National Strategy
for Information Security in the Slovak Republic

Table of Contents

1. Introduction

The purpose of this document entitled “National Strategy for Information Security in the Slovak Republic” (hereafter referred to as the “NSIS”) is to lay down an information security framework in the Slovak Republic (hereafter referred to as “SR”). With respect to the fact that ensuring information security (the document covers non-classified information only) requires a comprehensive approach, it is necessary to define its basic level, with an option of further upgrading in specific fields. Well-defined *information security* is important with a focus on the establishment of primary legislative rules in the respective area, as well as with respect to further steps to be taken to address the issue of information security in Slovakia.

The strategy defines starting points, allocates competences and proposes aims, priorities and steps to be taken in order to achieve the set purpose. The document also includes a basic description of individual tasks with an aim of ensuring the protection of the entire Slovak digital space, with the exception of classified information falling under the competence of the NSA (National Security Authority). These involve, in particular, measures to avoid leakage of information and its unauthorised use, violation of data integrity, violation of people’s right to protection of personal data; measures to protect against damage and misuse of information and communication systems, harm to reputation of public and private institutions (defamation); as well as measures to enforce applicable Slovak and EU laws. A poor level of protection of information and information and communication technologies raises doubts about reliability and credibility of information available from the Internet environment, a network currently connecting computer systems in more than 250 countries around the world. This world’s largest network provides today access to virtually unlimited information resources, enabling their exchange and providing a multitude of services such as e-mail, file transfer, etc. On that account, reliable operating information systems, reliable information exchange and related information security provide guarantees, to a certain degree, that citizens’ basic rights and freedoms and competitive development of each country are ensured. Implementation of measures envisaged under this strategy will also enhance credibility of electronic services, electronic commerce, as well as competitiveness and credit of our country abroad.

2. Importance of the document

2.1 Importance of information security

Information and communication technologies (hereinafter referred to as “ICT”) have a considerable effect on the development of human society. Interconnected information and communication systems form an information and communication infrastructure (hereinafter referred to as “ICI”) through which operations are currently carried out virtually in all areas of public life (transport, finance and banking, energy, telecommunications, healthcare and social security, defence, security, education, culture, public administration operations, etc.). ICT extend beyond the existing ICI. Ensuring information security of a country is essential to the functioning of society. In a broader sense, this means ensuring information security and protection of the entire information space and, from the practical point of view, in particular, the protection of the state ICI and its information content, called a digital space in this

strategy.[1] A cyberspace, whose protection is ensured by the NSA and which also covers classified information and other facts to be specified by a binding regulation (an EU/Commission directive, EU regulation, law, etc., and/or a government resolution), has specific characteristics.

Information security is multilateral; i.e. it must take into account interests of ICT system owners, users' needs, as well as rights of natural and legal persons whose data are processed by the systems. As far as users are concerned, the following factors are most important with respect to the processing of information: purpose and content of information, accuracy, relevance, accessibility, authenticity, structure and quality of information. From the perspective of owners and operators, the most important element is a reliable access to on-line information resources and their protection against leakage, unauthorised use and violation of data integrity, as well as the authority and reputation of a system owner.

ICT systems and data processed by such systems may be made dysfunctional due to a number of various factors. They, for example, include natural factors, technical failures, human errors and faults, malicious software, intentional attacks, computer crime, and international terrorism.

The ICI is based on the Internet which enables mutual communication between information resources and information seekers, either in public or commercial sectors, or among individuals. The Internet has no owner; no rules and limits are in place to regulate the use of personal information and preclude its misuse by third parties. Serious security problems are also associated with other Internet-based services, such as e-mail, file transfers, etc.

A failure to secure information may consequently result in irrecoverable losses and harm the credibility of an organisation or country. Given the fact that the state guarantees critical processes, its task is to take care of an overall level of competitiveness of society, thus preserving national welfare, including knowledge and information, therefore it cannot afford to have low security level criteria in place. The consequences may be devastating, particularly in some specific areas. The state is therefore obliged to ensure that information is protected against misuse, and minimise consequences where such misuse has occurred.

2.2 Information security from the perspective of EU and multinational organisations

The approach to addressing security is driven by the need to resolve a problem which originated from scientific and technological development and has by now fully translated into a global social issue. Society seeks to resolve this problem and ensure both the protection of its valuable assets and individuals' privacy. National governments, multinational bodies and organisations associating the world's most advanced countries (UN, G8, OECD, ISO) have also come to realise the need of information security. Various institutions and institutional systems have been set up to ensure the protection of information (ENISA, HLIG, CERT, etc.), strategic objectives have been defined and elaborated on, and measures have been taken to meet the set objectives.

[1] the term digital space corresponds to the term "cyberspace" widened by standards, norms and legislation, for which, however, the literal Slovak translation *kybernetický priestor* is not suitable due to its narrower meaning

In this context, the European Network and Information Security Agency (ENISA) was established, associating all EU Member States; Slovakia is represented by the Ministry of Finance in this body.

