NATIONAL SECURITY AUTHORITY

Action Plan for the Implementation of the Cyber Security Concept of the Slovak Republic for 2015-2020

National Security Authority I Bratislava, Budatínska 30, Post code: 85 106, Slovakia I www.nbusr.sk

Table of Contents

Introduction

Cyber security is emphasised as a priority in many planning and strategic documents of the European Union ("EU") and the North Atlantic Treaty Organisation ("NATO") as well as in documents of other important organisations around the world where cyberspace disruption is recognised as one of the key threats of the modern age. For this reason, progressive governments are moving to deploy effective measures focused on building up and strengthening cyber capabilities with the goal of preventing, registering, defending against and recovering from cyber-attacks. The EU defined starting points and cyber security goals within its cyberspace in the EU Cyber Security Strategy, while the principles, goals, priorities and processes of building cyber security in Slovakia are linked in particular to strategic and legislative documents in addition to this important document.

- **National Strategy for Information Security in the Slovak Republic, approved by Slovak Government Resolution No. 570/2008,**
- **Information Encryption Concept, approved by Slovak Government Resolution No. 771/2008,**
- **Proposed System of Education in the Area of Information Security/Cyber Security in the Slovak Republic, approved by Slovak Government Resolution No. 391/2009,**
- **Proposal of organisational, human, material, technical and financial resources to create a specialised computer incident response unit in Slovakia – CSIRT.SK, approved by Slovak Government Resolution No. 479/2009,**
- **Draft Action Plan 2009 – 2013 for the National Strategy for Information Security in the Slovak Republic, approved by Slovak Government Resolution No. 46/2010,**
- **Legislative intent of the Information Security Act, approved by Slovak Government Resolution No. 136/2010,**
- **European Union Cyber Security Strategy: An open, safe and secure cyberspace, approved by the European Commission 7 February 2013,**
- **Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA,**
- **Progress reports for the National Strategy for Information Security in the Slovak Republic and the Action Plan from 2009 to 2014, submitted to the Slovak government,**
- **Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union,**
- **Cyber Security Concept of the Slovak Republic for 2015 - 2020 ("Concept") approved by Slovak Government Resolution No. 328/2015,**
- **Progress reports based on the Preparations to fulfil cyber defence tasks based on the competence objectives of the Slovak Republic material, approved by Slovak Government Resolution No. 334/2015.**

Creating conditions to build up national cyber capabilities was characterised with other activities in the area of preparation, creation and submission of strategic and planning materials for the area of cyber security in Slovakia. As such, the Director of the National Security Authority was assigned Task B.3 from Slovak Government Resolution No. 328/2015 of 17 June 2015 to

prepare and submit the Action Plan for the Implementation of the Cyber Security Concept of the Slovak Republic for 2015-2020 ("Action Plan").

For urgency and efficiency reasons, the entire task of fulfilling Concept tasks in the 2015-2020 period is divided into period with specific tasks for fulfilment in 2015 with the remainder to follow from 2016 to 2020. Key tasks in the short-term and tasks in the preparatory phase were completed by the end of 2015.

Such tasks include in particular

- **adoption of Act No. 339/2015 Coll. amending Act No. 575/2001 Coll. on Organisation of the Activities of the Government and Central State Administration as amended, which defined the National Security Authority as the central government body for cyber security;**
- **establishment of the Cyber Security Committee, the statute of which as debated and acknowledged by the Slovak Government (material no. UV-33740/2015);**
- **adoption of Act No. 346/2015 Coll. amending Act No. 110/2004 Coll. on the Peacetime Operation of the Security Council of the Slovak Republic as amended by Act No. 319/2012 Coll. establishing the Cyber Security Committee of the Security Council of the Slovak Republic.**

Fulfilment of the second phase (2016 – 2020) is described in more detail in the Action Plan. The National Security Authority is responsible for the Action Plan while fulfilment of the defined tasks requires the full cooperation of other entities. As such, responsibility for the tasks is assigned to other central government bodies, including entities within their material areas.

