COUNTRY: **SLOVENIA**

Slovenia has yet to develop a comprehensive legal and policy framework for cybersecurity. As such, it also has yet to adopt a national cybersecurity strategy. SI-CERT is the national computer emergency response team, and it deals with all Slovenian networks. There are no defined public-private partnerships for cybersecurity in Slovenia.

	QUESTION	RESPONSE	EXPLANATORY TEXT
	LEGAL FOUNDATIONS		
1.	Is there a national cybersecurity strategy in place?	✖	Slovenia does not have a cybersecurity strategy in place.
2.	What year was the national cybersecurity strategy adopted?	–	
3.	Is there a critical infrastructure protection (CIP) strategy or plan in place?	✔	The Intergovernmental Coordination Group for Harmonisation of Preparations for Critical Infrastructure Protection, under the Ministry of Defence <www.mo.gov.si> publishes regular research reports that address critical infrastructure protection in Slovenia.
4.	Is there legislation/policy that requires the establishment of a written information security plan?	✖	There is no legislation or policy in place in Slovenia that requires the establishment of a written information security plan.
5.	Is there legislation/policy that requires an inventory of "systems" and the classification of data?	✔	The Classified Information Act 2006 <www.ip-rs.si/index.php?id=505> requires information relating to public security, defence, foreign affairs, or intelligence; or any related scientific, research, technological or financial affairs, to be classified. The information is classified according to a four-tiered classification system, as set out in chapter two of the act. The classification levels are assigned according to the level of risk involved in disclosing the classified information.
6.	Is there legislation/policy that requires security practices/ requirements to be mapped to risk levels?	✔	The Classified Information Act 2006 <www.ip-rs.si/index.php?id=505> maps various security practices to assigned classification levels. These levels are set out in chapter two of the act and are assigned according to the level of risk involved in disclosing the classified information. Further pieces of legislation dealing with classified information, such as the Decree on the Protection of Classified Information in Communication and Information Systems, require additional security practices to those set out in the Classified Information Act. These can be either general practices, or else mapped to the classification levels.
7.	Is there legislation/policy that requires (at least) an annual cybersecurity audit?	◑	There is no legislation or policy in place in Slovenia that requires an annual audit. The Electronic Communication Act <www.akos-rs.si/files/APEK_eng/Legislation/electronic-communications-act-zekom1.pdf> contains provisions that allow the Communications Networks and Service Agency to order a general information security audit — however, the agency is not required to do so according to a certain timeline.
8.	Is there legislation/policy that requires a public report on cybersecurity capacity for the government?	✖	There is no legislation or policy in place in Slovenia that requires a public report on cybersecurity capacity for the government.
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 Slovenia that requires each agency to have a chief information officer or chief security officer. The responsibility for information management and security is centralised in the Communications Networks and Services Agency (AKOS). <akos-rs.si>
10.	Is there legislation/policy that requires mandatory reporting of cybersecurity incidents?	✔	Communications Networks and Services Agency (AKOS) <akos-rs.si> is required by the Electronic Communication Act <www.akos-rs.si/files/APEK_eng/Legislation/electronic-communications-act-zekom1.pdf> to report incidents of breaches of security to SI-CERT. <www.cert.si>

COUNTRY: SLOVENIA

	QUESTION	RESPONSE	EXPLANATORY TEXT
11.	Does legislation/policy include an appropriate definition for "critical infrastructure protection" (CIP)?	✔	The Intergovernmental Coordination Group for Harmonisation of Preparations for Critical Infrastructure Protection published the report Definition and Protection of Critical Infrastructure, which 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?	Not applicable	There are no specific cybersecurity standards or certification requirements for procurement in Slovenia, as of August 2014.
	OPERATIONAL ENTITIES		
1.	Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)?	✔	SI-CERT <www.cert.si> is responsible for the coordination of security procedures and incident response measures across all Slovenian networks.
2.	What year was the computer emergency response team (CERT) established?	2010	
3.	Is there a national competent authority for network and information security (NIS)?	✔	The Communications Networks and Services Agency (AKOS) <akos-rs.si> acts as the national competent authority for network and information security in Slovenia.
4.	Is there an incident reporting platform for collecting cybersecurity incident data?	✔	SI-CERT <www.cert.si> is tasked with collecting information about cybersecurity incidents. It provides an email-based reporting system to log cybersecurity incidents.
5.	Are national cybersecurity exercises conducted?	◑	Slovenia has participated in cybersecurity exercises conducted by both the European Union and NATO.
6.	Is there a national incident management structure (NIMS) for responding to cybersecurity incidents?	✖	There is no clearly detailed national incident management structure for responding to cybersecurity incidents in place in Slovenia. The Electronic Communication Act <www.akos-rs.si/files/APEK_eng/Legislation/electronic-communications-act-zekom1.pdf> requires SI-CERT <www.cert.si> to assist the Communications Networks and Services Agency (AKOS) <akos-rs.si> when necessary, however this is not part of a clear structure or process.
	PUBLIC-PRIVATE PARTNERSHIPS		
1.	Is there a defined public-private partnership for cybersecurity?	✖	There is no defined public-private partnership for cybersecurity in Slovenia.
2.	Is industry organised (i.e. business or industry cybersecurity councils)?	◑	While there is no industry-led cybersecurity-specific platform in Slovenia, the Chamber of Commerce and Industry of Slovenia <www.gzs.si> 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 Slovenia.
	SECTOR-SPECIFIC CYBERSECURITY PLANS		
1.	Is there a joint public-private sector plan that addresses cybersecurity?	✖	Slovenia 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.
	EDUCATION		
1.	Is there an education strategy to enhance cybersecurity knowledge and increase cybersecurity awareness of the public from a young age?	✖	Slovenia participates in the Balkan Security Agenda, which promotes cybersecurity education in the region, but a specific Slovenian education strategy or program has not yet been developed. The Balkan Security Agenda Cyber Defence and Cybersecurity Initiative <www.balsec.org/category/blog/bsa-cyber-defence-and-cybersecurity-initiative> includes a recommendation to: "increase public awareness of how individuals can protect their own internet data, and promote cyber-security education and training".