At the Lisbon summit in the year 2000, representatives of states and governments agreed to make the EU "*the most dynamic and competitive knowledge-based economy in the world capable of sustainable economic growth with more and better jobs and greater social cohesion, and respect for the environment by 2010*", and adopted the so-called eEurope initiative, replaced by "*i2010 initiative" (European Information Society 2010)* later in 2005. The EU included information security among its main priorities and has published a number of strategic documents, recommendations, directives and regulations on the protection of personal data and computer software, electronic signature, e-commerce, combating computer crime, spam, etc.

2.3 Legislation and relations to other documents

The NSIS is based on the knowledge of the actual situation and experience in the world and in Slovakia, on EU directives, OECD recommendations, key international norms and standards for information security, the Slovak legal framework for the protection of information, and other documents adopted by the Slovak government and the National Council of the Slovak Republic. They mainly involve the following regulations:

- Act No. 275/2006 Coll. on Information Systems of Public Administration and on amendments to certain acts, as amended by Act No. 678/2006 Coll.;
- Act No. 215/2004 Coll. on the Protection of Classified Information and on amendments to certain acts, as amended;
- Act No. 428/2002 Coll. on the Protection of Personal Data as amended;
- Act No. 215/2002 on Electronic Signature and on amendments to certain acts, as amended;
- Act No. 618/2003 Coll. on Copyright and Rights Related to Copyright as amended;
- Act No. 483/2001 Coll. on Banks and on amendments to certain acts, as amended;
- Act No. 300/2005 Coll., the Penal Code, as amended;
- other laws and implementing regulations listed in *Annex 1*.

, By resolution No. 522 of 13 June 2001, the Slovak government has approved *"Information Society Policy in the Slovak Republic"* thus officially joining the eEurope+ initiative. In accordance with the aforementioned government resolution draft "*Strategy and Action Plan for the Development of the Information Society"* was prepared and approved by the government resolution No. 43 of 21 January 2004.

Convention on Cybercrime CETS 185/2001, issued by the Council of Europe, was ratified and incorporated into the Slovak Penal Code; Directive No 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures was transposed under the Act on Electronic Signature; and Directive No 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data was transposed under the Act on Personal Data Protection. Various decisions and directives issued by the Council of Europe are also currently valid in the area of information security.

Most important strategic documents in place in Slovakia include:

- "Slovak Security Strategy" (National Council, September 2005).
- "Draft Concept of Critical Infrastructure in Slovakia and Method of its Protection and Defence" (MoE, 2007).
- Concept of the Protection of Classified Information in Slovakia.

The present document complies with the relevant underlying international security standards and norms, as well as standards issued by the MF SR, the NSA, MoH, the Slovak Office for Personal Data Protection, and the Slovak Office of Standards, Metrology and Testing (SOSMT).

2.4 Areas of information security and competences

No comprehensive information security strategy has been adopted in Slovakia so far. Nevertheless, the issue of information security has been addressed in certain partial areas (in terms of legislation, competences, organisation and methodology). They are, in particular:

Information society (MF SR) and information security in public administration falling within the MF SR competence; activities pertaining to information security are carried out by the Committee for Information Security. The Committee is responsible for *"preparation of expert proposals and standpoints on information security"*; i.e. the Committee, inter alia, *"proposes the introduction of security standards, amendments to, or cancellation of, the existing applicable security standards for the information systems in public administration"*. (http://www.informatizacia.sk).

Protection of classified information (NSA) represents in terms of information security the area of classified information and systems working with classified information. Despite traditional terminology used in legislation[2], classified information is not classified in terms of *confidentiality* only; security requirements for its protection are complex and respect also the need of ensuring *integrity, authenticity and availability.* A dual management system is applied in relation to classified information that represents a cyberspace content and the part of Slovak digital space which does not work with classified information. For the sake of protection of Slovak digital space it will therefore be necessary to establish closer cooperation in the area of classified information protection and information security of the entire Slovak digital space.

Personal data protection (the Office for Personal Data Protection) and the use of **electronic signature** (NSA) are governed by laws[3] and the respective institutions supervise their compliance.

Electronic commerce (MoE) is governed by Act No. 22/2004 Coll. on Electronic Commerce and on amendments to Act No. 128/2002 Coll. on state inspection in internal market concerning consumer protection and on amendments to certain acts as amended by Act No. 284/2002 Coll. as amended by Act No. 160/2005 Coll. (hereinafter referred to as "Act No. 22/2004 Coll. on Electronic Commerce") under which Directive No 2000/31/EC of the

[2] Act No. 215/2004 Coll. on Protection of Classified Information and on amendments to certain acts, as amended by Act No. 638/2005 Coll. and Act No. 255/2006 Coll. and related regulations.
[3] Act No. 428/2002 Coll. on Protection of Personal Data as amended, Act No. 215/2002 Coll. on Electronic Signature and on amendments to certain acts

European Parliament and of the Council on Electronic Commerce, laying down the common legal framework of electronic commerce for all Member States, was transposed. Provisions and directives on electronic commerce are largely vague, therefore additional legislation is required. For this purpose, the Economic Commission for Europe - United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) officially published *Recommendation No. 33* in July 2005 in Geneva introducing a simple, transparent and effective processes for global commerce. Processes and services are governed by Directive No 2006/123/EC of the European Parliament and of the Council on services in the internal market; all Member States are obliged to put in force laws, other regulations and administrative measures necessary in order to ensure compliance with that directive. The respective measure requires that the directive be transposed into our legal system by the end of 2009.

