SIGOV-CA)</i>	SIGOV-CA is part of the Slovenian Governmental Certification Authority and has been functioning as a trusted third party since 2001 responsible for issuing digital certificates.	www.sigov-ca.gov.si

National authorities	Role and responsibilities	Website
6. Slovenian General Certification Authority (SIGEN-CA)	SIGEN-CA issues qualified digital certificates of the Certification Authority at the Ministry of Public Administration (MJU) for business entities and natural persons, who are registered in the Republic of Slovenia.	www.sigen-ca.si
7. The Slovenian Time Stamping Authority (SI-TSA)	SI-TSA is an issuing authority for trusted time stamps and part of the Public Key Infrastructure (PKI) of the Slovenian General Certification Authority. SI-TSA issues trusted time stamps, intended at present for applications used by public administration institutions.	www.si-tsa.si
8. Slovene Intelligence and Security Agency / Slovenska Obveščevalno Varnostna Agencija (SOVA)	The agency's area of work covers intelligence, counter-intelligence and all related security aspects. It closely interacts with telecommunications operators while enforcing its attributions linked to interception of telecommunications.	www.gov.si/sova/en/index.html
9. Office for the Protection of Classified Information / Urad Vlade RS za varovanje tajnih podatkov (UVTP)	Government office for the protection of classified information concerning personnel, physical, documentation, information and industrial security as well as training on these areas. It issued secondary legislation on the protection of classified information in communication - information systems.	www.uvtp.gov.si
10. Information Commissioner / Informacijski Pooblaščenec	The Information Commissioner / <i>Informacijski Pooblaščenec</i> supervises both the protection of personal data (covering the Personal Data Protection Act) and access to public Information (covering the Access to Public Information Act).	www.ip-rs.si
11. Ministry of Interior, Criminal Police Directorate, Computer Crime Section	The Computer Crime Section under the Criminal Police Directorate of the Slovenian Ministry of Interior has responsibilities related to investigation of the computer crime incidents.	www.policija.si

Computer Emergency Response Teams (CERTs)

CERT	Role and responsibilities	Website
12. SI-CERT	<ul style="list-style-type: none"> • FIRST¹⁹ member • TI²⁰ listed <p>SI-CERT is the Slovenian CERT. SI-CERT is a service offered by ARNES (Academic and Research Network of Slovenia). The constituency is extended to all computer networks in Slovenia, both academic and commercial. SI-CERT's main services include coordination of security incidents involving networks or systems in Slovenia, distribution of security-related information to the constituency, and providing technical expertise on network security related issues. SI-CERT is FIRST member and is TI listed</p>	www.arnes.si/en/si-cert/

¹⁹ <http://www.first.org/members/teams/>

²⁰ <http://www.trusted-introducer.nl/>

Industry organisations active in network and information security

Industry Organisations	Role and responsibilities	Website
13. Chamber of Commerce and Industry / Gospodarska zbornica Slovenije (GZS) – Association of Informatics and Telecommunications (ZIT)	Under the umbrella of the Chamber of Commerce and Industry of Slovenia (GZS), the Association of Informatics and Telecommunications (ZIT) brings together more than 2 000 (around 500 IT) companies and self-employed members. ZIT is member of EICTA.	www.gzs.si www.gzs.si/slo/panoge/zdruzenje_za_informatiko_in_telekomunikacije
14. Slovene Internet Service Provider Association / <i>Sekcija ponudnikov Internet storitev Slovenije (SISPA)</i>	Represents the Internet Service Providers of Slovenia. This organization was created to promote the interests of companies providing internet services. SISPA is also active at a regulatory, legislative and technical level on behalf of its members and of the industry in general. SISPA works as a section inside the Association of Informatics and Telecommunications at Chamber of Commerce and Industry of Slovenia. Its mission is stimulating faster development of information society in Slovenia with creative and innovative use of the Internet. In the section are 20 Internet suppliers, including all biggest operators.	www.sispa.org

Academic organisations active in network and information security bodies

Academic Organisations	Role and responsibilities	Website
15. Academic and Research Network of Slovenia (ARNES)	The Academic and Research Network of Slovenia (ARNES) is a public institute which provides network services for research, educational and cultural organizations and enables them to connect and cooperate with each other and with related organizations abroad. Together with the Faculty of Social Sciences runs the Slovenian awareness node SAFE.SI.	www.arnes.si
16. Faculty of Social Sciences, University of Ljubljana	The Faculty of Social Sciences, runs with ARNES the Slovenian awareness node SAFE.SI, financed through the 'Safer Internet plus' programme (www.safe.si). They also manage the Slovenian hotline project 'Spletno oko', financed through the 'Safer Internet plus' programme.	slovenia.ris.org www.ris.org
17. Institute of Informatics/ Faculty of Electrical Engineering and Computer Science	The institute of Informatics/Faculty of Electrical Engineering and Computer Science is focused on research and development of state-of-the-art information systems and security systems and methods	lisa.uni-mb.si/index_ang.htm
18. Faculty of Computer and Information Science, University of Ljubljana, Laboratory for system research and information technologies	The Faculty of Computer and Information Science is focused on research (security, privacy, trust management) and security-oriented decision support systems. The activities of the laboratory are aimed at research and development of next generation networks, telecommunication technologies, and promotion of the concept of information society. The main areas of research include also security, cryptography and privacy in information systems	www.fri.uni-lj.si