Fulfilment of tasks in the Action Plan for 2016-2020 is divided into seven strategic areas, specifically:

1) **Building an Institutional Framework for Cyber Security Administration.**
2) **Creation and Adoption of a Legal Framework for Cyber Security.**
3) **Development and Application of Basic Mechanisms Providing for the Administration of Cyber Space.**
4) **Support, Formulation and Implementation of an Education System in the Area of Cyber Security.**
5) **Determination and Application of Risk Management Culture and Communication System Between Stakeholders.**
6) **International Cooperation.**
7) **Support of Science and Research in the Area of Cyber Security.**

The Action Plan defines tasks and the manner of their implementation, a responsible party, cooperating parties and a time frame for completion (deadline or length of time) for each individual area. The tasks are detailed in every area to meet the individual strategic goals of the Concept and achieve a level where the level of protection of national cyberspace is systematically increased in Slovakia by a system operating in a strategic, coordinated, effective and efficient manner on a legal basis and with awareness of security and its importance among all elements of society.

The proposal of these tasks also clearly defines the goal of active participation of the private sector, the academic community and civil society in forming and implementing Slovakia's

policy in the area of cyber security and to ensure effective cooperation at the national and international level.

It must be emphasised that the tasks and measures for their implementation are adequate and respect the right to protection of the privacy of inhabitants and basic human rights and freedoms to an appropriate extent.

The individual tasks in the Action Plan represent dynamic units that may be updated as needed based on research and current conditions and situations in the area of cyber security. The scope of tasks in individual areas, the time frame for their completion and responsible parties, are detailed in the following task table.

Task table

AREA 1: BUILDING AN INSTITUTIONAL FRAMEWORK FOR CYBER SECURITY ADMINISTRATION

Task no.	Task	Method of implementation	Responsible party	Cooperating party	Time frame for completion
1.1.	Prepare a proposal to create a formal platform for cooperation.	Secure conditions for the Cyber Security Committee and its working groups established on a platform of cooperation between the public sector, academic community, scientific circles and the private sector.	NSA	Academic community Associations	continuously
		Establish a working committee for cyber security in the Security Council of the Slovak Republic and secure organisational conditions for its activities.	Gov't Office	NSA	2016 and on a continuous basis
1.2.	Create conditions for the performance of competencies of applicable authorities involving cyber security within their material areas.	Complete a proposal of the human resources and material and technical prerequisites needed to perform the competencies of competent authorities for cyber security.	CSA		04/2016
		Create conditions for material and technical assurance and the consolidation of organisational and human resources and the fulfilment of the basic tasks of competent authorities.	CSA		continuously
		Secure cooperation with competent authorities for cyber security.	CGBs		2016-2020
1.3.	Secure an institutional framework of cyber security management.	Create a national cyber security centre within the material area of the authority.	NSA		2017
		Create an inter-departmental working group to respond to large-scale computer/cyber-attacks and a fast response team with operative steps taken in the event of a potential threat to Slovakia's cyber space.	NSA	MoF MoI MoD SIS	2016 and on a continuous basis
1.4.	Build up cyber security competencies.	Build out the competencies of CSIRT.MIL.SK as the incident response unit to defend Slovakia and responsible for active cyber protection, the capabilities of military mobile networks and the implementation of cyber security elements into departmental data networks.	MoD		2016-2020
		Build out selected CSIRT.SK (government unit) capabilities in the Data Centre in the material area of	MoF	DC/CSIRT.SK	2016-2020

Task no.	Task	Method of implementation	Responsible party	Cooperating party	Time frame for completion
		the Ministry of Finance of the Slovak Republic.			
		Establish a unit in its material area and build out its capabilities.	Gov't Office	NASES	2017
		Secure the establishment and performance of activities by the section designed to respond to CERT/CSIRT-type incidents or secure these activities by utilising existing sections/units active in the material area of another competent authority in accordance with the provisions of the Cyber Security Act.	CSA		2017-2020
1.5.	Create a framework for cyber security management during states of emergency, martial law, hostilities and war.	Propose the institutional management of cyber security during states of emergency, martial law, hostilities and war.	NSA	MoD MoI Sec. Council	2017/18
		Propose a contingency plan for the transfer of responsibility for the management of cyber security during peacetime, states of emergency, martial law, hostilities and war under Constitutional Act No. 227/2002 Coll.	NSA	MoD MoI Sec. Council	2017/18
1.6.	Create an inter-departmental/multi-departmental budget program titled "Protection of the Cyberspace of the Slovak Republic".	Submit the multi-departmental budget program titled "Protection of the Cyberspace of the Slovak Republic" to the Slovak government for approval.	NSA	MoF MoI MoT MoE MoD Gov't Office SIS	06/2016
		Submit the "Protection of the Cyberspace of the Slovak Republic" implementation plan for the period until 2025 to the Slovak government; the plan includes a summary of projects, activities, work and deliverables completed to fulfil the objectives and goals following the budgetary rules for the multi-departmental budget program.	NSA	MoF MoI MoT MoD Gov't Office NASES	12/2016