Computer crime (Ministry of Justice, Ministry of the Interior) – this area is covered by the existing legislation as well. The Slovak Republic ratified the Convention on Cybercrime CETS 185/2001 issued by the Council of Europe; its principles were incorporated into the Penal Code[4].

Copyright (Ministry of Culture) and related rights are governed by the Copyright Act[5].

Norms and standards[6]. International standardisation organisations (ISO, IEC, CEN) publish also norms stipulating security requirements with respect to information and communication systems. Competences for the publication of these norms are divided among several institutions in Slovakia. Generally applicable norms are published by the SOSMT (Slovak Standards Institute - SUTN), standards pertaining to classified information and electronic signature are defined by the NSA, and standards for public administration information systems are published by the MF SR. Standards published by other central government authorities may also include some security aspects, e.g. standards issued by the Ministry of Health pertaining to the medical records. Coordination of standards publishment area in between individual institutions is ensured through involvement of their employees in relevant committees of the MF SR and the SOSMT; however, standardization of information security is not coordinated at the institutional level.

International cooperation in information security is necessary in order to ensure compatibility of solutions and sufficient level of protection of the global ICI. International cooperation is equally necessary due to the complexity of the area of information security as such, resulting in a situation where majority of countries do not have sufficient capacities to build the necessary know-how individually, and development and implementation of necessary solutions may take undesirably long even for the most advanced countries.

Slovakia is engaged in international cooperation efforts in information security; Slovakia is represented in the ENISA, EU working groups (OECD working group for information security; working groups for certification of means and accreditation of systems and networks for secure data transfer in EU electronic and communication systems, etc.), NATO working groups, FESA; Slovakia has also access to ISO information security standards under preparation. Individuals and non-state organisations are represented in other international organisations (IFIP TC11, etc.) as well. Using an ISO terminology, Slovakia is

[4] Act No. 300/2005 Coll., the Penal Code, § 247 Damage and misuse of a record on information media

[5] Act No. 618/2003 Coll. on Copyright and Related Rights as amended

[6] In the international context, the term standard means a norm; in Slovakia, the term norm describes a standardisation document issued by SUTN and a standard is a standardisation document issued by central government bodies

so far only an observer in the majority of the aforementioned organisations; to become a full, active member, Slovakia still lacks expert capacities, material resources and a base to be able to meet tasks arising under a full membership.

3. Strategy

The main task in information security is to develop an uniform platform for the building of information society, based on legal principles and ensuring adequate protection and credibility of Slovak digital space. In order to accomplish this task, it is necessary to create a National Strategy for Information Security in Slovakia as a basic national document and, subsequently, to elaborate on and implement the specific tasks defined under the strategy. The document builds on the principles defined under *A strategy for a Secure Information Society – "Dialogue, partnership and empowerment"* issued by the European Union in 2006, the Slovak Security Strategy, and other strategic documents of most advanced information societies, including the US, Germany, UK, Finland, Japan, etc.

The NSIS is divided into three levels. The first level specifies long-term **strategic objectives** in information security that cover all relevant problems Slovakia needs to resolve in this area.

Strategic priorities represent the second level of the NSIS, where strategic objectives translate into specialised areas; at the third level, the NSIS defines the most important problems that are then reflected in **key tasks**.

3.1 Strategic objectives

European Union strategy says it is necessary to promote global cooperation in information security and ensure that European industry is user, demanding high-level security products and services and, at the same time, their competitive provider as well. The second basic requirement of the EU is to standardise Member States' national policies pertaining to information security. When seeking to meet these requirements, the principles of a democratic society should be observed and legitimate interests of citizens, the business sector and public administration taken into account. The following strategic objectives have been set in order to ensure and maintain the necessary level of information security under the strategy:

1. **prevention:** to ensure adequate protection of Slovak digital space so as to prevent the occurrence of security incidents as much as possible;
2. **readiness:** to ensure the ability to effectively respond to security incidents, mitigate their impacts and the time necessary to restore the operation of information and communication systems after an incident has occurred;
3. **sustainability:** to achieve, maintain and upgrade Slovakia's competence in information security.

The set strategic objectives comply with the Slovak Security Strategy, approved by the National Council of the Slovak Republic in September 2005, and with the ongoing building of information society in Slovakia. The meeting of the set objectives requires that the state ensure cooperation of all government bodies, special state administration, academia, the private sector and citizens. An essential role the state plays in this intricate process is to create a suitable legislative environment and provide organisational, material and financial resources. Government tasks also include a consistent control of the fulfilment of action

plans and imposing sanctions for their non-fulfilment, as well as a flexible response to changes in external conditions.

