COUNTRY: **SLOVAKIA**

Slovakia adopted its first, five-year cybersecurity strategy in 2009. Details on the new strategy for 2014 to 2020 remain limited. Slovakia has a computer emergency response team, CSIRT.SK, that focuses on government agencies and critical infrastructure operators. There are no defined public-private partnerships for cybersecurity.

	QUESTION	RESPONSE	EXPLANATORY TEXT
	LEGAL FOUNDATIONS		
1.	Is there a national cybersecurity strategy in place?	✔	The National Strategy for Information Security in the Slovak Republic 2009-2013 <www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/Slovakia_National_Strategy_for_ISEC.pdf> was adopted in 2008. The strategy provides a range of objectives and priorities for the Slovak Republic to pursue, and includes a section on the implementation and financing of the strategy. As of August 2014, the Slovak government is preparing the 2014-2020 strategy.
2.	What year was the national cybersecurity strategy adopted?	2008	
3.	Is there a critical infrastructure protection (CIP) strategy or plan in place?	✔	The Act of 8 February 2011 on Critical Infrastructure <www.informatizacia.sk/index/open_file.php?ext_dok=10361> covers the regulation and practices surrounding Slovakia's critical infrastructure.
4.	Is there legislation/policy that requires the establishment of a written information security plan?	◑	There is no legislation or policy in place in the Slovak Republic that requires the establishment of a written information security plan. Information practices for the Government of the Slovak Republic are set in the Act of 20 April 2006 on Information System of Public Administration and on Certain Amendments 2006 <www.informatizacia.sk/index/open_file.php?ext_dok=17645> and the Act of 11 March 2004 on the Protection of Classified Information and on the Amendment and Supplementing of Certain Acts 2004. <www.nbusr.sk/ipublisher/files/nbusr.sk/english/215_2004_eng.pdf>
5.	Is there legislation/policy that requires an inventory of "systems" and the classification of data?	✔	The Act of 11 March 2004 on the Protection of Classified Information 2004 <www.nbusr.sk/ipublisher/files/nbusr.sk/english/215_2004_eng.pdf> requires information, of which disclosure or destruction may damage the interests of the Slovak Republic, to be classified. Information is classified according to a four-tiered classification system. The classification levels are assigned according to the level of risk involved in disclosing the information.
6.	Is there legislation/policy that requires security practices/requirements to be mapped to risk levels?	✔	The Act of 11 March 2004 on the Protection of Classified Information 2004 <www.nbusr.sk/ipublisher/files/nbusr.sk/english/215_2004_eng.pdf> maps security practices and requirements to the assigned classification level of the information being handled. The classification levels are outlined in Article 3 of the act and are assigned according to the level of risk involved in disclosing the information.
7.	Is there legislation/policy that requires (at least) an annual cybersecurity audit?	✖	There is no legislation or policy that requires an annual cybersecurity audit. The National Strategy for Information Security in the Slovak Republic <www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/Slovakia_National_Strategy_for_ISEC.pdf> calls for the creation of a system that would prepare an annual report on Slovakia's information systems. The report would cover cybersecurity only in part, and the processes and requirements of such a report are not detailed in the strategy.
8.	Is there legislation/policy that requires a public report on cybersecurity capacity for the government?	◑	The National Strategy for Information Security in the Slovak Republic calls for the creation of a system that would prepare an annual report on Slovakia's information systems. Though aspects of cybersecurity would be covered, it would not report on cybersecurity capacity in particular.
9.	Is there legislation/policy that requires each agency to have a chief information officer (CIO) or chief security officer (CSO)?	✖	There is no legislation or policy in place in the Slovak Republic that requires each agency to have a chief information officer or chief security officer. The responsibility for information security is centralised in the National Security Authority. <www.nbusr.sk>

COUNTRY: SLOVAKIA

	QUESTION	RESPONSE	EXPLANATORY TEXT
10.	Is there legislation/policy that requires mandatory reporting of cybersecurity incidents?	✖	There is no legislation or policy in place in the Slovak Republic that requires mandatory reporting of cybersecurity incidents.
11.	Does legislation/policy include an appropriate definition for "critical infrastructure protection" (CIP)?	✔	The Act of 8 February 2011 on Critical Infrastructure <www.informatizacia.sk/index/open_file.php?ext_dok=10361> includes an appropriate definition for "critical infrastructure protection".
12.	Are requirements for public and private procurement of cybersecurity solutions based on international accreditation or certification schemes, without additional local requirements?	✖	The Decree on Standards for Information Systems (Edict No. 55/2014 on Standards of Information Systems of Public Administration) <www.informatizacia.sk/standardy-is-vs/596s> imposes detailed security requirements that cover government procurement opportunities in the Slovak Republic.
	OPERATIONAL ENTITIES		
1.	Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)?	✔	CSIRT.SK <www.csirt.gov.sk> was established in 2009. It is responsible for coordinating incident response measures for Slovak state authorities and entities engaged with critical infrastructure.
2.	What year was the computer emergency response team (CERT) established?	2009	
3.	Is there a national competent authority for network and information security (NIS)?	✔	The National Security Authority <www.nbusr.sk> acts as the national competent authority for network and information security. The Information Society Section of the Ministry of Finance <www.finance.gov.sk/en> is becoming increasingly active in developing and adopting information security standards.
4.	Is there an incident reporting platform for collecting cybersecurity incident data?	✔	CSIRT.SK <www.csirt.gov.sk> is tasked with collecting information about cybersecurity incidents. They have an online reporting structure in place to log cybersecurity incidents.
5.	Are national cybersecurity exercises conducted?	✔	The Slovak Republic conducted a national cybersecurity exercise in 2011. The Slovak Republic has also participated in multi-national cybersecurity exercises organised by the European Union.
6.	Is there a national incident management structure (NIMS) for responding to cybersecurity incidents?	✖	There is no clear national incident management structure for responding to cybersecurity incidents in the Slovak Republic.
	PUBLIC-PRIVATE PARTNERSHIPS		
1.	Is there a defined public-private partnership for cybersecurity?	✖	There is no defined public-private partnership for cybersecurity in the Slovak Republic.
2.	Is industry organised (i.e. business or industry cybersecurity councils)?	◑	While there is no industry-led cybersecurity platform in the Slovak Republic, the IT Asociacia Slovenska (ITAS) <itas.sk>, which represents both Slovak and international information technology companies, engages with cybersecurity in the course of its operations.
3.	Are new public-private partnerships in planning or underway (if so, which focus area)?	✖	There are no new public-private partnerships being planned in the Slovak Republic.
	SECTOR-SPECIFIC CYBERSECURITY PLANS		
1.	Is there a joint public-private sector plan that addresses cybersecurity?	✖	The Slovak Republic does not have sector-specific joint public-private plans in place.
2.	Have sector-specific security priorities been defined?	✖	Sector-specific security priorities have not been defined.
3.	Have any sector-specific cybersecurity risk assessments been conducted?	✖	Sector-specific risk assessments have not been released.

COUNTRY: SLOVAKIA

	QUESTION	RESPONSE	EXPLANATORY TEXT
	EDUCATION		
1.	Is there an education strategy to enhance cybersecurity knowledge and increase cybersecurity awareness of the public from a young age?	✔	The National Strategy for Information Security in the Slovak Republic 2009-2013 <www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/Slovakia_National_Strategy_for_ISEC.pdf> includes several cybersecurity education initiatives, such as: • including information security in IT or other classes taught at secondary schools; • developing a lifelong learning scheme (basic and follow-up training courses) for IT specialists (system administrators) from the state and private sector; and • publishing specialised literature and methodology documents addressing particular issues of information security.