AREA 2: CREATION AND ADOPTIONG OF A LEGAL FRAMEWORK FOR CYBER SECURITY

Task no.	Task	Method of implementation	Responsible party	Cooperating party	Time frame for completion
2.1.	Create the legislative conditions needed for the area of cyber security.	Prepare a draft Cyber Security Act and submit it within the formal legislative process.	NSA	MoF CSA NASES CSIRT.SK	06/2016
		Submit the draft Cyber Security Act to the Slovak government.	NSA	MoF	09/2016
		Create the conditions for implementation of specific provisions of the Cyber Security Act in its material area.	Obliged parties		From 2017
2.2.	Align related legal regulations with the Cyber Security Act.	Conduct analysis of the environment and prepare a list of legal regulations with a proposal for their amendment and a schedule.	NSA	CGBs	06/2017
2.3.	Prepare executing regulations to the Cyber Security Act and secure due legislative process (approval) thereof.	Prepare executing regulations defining the details in specific areas based on blanket standards in the Cyber Security Act.	NSA	CGBs	06/2017
2.4.	Publish standards, methods and guidelines in the area of cyber security.	Establish working groups in the material area of the National Security Authority's Cyber Security Committee for: - cyber-crime and computer-based criminality - methods and standards - terminology in the area of cyber security.	NSA		04/2016
		Publish standards, methods and guidelines.	NSA	SOSMT CSA SIS	continuously
		Establish a central access point for standards to protect critical infrastructure elements and ensure the regular updating of its contents.	NSA	SOSMT DC SNAS NASES	06/2017
2.5.	Terminology in the area of cyber security.	Update the crisis management glossary in accordance with the materials produced by the National Security Authority's Cyber Security Committee in the area of terminology and add new terms as needed.	Gov't Office	CSA NSA Sec. Council	06/2016
		Create a terminology-based reference glossary to unify the terms used to create planning, strategic and legislative materials in the area of cyber security and secure their updating.	NSA	Academic community	06/2017 and then continuously

AREA 3: DEVELOPMENT AND APPLICATION OF BASIC MECHANISMS PROVIDING FOR THE ADMINISTRATION OF CYBER SPACE

Task no.	Task	Method of implementation	Responsible party	Cooperating party	Time frame for completion
3.1.	Create a risk assessment method for risks in cyberspace.	Elaborated a risk assessment method for the area cyber security at the national level.	NSA	Academic community Associations	12/2016
		Create processes to analyse status levels, assess the current status level and propose security measures to mitigate/minimise risks and potential crisis situations on a national scale.	NSA		2016 (annually)
3.2.	Introduce unified measures at the level of competent authorities within the mechanism of prevention.	Introduce measures to minimise potential risks and crisis situations within its material area.	CSA		2018
3.3.	Create processes and mechanisms during coordination of securing protection for the state's important information assets at the national level.	Create a method for joint processes and support (a hotline) to ensure prevention and readiness to respond against disruption of critical infrastructure information assets.	MoF	NSA MoI DC/CSIRT.SK	2016
3.4.	Create and implement an early warning and incident response system.	Implement a unified early warning, incident response and information exchange system based on the schedule to mitigate the risks associated with threats to information and communication systems and ensure their uninterrupted operation in accordance with fulfilment of "OAS02 Inter-departmental programme to protect critical infrastructure in the Slovak Republic."	NSA	DC/CSIRT.SK CSA/Incident response unit	2016-2020
		Establish the National Portal for Cyber Security as a part of the central government portal.	Gov't Office	NASES	2017