3.2 Strategic priorities

A relevant legislative framework needs to be completed; competences, technical, organisational and financial issues, hierarchy and management, education and many other problems should be addressed in order to meet the set strategic objectives. The NSIS defines the following seven basic strategic priorities:

1. protection of human rights and freedoms in using NICI;
2. building of awareness and competence in information security;
3. creation of secure environment;
4. improvement of effectiveness in information security management;
5. ensurance of sufficient protection of the state ICI and ICI supporting the state critical infrastructure;
6. national and international cooperation;
7. enhancement of national competence.

3.2.1 Protection of human rights and freedoms

The potential offered by ICT may be misused, therefore ways should be sought to protect legitimate interests of all stakeholders involved in the use of ICT. However, traditional regulatory and defence mechanisms that society developed in the past may only hardly be carried over into the digital space. In particular ethics and moral, which are being formed gradually, belong to a private sphere of individuals, or communities at the most, and have no legal force. Good legislation is necessary in order to make sure that detected crimes tending to violate human rights and freedoms are effectively prosecuted. Amidst growing security problems of the digital space (computer crime, organised crime, terrorism) and the significance of the global (as well as national) ICI for society it will be necessary to define a legal framework for the protection of digital space (both at the international and national level). Interests and rights of various individuals and organisations coincide in this area. Proposed measures (legal arrangements) have to take into account not only interests of the state and ICT system owners, but also the rights of users and those parties whose data ICT systems contain[7].

The NSIS builds on the Slovak legal framework for the protection of information, EU directives and OECD recommendations, taking into account core technical standards. A regulation of the supreme legal force concerning the protection of human rights in the case of safeguarding the digital space is the Charter of Human Rights and Freedoms under which citizens are guaranteed a right to personal integrity and privacy, protection of human dignity, personal honour, good reputation and name, private, personal and family life, and protection against unauthorised collection, disclosure or other misuse of personal data. The Constitution of the Slovak Republic is another fundamental document. The strategy identifies two key tasks in the protection of human rights and freedoms:

[7] The security of information systems and networks should be compatible with essential values of a democratic society. (OECD Guidelines for the Security of Information Systems and Networks)

a) to pursue democratic principles in measures designed to protect Slovak digital space;

b) to lay down legislation on access to personal data in such a way that no person could have a right to misuse such data in the scope extending beyond the purpose of its processing.

3.2.2 Building of awareness and competence in information security

Analyses have shown that many security incidents are caused by insufficient expertise and knowledge of information system administrators, users, as well as information security managers. On that account, the issue of their qualification and education needs to be addressed. Qualification does not entail only education but, above all, experience in a given field and expertise obtained.

In the light of potential threats, it is necessary to achieve the required level of *security awareness* (i.e. understanding the need and nature of information security) among all its users in order to safeguard the digital space and, subsequently, translate security awareness into a *competence* (recognising and assuming one's own responsibility for information security when working with ICT). The strategy identifies the following key tasks to achieve and retain the necessary level of security awareness and competence:

a) to raise an awareness – using the Internet, mass media and methodology materials – among citizens, commercial and non-commercial organisations and public institutions of the risks related to the use of ICT and of means available to protect against threats;

b) to strengthen education activities (making the information security basics part of informatics classes at schools);

c) to introduce programmes on enhancing security awareness and competence of ICT users, with special requirements for information security.

3.2.3 Creation of secure environment

The role of the state is to create good conditions for cooperation among all involved stakeholders. It includes, in particular, laying down a legal framework, drafting strategic documents and methodology materials, determining competences, obligations and responsibility. Another important task is to create uniform information security standards and coordinate their issuing. The entire public administration, the academic and private sector, including individuals, should be involved in the preparation of conceptual documents. It is in the state's interest to have the entire digital space protected, through suitable forms of cooperation between owners and users. The strategy defines the following key tasks that lead to creating a secure environment:

a) to coordinate the protection of Slovak digital space and ensure national security;

b) to create[8] a sufficient information security legislative framework in Slovakia, taking into account human rights and freedoms and Slovakia's international commitments (especially towards the EU);

[8] analysis of the existing legislation and possible amendments or updates to it

c) to assess the existing competences and determine responsibility/define duties of state authorities in the area of information security;

d) to harmonize STN (Slovak Technical Norms) with the applicable international information security standards; coordinate issuing of information security standards in Slovakia;

e) to create a uniform methodology of non-classified information and information and communication systems security categorisation;

f) to prepare basic ICT security requirements mandatory for the state ICI, and optional for other NICI components (mainly for e-Health, e-Government system and KRIS), compatible with international norms and standards.

g) to prepare and make available methodology materials with a goal to achieve the required/basic level of information security (guidelines and best practices); to promote convergence of best-practice based security procedures applied by the state and private sector;

h) to promote solutions and services based on available (open) standards in order to improve availability of security solutions to small businesses and individuals;

i) to engage the commercial sector and expert public in the process of drafting and reviewing conceptual documents, norms and standards; to create room for knowledge and experience exchange.