Academic Organisations	Role and responsibilities	Website
19. Jozef Stefan Institute Laboratory for Open System and Networks	Research of privacy and security issues in next-generation networks, telecommunication technologies, applications and services. Studies on forensic tools, cyber-crime and legislation aspects. Organization of conferences, workshops and summer schools. Education and training in information security.	www.ijs.si
20. Laboratory for Telecommunication, Faculty of Electrical Engineering, University of Ljubljana	The laboratory for Telecommunication, Faculty of Electrical Engineering at the University of Ljubljana is performing Research work oriented to the traffic measurement and traffic theory, simulation of switching and routing of traffic in synthetic and real networks. Research work is also related to the quality of services mechanisms in combination with transmission of data, audio and video traffic over wireline and wireless IP networks. Security in IP and mobile systems is also one of the important research areas. Significant effort is given to exploration of the use of telecommunications and information technology for people with disabilities.	lt.fe.uni-lj.si/default.asp
21. Faculty of Organisational Sciences/ University of Maribor	Faculty of Organisational Sciences at the University of Maribor is performing various research projects regarding eCommerce, eMarkets, eProcurement, information systems auditing, groupware and analysis & design of inter-organizational processes.	ecom.fov.uni-mb.si/ecomENG/index.htm
22. Centre for Legal Informatics (CEPRIS)	Research of e-business legislation, new legislative proposals, legal counselling, dissemination and development of complex, secure e-business solutions.	www.cepris.si

Other bodies and organisations active in network and information security

Others	Role and responsibilities	Website
23. Slovene Consumers Association (ZPS)	The Slovene Consumer Organization is an independent, non-profit, internationally established, non-governmental organisation that represents, advises, informs and promotes awareness of the consumers. Its role in Spletno oko project is mainly in promotion and advertising of the hotline.	www.zps.si
24. Spletno-Okno	Spletno-Okno.SI is a Slovenian hotline to facilitate the anonymous reporting of illegal Internet content: child pornography and hate speech.	www.spletno-okno.si/en
25. SAFE-SI	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. Its goal is also to fight against illegal content and content unwanted by the end-user. The initiative is part of the EU's coherent approach.	www.safe.si

References

- Report on the Development of the Slovenian Electronic Communications Market for the Second Quarter of 2009, Ljubljana, September 2009 issued by the Post and Electronic Communications Agency of the Republic of Slovenia, available at http://www.apek.si/en/telecommunications_market
- The latest published annual report on the work of the Slovenian Police, available at: http://www.policija.si/portal_en/statistika/lp/pdf/report2008.pdf
- Slovenian Electronic Communications Act (ZEKom-UPB1); available at <http://www.apek.si>
- Slovenian Official Gazette No. 86/2004, Personal Data Protection Act (ZVOP-1)
- Slovenian Official Gazette No. 67/2007; Personal Data Protection Act - amendments (ZVOP-1A).
- An overview of the eGovernment and eInclusion situation in Europe, available at <http://www.epractice.eu/en/factsheets>
- ENISA, Information security awareness in financial organisation, November 2008, available at • http://www.enisa.europa.eu/doc/pdf/deliverables/is_awareness_financial_organisations.pdf
- Slovenia - ENISA CERT Directory: <http://www.enisa.europa.eu/act/cert/background/inv/certs-by-country/slovenia>
- The eGovernment Strategy of the Republic of Slovenia for the period 2006 to 2010 available at http://www.mju.gov.si/fileadmin/mju.gov.si/pageuploads/mju_dokumenti/english/SEP2010_english_final.doc
- The Action Plan for eGovernment for the period 2006 to 2010 available at http://e-uprava.gov.si/eud/e-uprava/akcijski_nacrt_e-uprave_2010.doc
- The Slovenia's Development Strategy 2006-2013 available at http://www.slovenijajutri.gov.si/fileadmin/urednik/dokumenti/Slovenia_s_Development_Strategy.pdf
- The Act amending the Electronic Commerce and Electronic Signature Act available at <http://www.uradni-list.si/1/objava.jsp?urlid=200425&stevilka=1066>
- More details about the Convention on Cybercrime available at <http://www.conventions.coe.int/Treaty/en/Treaties/Html/185.htm>
- The annual report 2009 of the Slovenian Information Commissioner, available at http://www.ip-rs.si/fileadmin/user_upload/Pdf/porocila/Annual-report-2009.pdf



PO Box 1309, 71001 Heraklion, Greece, Tel: +30 2810 391 280
www.enisa.europa.eu