COUNTRY: **BULGARIA**

The legal framework for cybersecurity in Bulgaria is limited, and there is no national cybersecurity strategy in place. There are also no formalised public-private partnerships, although a significant number of cybersecurity events and academic discussions are focused on cybersecurity and critical information infrastructure protection.

CERT Bulgaria is the country's most significant cybersecurity entity and the focus of recent efforts from the government to strengthen cybersecurity.

	QUESTION	RESPONSE	EXPLANATORY TEXT
	LEGAL FOUNDATIONS		
1.	Is there a national cybersecurity strategy in place?	✖	Bulgaria does not have a national cybersecurity strategy in place. Risks and measures concerning cybersecurity are addressed, in part, within the broader National Security Strategy of the Republic of Bulgaria 2011 <www.mi.government.bg/en/themes/bulgaria-s-national-security-strategy-904-300.html>.
2.	What year was the national cybersecurity strategy adopted?	–	
3.	Is there a critical infrastructure protection (CIP) strategy or plan in place?	◑	Bulgaria does not have a critical infrastructure protection strategy or plan in place. The Law on Crisis Management 2005 provides a basic definition of critical infrastructure.
4.	Is there legislation/policy that requires the establishment of a written information security plan?	✖	There is no legislation or other formal requirement for the development of a written information security plan in Bulgaria.
5.	Is there legislation/policy that requires an inventory of "systems" and the classification of data?	✔	The Classified Information Protection Act 2002 <www.dksi.bg/NR/rdonlyres/71B685D9-EC95-40C8-8C41-031DC93FB3C9/0/Classified_Information_Protection_Act.pdf> requires data, which disclosure may cause a threat to the sovereignty, foreign policy or national security of Bulgaria, to be classified. Article 28 of the act outlines a four-tiered system of classification levels. The 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 Protection Act 2002 <www.dksi.bg/NR/rdonlyres/71B685D9-EC95-40C8-8C41-031DC93FB3C9/0/Classified_Information_Protection_Act.pdf> maps various security practices including the storage to classified information, access term limits on classified information, and security clearance procedures for individuals wanting to access classified information to assigned classification levels. These levels are set out in Article 28 of the act, and are assigned according to the level of risk involved in disclosing the classified information.
7.	Is there legislation/policy that requires (at least) an annual cybersecurity audit?	✖	There is no formal requirement in place for an annual cybersecurity audit. A relevant provision is Article 7, Paragraph 1 of the Classified Information Protection Act 2002 <www.dksi.bg/NR/rdonlyres/71B685D9-EC95-40C8-8C41-031DC93FB3C9/0/Classified_Information_Protection_Act.pdf>. This requires the chairperson of the State Information Security Commission <www.dksi.bg> to submit a yearly report on the "overall activity relating to the protection of classified information" to the executive of the Government of Bulgaria. Article 7, Paragraph 2 requires the executive to introduce this report before the parliament, who will adopt it. This does not, however, include any specific requirement for a cybersecurity audit.
8.	Is there legislation/policy that requires a public report on cybersecurity capacity for the government?	✖	There is no legislation or other formal requirement for the development of a public report on cybersecurity capacity in Bulgaria.
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 other formal requirement for agencies to appoint a chief information officer in Bulgaria.
10.	Is there legislation/policy that requires mandatory reporting of cybersecurity incidents?	✖	There is no legislation or other formal requirement for mandatory reporting of cybersecurity incidents in Bulgaria.

COUNTRY: BULGARIA

	QUESTION	RESPONSE	EXPLANATORY TEXT
11.	Does legislation/policy include an appropriate definition for "critical infrastructure protection" (CIP)?	✔	The Law on Crisis Management 2005 provides a basic definition of critical infrastructure.
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 Bulgaria, as of August 2014.
	OPERATIONAL ENTITIES		
1.	Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)?	✔	CERT Bulgaria <www.govcert.bg> was established in 2008. It is responsible for coordinating security and incident response measures for Bulgarian government institutions. Information on the precise scope of its operations is limited.
2.	What year was the computer emergency response team (CERT) established?	2008	
3.	Is there a national competent authority for network and information security (NIS)?	✔	The State Information Security Commission <www.dksi.bg>, whose composition and duties are set out in the Classified Information Protection Act 2002 <www.dksi.bg/NR/rdonlyres/71B685D9-EC95-40C8-8C41-031DC93FB3C9/0/Classified_Information_Protection_Act.pdf> acts as the national competent authority for network and information security in Bulgaria.
4.	Is there an incident reporting platform for collecting cybersecurity incident data?	✔	CERT Bulgaria <www.govcert.bg> runs an incident reporting service. It is only available to state employees, who must register with CERT Bulgaria.
5.	Are national cybersecurity exercises conducted?	✔	Bulgaria conducted the cybersecurity exercise PHOENIX <phoenix.armf.bg> in 2010.
6.	Is there a national incident management structure (NIMS) for responding to cybersecurity incidents?	◑	There is no national incident management structure for responding to general cybersecurity incidents. In the case of a cybersecurity incident, CERT Bulgaria <www.govercert.bg> will issue a general security alert and warning. The Classified Information Protection Act 2002 <www.dksi.bg/NR/rdonlyres/71B685D9-EC95-40C8-8C41-031DC93FB3C9/0/Classified_Information_Protection_Act.pdf> and the Regulation for Implementation of the Law of Protection of the Classified Information 2002 <www.dksi.bg/NR/rdonlyres/472CF625-FD69-4102-963C-13596AF37EED/0/PPZZKI_ENG_19_01_2010.rtf> outline the coordinating response the State Information Security Commission will have in the event of the detection of a breach of or threat to information security, which in the case of top secret documents includes reporting directly to the Prime Minister. This does not cover cybersecurity incidents unrelated to duties of the State Information Security Commission.
	PUBLIC-PRIVATE PARTNERSHIPS		
1.	Is there a defined public-private partnership for cybersecurity?	◑	While Bulgaria does not have a defined public-private partnership for cybersecurity, it has endeavoured to expand the role of CERT Bulgaria <www.govcert.bg> (the national computer emergency response team), to include liaising with and promoting cooperation between public and private organisations. The Centre for Security and Defence Management <www.it4sec.org/csdm>, based at the Bulgarian Institute of Sciences, is an academic centre that works closely with advising and training in state departments.
2.	Is industry organised (i.e. business or industry cybersecurity councils)?	◑	While there are no dedicated industry-led cybersecurity associations in Bulgaria, the Bulgarian Association of Software Developers <www.devbg.org> (an advocacy and support body that represents software professionals), and the Bulgarian Association of Information Technologies <www.bait.bg> engage with cybersecurity and informational security as part of their regular duties. Additionally, Bulgaria has hosted industry-led cybersecurity forums, including the South East European Regional Forum on Cybersecurity and Cybercrime. <cybercrimeforum.bg>
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 Bulgaria.

COUNTRY: BULGARIA

	QUESTION	RESPONSE	EXPLANATORY TEXT
	SECTOR-SPECIFIC CYBERSECURITY PLANS		
1.	Is there a joint public-private sector plan that addresses cybersecurity?	✖	Bulgaria 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, as of August 2014.
	EDUCATION		
1.	Is there an education strategy to enhance cybersecurity knowledge and increase cybersecurity awareness of the public from a young age?	◑	Bulgaria identified education as one of its key cybersecurity policy objectives in 2010. <www.atlantic-bg.org/images/news/round-table-cyber-sec-28_09-2010/docs/radev-privetstvie-28-09-10.pdf> However, there do not appear to have been significant efforts to implement cybersecurity education in schools or other educational institutions.