3.2.4 Improvement of effectiveness in information security management

In order to achieve and retain the required level of information security it is necessary to coordinate the protection of organisation's assets and, at the same time, develop an effective system of its management. Improving the quality of management requires that institutions would be provided with not only the methodological assistance while solving conceptual issues, but also with the support in solution of particular urgent problems (including preparation of regulations, methodology documents and trainings, as well as advice and technical assistance). In this respect, security level should be monitored and evaluated, with respective statistics on security incidents being provided to target groups, in order to make management more effective. The following tasks should be set in order to resolve the aforementioned problems:

a) threat monitoring;

b) creation of an early warning system (notification of target groups about existing threats, warning of possible target groups, alarm signalling);

c) help with security incidents solutions;

d) identification, recording and evaluation of security incidents;

e) monitoring effectiveness of measures proposed to resolve security incidents;

f) coordination of security strategies of individual NICI system to ensure cooperation in NICI management.

3.2.5 Ensurance of sufficient protection of state ICI and ICI supporting the state critical infrastructure

The state as an owner of information and communication systems is obliged to ensure their adequate protection so that no damage is caused if they are attacked, or that such damage is minimal. They mainly include systems that are part of the state critical infrastructure which ensures the functioning of the state, services in industry, energy sector, healthcare and social security, transport, banking, etc. The Slovak Security Strategy, approved by the National Council of the Slovak Republic in 2005, implies that "the Slovak Republic will take measures to reduce vulnerability of critical infrastructure components, with focus on information and communication systems, and to minimise negative impacts of attacks against them. It will continue its activities focused on the security and integrity of information and communication systems, particularly systems that are essential for the safe performance of the basic functions of the state." The issue of information protection in critical infrastructure is also addressed by the National Programme for the Protection and Defence of Critical Infrastructure in the Slovak Republic, approved by government resolution No. 185/2008 of 26 March 2008. Since the critical infrastructure involves even non-state systems and the state is a partner to citizens and private companies in administrative as well as commercial matters, the state must, in addition to the protection of its own systems, ensure security awareness raising among the general public and promote reasonable security requirements for non-state systems. Tasks to ensure sufficient protection of state ICI and ICT systems supporting the state critical infrastructure are as follows:

a) to improve information security level in state institutions through the introduction of an information security management system;

b) to implement and promote the use of secure ICT-based products and services;

c) to prepare framework conditions, guidelines and recommendations (stipulating binding framework security requirements (security standards) for systems controlled by individual state authorities, and guidelines on how to meet them; and/or recommendations for systems not controlled by state authorities).

d) analyse the security level of that part of the NICI which represents a component of the state critical infrastructure, or supports it; update adopted or adopt new measures if necessary.

3.2.6 National and international cooperation

Given the global nature of information security, local solutions often prove insufficient. Active involvement in the activities carried out by key international organisations, such as ENISA, OECD, CERT, ISO, etc., is necessary. To that end, the following is needed:

a) to coordinate national efforts in the protection of Slovak digital space;

b) to effectively engage in international cooperation based on an analysis of Slovakia's needs and options in the area of information security.

3.2.7 Enhancement of national competence

Highly qualified experts, reliable ICT-based products and credible IT services, along with the sponsorship and helpfulness of the state and other stakeholders, are important in order to sustain the necessary level of protection of Slovak digital space. The following is needed in this area:

a) to analyse qualification needs in Slovakia with respect to information security, possibilities of curricular and extra-curricular education and training, and introduce a training system;

b) to promote research and development aimed at possible and existing problems in information security (in particular, intensified cooperation of the state, the private sector and academia);

c) to use the results of international cooperation to support economic competitiveness (providing information about problems, solutions, trends, legislation and standards, international initiatives in information security).

3.3 Information security management structure

3.3.1 Existing management structure

Slovakia has currently a 3-tier information security management structure in place, based on Act No. 575/2001 Coll. on organisation of the activities of the Government and organisation of the central public administration, as amended, and on amendments to certain acts (the Transfer of Powers Act). The Government of the Slovak Republic, which discusses and approves strategic and conceptual materials, is the supreme body. These materials are submitted to the government by individual ministries pursuant to their powers laid down by relevant laws. The 2nd tier includes a central government body responsible for information security in public administration, currently the Ministry of Finance of the Slovak Republic, and other state authorities and offices responsible for specific aspects of information security, such as Ministry of Defence, Ministry of the Interior, Ministry of Economy, Ministry of Culture, Ministry of Education, the National Security Authority, the Office for Personal Data Protection, and the Slovak Office of Standards, Metrology and Testing. The 3rd tier consists of organisational units of state authorities that perform particular tasks in the field of information security. Department of legislation, methodology, standards and information system security of the Information Society Section at the MF SR and directly coordinated Committee for Information Security, chaired by a director general of the Information Society Section, has both a specific position. Pursuant to its statute[10] the Committee performs analytical and conceptual activities and prepares strategic and technical materials on information security.