Task no.	Task	Method of implementation	Responsible party	Cooperating party	Time frame for completion
3.5.	Propose minimum security measures for individual categories of information assets within the security incident response mechanism and ensure their implementation.	Introduce individual measures at the national level with the objective of providing a qualified and effective response to security incidents.	NSA	CSA	2018
		Propose and introduce rules to block attacks in order to increase Slovakia's defensive capabilities against cyber-attacks on major information systems from the external environment/Internet, in particular against the dissemination of harmful code from networks of infected computers and the dissemination of harmful activity from the Slovak IP address range.	NSA	DC/CSIRT.SK NASES SIS	2016
3.6.	Update the crisis response plans for the area of cyber security.	Update catalogue pages and supplement as needed to reflect cyberspace security incidents.	NSA		2017
3.7.	Regularly review the level of security in government networks and critical infrastructure.	Conduct internal and external penetration tests of information systems in selected public organisations, including elements of critical information infrastructure and major information systems.	MoF	CGBs DC/CSIRT.SK Operators of critical information infrastructure elements SIS	continuously

AREA 4: SUPPORT, FORMULATION AND IMPLEMENTATION OF AN EDUCATION SYSTEM IN THE AREA OF CYBER SECURITY

Task no.	Task	Method of implementation	Responsible party	Cooperating party	Time frame for completion
4.1.	Map the current status of education in the area of cyber security.	Map the current status of education in the area of cyber security within the following systems: a) general education (primary and secondary level of education) and b) specialised education (secondary and university level of education, specialists).	MoE		06/2016
4.2.	Secure education in the area of cyber security.	Complete a proposal to innovate and secure education in the area of cyber security within the general education system (primary and secondary level of education) and support specialised education (secondary and university level of education, specialists) based on the results of the mapping of the current status of education.	MoE	NSA MoD SIS MoI NASES	03/2017
4.4.	Create a National Education Centre in the area of cyber security.	Create a National Education Centre in the area of cyber security to secure education and achieve, at a minimum, a basic level of competencies in the area of cyber security among all educational employees in regional schools and innovate the practical training of future teachers at the individual levels of education.	MoE	MoL	06/2017
4.5.	Systematically increase awareness of cyber security aspects.	Ensure the dissemination of knowledge concerning security threats, security risks and rules of conduct in government information systems	NSA	MoF MoC MoL NASES	continuously
4.6.	Secure cyber security training.	Expand the content of existing training in the development of the Govnet network and the central government portal to include the area of cyber security.	Gov't Office	NASES	2016-2020
		Expand the existing education project for public employees to include specific new areas and ensure continuing education.	NSA	Academic community	2017
		Conduct training activities for government employees in the area of protection of information assets from external cyber-attacks.	MoF	DC/CSIRT.SK	

Task no.	Task	Method of implementation	Responsible party	Cooperating party	Time frame for completion
4.7.	Create academic programmes within life-long education for professional soldiers.	Create programmes in the Education Centre at the Armed Forces Academy for all professional soldiers who are ICT specialists focused on cyber security.	MoD		2016-2017
		Create programmes in the Education Centre at the Armed Forces Academy for all professional soldiers focused on cyber security.	MoD		2017-2019
4.8.	Secure education in the area of information and cyber security within judicial authorities.	Introduce a minimum level of systematic education for all judges and prosecutors at all levels.	MoJ	GPO Jud. Acad. Court Council	2016-2020
		Introduce enhanced education for select judges and prosecutors at all levels.	MoJ	GPO Jud. Acad. Court Council	2016-2020
4.9.	Secure education in the area of information and cyber security within investigative bodies.	Introduce a minimum level of systematic education in the area of cyber security for investigators at all levels.	MoI	Police Force Academy	2016-2020
		Introduce enhanced education in the area of cyber security for select investigators at all levels.	MoI	Police Force Academy	2016-2020
4.10.	Secure the creation of a description of qualifications in the area of information and cyber security within the national system of qualifications in Slovakia.	Conduct analysis of the current situation for the area of ICT security and prepare a proposal to supplement the list of qualifications in cooperation with relevant central government bodies and submit this material to the Slovak government.	NSA	MoL	2017