3.3.2 Proposal for a new arrangement

The proposal for a new structure builds on the existing management structure *"government - MF SR, other central government bodies and authorities that are presently competent for information security."* Based on an in-depth analysis of the existing security processes, competences should be optimised (a material to be submitted to the government is under preparation). The next step will be the setting up of a national centre for computer security incidents, CSIRT.SK (Section 3.4.1 and Annex 4). Within the next five years, the issue of information security in Slovakia will need to be settled in terms of applicable

[10] Statute of the Committee for Information Security, *IRA_MFSR_12.2007_ROM.kom.inf.bezpečnosť, Číslo : MF/ 14462/2007 – 23*

legislation (drafting an act on information security), organisation and staffing; due attention should also be given to funding. A national institution for information security of non-classified segment of the NICI (a National Information Security Authority of the Slovak Republic (NISA)) is recommended to be formed in the final stage. A more detailed approach to safeguarding information security in Slovakia will be included in an action plan to NSIS, to be prepared by the end of 2008.

3.4 Current priorities for information security in Slovakia

The current priorities in information security are driven by an unfavourable situation in this field in Slovakia, and by Slovakia falling considerably behind countries advanced in terms of information society development. The unfavourable situation is mainly caused by poor implementation of objectives specified in strategic documents, absence of a state concept of information security and interoperability framework in Slovakia, legislation, competences, awareness, support from competent bodies and other factors.

3.4.1 CSIRT.SK

The aim of this task is to prepare a proposal on how to ensure organisational, personal, material, technical and financial resources for a contact point for security incidents, and subsequent formation of a specialised organisation to combat computer crime and ensure mutual cooperation, exchange of information and experience at the domestic level with links to a Europe-wide environment. The institution will perform the tasks specified in Section 3.2.4 (the first 4 tasks in particular). It will also participate in performing tasks specified in Section 3.2.6, action plan tasks, etc. This fact is also appreciated by international organisations concerned with IT security, which have pointed out that there is no contact point available in Slovakia in the case of international IT security incidents. Given the lack of expert capacities in the field of information security, CSIRT.SK is expected to also utilise personnel capacities of non-state organisations. Since this situation will only be provisional, CSIRT.SK will have limited powers. It will later be necessary to consider enhancing its executive powers laid down by the law.

3.4.2 Coordination of standardisation activities

Standards are a means to achieve international interoperability of all solutions and the necessary level of information society. Slovakia **has no access** to international standards under preparation, the publication of standards is not coordinated; **equally**, there is **no overview** of relevant international norms and no funds for their introduction into STN. Slovak representatives participate in international standardisation organisations only sporadically. Problems also stem from **fragmented competences**, dual publication of standards and their mutual incompatibility. A solution could be to better allocate competences and coordinate preparation and publication of norms and standards in key organisations including MF SR, MoH, MoC, the NSA, the Geodesy, Cartography and Cadastre Authority of the Slovak Republic, and the SOSMT. Participation of Slovak representatives in international standardisation organisations is necessary when transposing approved standards. On that account, an overview of standardisation activities in the field of information security needs be prepared with respect to:

a) powers of Slovak authorities in issuing of standards;

b) existing Slovak standards;

c) international standardisation organisations;

d) international standards that Slovakia should adopt;

e) de facto standards[11],

f) Slovakia's capacities for competent standardisation activity;

g) Slovak representation in international standardisation organisations and initiatives.

Based on this overview, a proposal could be made on the allocation of competences in standardisation activities and coordination of updates to existing and/or publication of new norms and standards, as well as a mechanism to control the compliance with the existing norms and standards.

3.4.3 Knowledge building and dissemination

Knowledge building and dissemination is a precondition for improving employees' qualification and level of expertise in information security. This mainly involves production of knowledge, which is a result of a creative, scientific and technical research. Knowledge dissemination, i.e. reproduction, is related to education and training in educational institutions. Knowledge of information security can be categorised as follows:

a) general basic knowledge – on a level of a user who needs to know what to do and what not to do, but does not need to understand causes in detail;

b) general IT knowledge – on a level of an IT specialist, but not an information security expert, who knows the system, is able to implement and maintain its security mechanisms based on recommendations (security policies) and transform security requirements into system operating rules;

c) specialised security knowledge – on a level of an information security expert who can analyse the system and its security environment, perform a risk analysis and propose measures to eliminate risks, or comprehensively assess system security (auditor); The expert is familiar with the existing situation and trends in threats and security solutions, managerial and legal aspects of information security, and is capable of producing conceptual materials;

d) application security knowledge – on a level of an expert in a different field (lawyers and investigators in particular) who, when performing his/her tasks, needs to understand the nature of security problems and is able to cooperate with specialists at all levels;

e) innovative knowledge – on a level of a research specialist in information security (or some of its sub-fields) enabling him/her to find fundamentally new solutions.

Along with IT and expert training, language skills are equally necessary; in Slovakia, due attention should be given to education in all aforementioned categories.

3.4.4 International cooperation

[11] generally accepted technical norms which, formally, do not have the status of a standard (e.g. PKCS in the case of electronic signature and cryptology)

Slovak membership in the EU, OECD, ISO and other international organisations implies obligations but also a possibility for Slovakia to participate in the policy making by these institutions so that their policies takes also account of Slovakia's interests. Bodies of those international institutions which perform this activity in the field of information security should be identified; subsequently, it is necessary to make sure that Slovakia is represented by qualified experts on such bodies. Cooperation also requires that appropriate conditions be created for activities performed by, and ensuring participation of, Slovak experts in these specialised bodies.

The Committee for Information Security at the MF SR will serve as a coordination authority for international activities in the field of information security of the non-classified segment of the NICI. In addition to active involvement in international organisations, bilateral and multilateral cooperation in addressing specific problems (e.g. information security standardisation in Slovakia and the Czech Republic, recognition of digital signatures, etc.) will need to be facilitated as well. International cooperation can contribute to knowledge dissemination and increasing numbers of qualified experts in Slovakia.

3.4.5 Education and training

A critical factor directly affecting the ability to find and implement adequate solutions to security problems is people's competence which is closely related to obtaining knowledge. In this respect, the following needs be analysed:

a) knowledge needs of individual ICT user categories (lay users, IT specialists and information security experts);

b) capacity and content possibilities of in-school and other types of training (lifelong learning, corporate trainings, e-learning, ECDL, EUCIP, etc.);

Based on that analysis, the following should be proposed:

c) to include information security into IT or other classes taught at secondary schools;

d) a lifelong learning scheme (basic and follow-up training courses) for IT specialists (system administrators) from the state and private sector;

e) to publish and support publishing of specialised literature and methodology documents addressing particular issues of information security.

Education and publication of specialised literature are directly addressed under task No. 3 in Section 4.2. A simplified form of the task, which should be updated, is included in the Action Plan for Information Society under *3.c.2.*

4. Delivering the strategy

4.1 Strategy implementation

Implementation consists in approving the NSIS document by the Slovak government, resolving the key tasks defined under the strategic priorities, and preparing a Slovak information security action plan for 2008-2013 and its approval by the government. Progress reports, including task assessments, will be submitted to the government on an annual basis, along with any proposals.

4.2 Framework schedule for the performance of tasks in 2008

The tasks defined for the forthcoming period are based on the current state of play in information security in Slovakia compared to the situation in other EU Member States and other advanced countries of the world. They are proposed in accordance with key EU/EC documents, directives and recommendations, and strategic priorities defined under this document.

The following tasks have been defined:

1. To prepare a proposal for organisational, personnel, material, technical and financial arrangement for the formation of a specialised unit (CSIRT.SK) to address computer security incidents in the Slovak Republic. CSIRT.SK will:
   - collect knowledge of existing threats and possible solutions, and publish them;
   - serve as an early warning centre;
   - assist in addressing security incidents;
   - collect information on security incidents and their effects in Slovakia;
   - cooperate with similar institutions abroad;
   - systematically assist in building similar units in state and private organisations in Slovakia;
   - bring together experts on information security and train new experts by engaging them in its operations.

   Linkage between this task and other action plan tasks and key National Strategy tasks will be described in more detail in a “Draft action plan for 2008-2013”.

2. To prepare a legislative basis for the drafting of an act on information security in the Slovak public administration and draft an update to decree of the Ministry of Transport, Posts and Telecommunications No. 1706/M-2006 on standards for public administration information systems, i.e. to revise its Part Five, “Security Standards”.

3. To prepare a proposal of an information security training system. The aim of this task is to find out what individual NICI users should know about information security, how to teach them that, and prepare a specific solution for lay users/IT specialists in the state administration. This task involves:

   a) preparation of a feasibility study to analyse the following:
      - how experts on information security, IT specialists and lay users are trained in the world;
      - the current situation in information security trainings in Slovakia;
      - training needs (who needs to know what, to what extent);
      - who and under what conditions could provide necessary trainings;

   b) preparation of a proposal for a training system for IT specialists from state authorities:
      - two target groups (basic training for lay users, lifelong learning for IT specialists to update their knowledge);

- drafting a proposal for the organisation and content of trainings;
- draft training programme;

c) preparation of a pilot project for the information security training of lay users/IT specialists from public administration.

4. To draft an action plan to the National Strategy for Information Security in the Slovak Republic for the 2008-2013 period;

5. To prepare an overview of standardisation activities in the field of information security. The aim of this task is to summarise all information security norms which Slovakia might find useful, both the existing ones and those under preparation; what is the situation with information security norms and standards in Slovakia; who is responsible for their publication. Outcomes of this project could serve as a basis for updating STN applicable to information security; aligning and improving publication of norms and standards in Slovakia; as well as for Slovak activities in international standardisation organisations. The output will be an analytical study with the following content:
   - a summary of relevant international standardisation organisations and Slovak representation therein;
   - a summary of competences of Slovak organisations in standardisation activities;
   - a summary of existing Slovak norms (currently applicable as well as to be cancelled);
   - a list of norms which need be included into STN;
   - a summary of useful standards which, however, are impossible to be included into STN;
   - an analysis of the current state of play, shortcomings and a proposal on how to address the existing situation in standard-setting in the field of information security in Slovakia.

   Based on this overview, a proposal could be made on the allocation of competences in standardisation activities and coordination of updates to existing and/or publication of new norm and standards.