AREA 5: DETERMINATION AND APPLICATIONOF RISK MANAGEMENT CULTURE AND COMMUNICATION SYSTEM BETWEEN STAKEHOLDERS

Task no.	Task	Method of implementation	Responsible party	Cooperating party	Time frame for completion
5.1.	Create an effective model of cooperation at the national level between individual cyber security entities.	Complete a proposal for cooperation at the national level between incident response units (CERT/CSIRT, etc.) for the purposes of exchanging and sharing information, in particular regarding security incidents.	NSA	CSA	2016
		Create a secure communication channel used by individual units to automate the receipt and processing of reports of serious cyber security incidents for incident response units.	NSA	DC NASES	2017
5.2.	Implement a system for reporting and responding to security incidents.	Implement an on-line system for reporting and responding to security incidents.	NSA	DC/CSIRT.SK NASES	2017

AREA 6: INTERNATIONAL COOPERTION

Task no.	Task	Method of implementation	Responsible party	Cooperating party	Time frame for completion
6.1.	Actively participate within EU membership in the preparation and implementation of legislative and non-legislative initiatives involving cyber security.	Secure the active participation of experts in involved working groups and committees of EU institutions, in particular within negotiations and the implementation of the Network and Information Security Directive.	NSA	MoFEA, MoF	continuously
		Secure the active participation of experts in programmes, projects and other initiatives involving information/cyber security within the context of the multi-year EU 2014-2020 financial framework and implementation of the EU Cyber Security Strategy and the single digital market.	NSA	MoFEA MoF	continuously
		Cooperate and actively participate in activities at international platforms within international organisations.	MoFEA	NSA MoF	2016-2020
6.2.	Support NATO collaboration in the area of cyber security within NATO membership.	Sign a memorandum of cooperation in the area of cyber defence.	NSA	MoD	02/2016
		Support collaboration with NATO in the area cyber defence, in particular with respect to the response to computer security incidents and the exchange of technical information on threats and vulnerabilities.	NSA	MoD MoFEA	2016-2020
		Sign a “Statement of Interest” regarding Slovakia's accession to the NATO MISP (Malware Information Sharing Platform) project.	NSA	MoD MoFEA	06/2016
6.3.	Cultivate relations and engage in bilateral cooperation with specific countries in the central European region in the area of cyber security.	Actively participate in, develop and support collaboration within V4 countries, in particular through the Central European Cyber Security Platform (CECSP).	NSA	DC MoD	continuously
		Engage in and deepen bilateral cooperation with countries conducting similar activities as Slovakia.	NSA	MoFEA	continuously

Task no.	Task	Method of implementation	Responsible party	Cooperating party	Time frame for completion
6.4.	Engage and participate in international cyber drills and exercises.	Secure regular and active participation in international cyber drills and exercises (Cyber Coalition, Locked Shields, Cyber Europe and others).	NSA MoF/DC MoD		continuously
6.5.	Intensify collaboration with the NATO Cooperative Cyber Defence Centre of Excellence (CCD CoE).	Enhance the personnel capacities of Slovak representatives sent to the CCD CoE to fulfil assigned duties.	MoD		2018
		Regularly inform parties of the range of CCD CoE training and educational activities available and facilitate their participation in such activities.	MoD		continuously

AREA 7: SUPPORT OF SCIENCE AND RESEARCH IN THE AREA OF CYBER SECURITY

Task no.	Task	Method of implementation	Responsible party	Cooperating party	Time frame for completion
7.1.	Support research activities in the area of cyber security.	Support research activities in the area of cyber security through domestic grant schemes.	MoE	Academic community MoF NASES	2016-2020
		Support research activities in the area of cyber security through resources dedicated for the European Research Area.	MoE	Academic community MoF NASES	2016-2020
7.2.	Support the building of forensic workplaces.	Support the building of new specialised workplaces to strengthen the protection of the state's major information assets with subsequent exploitation of developed knowledge and know-how to develop science and research in the area of cyber security.	NSA		2016-2020
		Create forensic workplaces within its material area focused on conducting analytical activities during responses to security incidents/attacks and when conducting activities related to the collection and evaluation of digital evidence in organisations for providing services to government organisations and securing their operation.	CGBs		2016-2020

Conclusion

The Action Plan contains a proposal of tasks, the purpose of which is to secure adequate protection of state cyberspace from potential threats that could cause significant or irrecoverable damage to Slovakia and that could undermine the credibility of the state or organizations. The Action Plan is one of the basic documents defining the list of tasks for the period from 2016 to 2020 focused on the creation of legal regulations, standards, methods, rules, safety policies and other activities needed to ensure the protection and defence of national cyberspace. Fulfilment of the tasks, which themselves may be amended as a result of the dynamically developing environment, will create the prerequisites for an effective, coordinated and efficient system to protect Slovakia's cyber space.

The proposal of tasks is based on the real environment in Slovakia as formulated in the strategic goals of the Concept. Fulfilment of the tasks in the Action Plan is scheduled for the period from 2016 to 2020. Implementation of the tasks in the Action Plan anticipates funding from multiple Operational Programmes with a financing framework defined in the National Information Security Strategy of the Slovak Republic, including partial financing within the approved limits in the budgetary chapters for central government bodies. Activities focused on creating tools to recognise, monitor and manage security incidents, securing critical infrastructure and implementing measures including in the European Cyber Security Strategy require modification and harmonisation of legislation, a fact which the proposal of tasks takes into account adequately.

Expected sources of financing for these activities include:

- **Operational Programme for Integrated Infrastructure - OPII, sponsored by the Ministry of Transport, Construction and Regional Development of the Slovak Republic,**
- **Operational Programme Research and Innovation, sponsored by the Ministry of Education, Science, Research and Sport of the Slovak Republic,**
- **Operational Programme Human Resources, Priority Axis 1: education, sponsored by the Ministry of Education, Science, Research and Sport of the Slovak Republic/Ministry of Labour, Social Affairs and Family of the Slovak Republic,**
- **Inter-departmental programme to protect critical infrastructure, sponsored by the Ministry of Interior of the Slovak Republic,**
- **The National Security Authority budgetary chapter and the budgetary chapters of other affected entities.**

Another considered source of financing is the multi-departmental/inter-departmental Protection of the Cyberspace of the Slovak Republic programme sponsored by the National Security Authority. Completion of the programme proposal is included in this material in task 1.6. The expected time frame of draw down from this programme is in 2017-2020.

The Action Plan may be updated and enhanced to include other relevant tasks reflecting the current situation as the environment is subject to constant and dynamic changes. Fulfilment of individual tasks and progress will be continuously monitored and evaluated on the basis of annual evaluations. Summary progress reports on their delivery will be submitted to the government.

List of abbreviations and acronyms

CCD CoE	NATO Cooperative Cyber Defence Centre of Excellence
CECSP	Central European Cyber Security Platform
CERT	Computer Emergency Response Team
CGBs	Central government bodies
CSA	Competent cyber security authority (central government bodies as defined in Act No. 45/2011 Coll. on Critical Infrastructure or other entities based on other applicable regulations are defined as the competent authority in the Action Plan
CSIRT	Computer Security Incident Response Team
CSIRT.SK	Unit for computer security incident response established by Ministry of Finance of the Slovak Republic
DC	Data centre
EU	European Union
Gov't Office	Government Office of the Slovak Republic
GPO	General Prosecutor's Office of the Slovak Republic
ICT	Information and communication technology
Jud. Acad.	Judicial Academy of the Slovak Republic
MoC	Ministry of Culture of the Slovak Republic
MoD	Ministry of Defence of the Slovak Republic
MoE	Ministry of Education, Science, Research and Sport of the Slovak Republic
MoF	Ministry of Finance of the Slovak Republic
MoFEA	Ministry of Foreign and European Affairs of the Slovak Republic
MoI	Ministry of Interior of the Slovak Republic
MoJ	Ministry of Justice of the Slovak Republic
MoL	Ministry of Labour, Social Affairs and Family of the Slovak Republic
MoT	Ministry of Transport, Construction and Regional Development of the Slovak Republic
NASES	National Agency for Network and Electronics Services
NATO	North Atlantic Treaty Organisation
NBAC	National Security Analytical Centre
NSA	National Security Authority
Sec. Council	Security Council of the Slovak Republic
SIS	Slovak Information Service
SNAS	Slovak National Accreditation Service
SOSMT	Slovak Office of Standards, Metrology and Testing