6. To analyse the situation in information security in Slovakia. Four basic sources of information may help to characterise the situation in information security:
   - published studies, statistics, analyses from domestic and foreign sources;
   - internal analytical studies (focused either on an system or product analysis or on a survey into situation in selected NICI segments);
   - data from security incident monitoring;
   - obligatory reports, for example on the computer programmes used, security solutions, security incidents, etc. [12]

[12] this source of information could be used at least in the state segment of the NICI

An information collection and processing system needs to be created, which will help to continuously create a picture of the situation in information security in Slovakia and prepare an annual report, including requirements for information resources, proposal for the use of processed information (what will be provided to who, under what conditions and what will be published). Alongside creating the system, it is necessary to continuously prepare information on the situation in information security in at least selected areas (malicious software, spam, illegal software) and publish such information.

7. To issue methodology documents on information security. The first such document will be an information security dictionary which should, in particular, unify information security terminology for the purposes of drafting legislative materials and strategic documents. The dictionary should be updated once in 2 years.

4.3 Financial resources and time schedule

4.3.1 Financial resources for 2008

Financial resources to be allocated from the state budget in 2008 under the proposed material are covered from a MF SR budgetary chapter. Individual tasks, estimated personnel capacities and deadlines are shown in the table below.

Table: General cost estimate and deadlines for 2008

	Task	Estimated time capacity (man-hours)	Estimated costs ('000 SKK)	Deadline	Responsible body	Note
1.	CSIRT.SK proposal	600		31. 12. 2008	MF SR	proposal
2.	Situation overview concerning standardisation activities (situation, norms)	1500		30. 11. 2008	MF SR	Study
3.	Analysis of the state of information security in Slovakia	600		30. 11. 2008	MF SR	study
4.	Proposal of a training system, including implementation of a pilot project	2000		31. 12. 2008	MF SR	Study, system, pilot, methodologies
5.	Action plan to the strategy			31. 03. 2009	MF SR	proposal
6.	Information security terminology dictionary	1600		31. 12. 2008	MF SR, Ministry of Culture	electronic issues
7.	Legislative basis for an information security act	600		31. 12. 2009	MF SR	proposal
	Total general costs		**6 000**			

4.3.2 Financial resources for 2009-2013

Financial resources for the 2nd phase of the tasks for 2009 – 2013, including quantification, deadlines and estimated costs, will be included in an action plan to the strategy. The funding is proposed from the state budget, the MF SR budgetary chapter and other chapters, and from EU Structural Funds under the Operational Programme Information Society (OPIS). On that account, the drawing of funds for performing proposed activities will need to be brought into compliance with conditions and rules for the drawing of Structural Funds; they will be provided within approved limits. Some activities are expected to be co-financed by the private sector.

5. Conclusions

The NSIS has been prepared for a five year period, i.e. from 2008 to 2013; the funding is expected to be provided from the state budget, Structural Funds under OPIS and the private sector. The document was prepared by the MF SR in cooperation with the academic and private sector. It was subsequently discussed by an advisory body to the Minister of Finance, i.e. the Committee for Information Security. The content of this document is based on strategic materials approved by the Slovak government, and EU/EC directives, regulations, recommendations and strategic materials.

The rate of return on funds to be spent on safeguarding information security cannot be directly quantified; the implementation of effective security solutions reduces the risk of security incidents which would cause losses resulting from damage to and inaccessibility of information and communication systems, misuse of information, or threats to the functioning of control, production and/or other systems. To measure whether the funds have been spent effectively will only be possible after the data on the number and impacts of security incidents before and after the implementation of security safeguards is available. So far, impacts may only be estimated based on information from abroad[13]. Effects of information security, besides reducing financial impacts of security incidents, can be evaluated with respect to Slovakia's credibility abroad and creating conditions for citizens and business entities. This requires expeditious elimination of security problems originating from sources located in Slovakia (attacks on foreign systems from computers in Slovakia, dissemination of illegal content from Slovakia, international crime using the Slovak NICI) and Slovakia's competent engagement in international cooperation in the field of information security. Positive impacts can also be felt in relation to the implementation of eGovernment, eHealth or eBusiness projects, as well as in terms of the protection of copyright, disclosure of future requirements for products (future standards) etc. Impacts of information security will be assessed separately in a joint material[14] being prepared by the Ministry of Economy, part "*6. Description of the method to analyse impacts on the building of information society"*.

[13] Implementation of a EUR 570,000 worth anti-spam equipment in the Netherlands translated into an 85-percent reduction in spam of Dutch origin.

[14] The material entitled "Draft uniform methodology for the assessment of selected impacts" (hereinafter referred to as "uniform methodology") was prepared in compliance with the Manifesto of the Government of the Slovak Republic, government resolution No. 833 of 3 October 2007, and the National Lisbon Strategy which includes impact assessment of regulations among its priorities.
"In order to make progress in this area, the Government of the Slovak Republic approved on 3 October 2007 resolution No. 833 on the Better Regulation Agenda in the Slovak Republic and *Programme of Action to Reduce Administrative Burden on Business in the Slovak Republic 2007-2012"*.