BSA The Software Alliance

COUNTRY: **SOUTH KOREA**

Legal Foundations: South Korea takes a national security and defense-focused approach to cybersecurity. As such, the country's Cyber Security Master Plan, issued in 2011, is more a cyberdefense strategy than a cybersecurity strategy. There are some minor gaps in their legal framework.

Operational Entities: Both KrCERT/CC and KN-CERT (government only) are established computer emergency response teams. Information security responsibilities are centralized in the Korea Internet and Security Agency, which has a considerable online presence.

Public-Private Partnerships: KrCERT/CC liaises with the private sector as part of its incident response duties; however, there is no formal public private partnership for cyber or information security in South Korea.

Sector-Specific Cybersecurity Plans: There is no joint public-private sector plan in South Korea that addresses cybersecurity.

Education: The Korea Information Security Agency is responsible for promoting the responsible use of the internet among users, and the agency conducts a range of online and broadcast awareness-raising campaigns.

Additional Cyberlaw Indicators: South Korea places certain undue restrictions on cybersecurity service providers, including Korea-specific testing rules.

	QUESTION	RESPONSE	EXPLANATORY TEXT
	LEGAL FOUNDATIONS		
1.	Is there a national cybersecurity strategy in place?	◑	The National Cyber Security Master Plan <service1.nis.go.kr/eng/main.jsp> was produced by the Korean Communications Commission <service1.nis.go.kr/eng/main.jsp> in 2011. It is a limited defense-focused plan that grants additional powers to the National Intelligence Agency <www.nis.go.kr> and to the Ministries of Defense and Home Affairs.
2.	What year was the national cybersecurity strategy adopted?	–	
3.	Is there a critical infrastructure protection (CIP) strategy or plan in place?	◑	South Korea does not have a discrete critical infrastructure protection plan in place, however plans issued by the Korean Communications Commission <service1.nis.go.kr/eng/main.jsp>, such as Plan 11, have addressed critical information infrastructure in part. The Information Infrastructure Protection Act is the central law addressing information infrastructure protection.
4.	Is there legislation/policy that requires the establishment of a written information security plan?	◑	There is no legislation/policy in place in South Korea that requires the establishment of a written information security plan. The Korean Internet and Security Agency (KISA) <www.kisa.or.kr> is the authority responsible for information security and has previously published reports the address information security in part. In addition, the Act on Promotion of Information and Communication Network Utilization and Information Protection 2000 details the responsibilities of KISA and the wider information security requirements and practices of the South Korean government.
5.	Is there legislation/policy that requires an inventory of "systems" and the classification of data?	✓	The Law on Military Secrets <www.law.go.kr/LSW/LsInfoP.do?lsiSeq=72906#0000> requires information whose unauthorized disclosure may pose a threat to national security to be classified. The three-tiered classification system used is detailed in the Decree on the Law of Military Secrets 2006. Classification levels are assigned according to the level of risk in disclosing the classified information.
6.	Is there legislation/policy that requires security practices/ requirements to be mapped to risk levels?	✓	The Law on Military Secrets <www.law.go.kr/LSW/LsInfoP.do?lsiSeq=72906#0000> and the Decree on the Law of Military Secrets 2006 both contain security practices that are mapped to classifications levels. These levels are detailed in the decree and are assigned according to the level of risk in disclosing the classified information.

COUNTRY: SOUTH KOREA

	QUESTION	RESPONSE	EXPLANATORY TEXT
7.	Is there legislation/policy that requires (at least) an annual cybersecurity audit?	◑	There is no legislation or policy in place in South Korea that requires at least an annual cybersecurity audit. The Korean Internet and Security Agency (KISA) <www.kisa.or.kr> is the authority responsible for network and information security, and periodically publishes reports that address internet and cybersecurity, however there is no legal requirement dictating the content or requiring their publication within a specific timeframe.
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 South Korea that requires a public report on cybersecurity capacity for the government. The Korean Internet and Security Agency (KISA) <www.kisa.or.kr>, responsible for cybersecurity in South Korea, publishes regular reports, however there is no legal requirements around the content or frequency of such publications.
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 South Korea that requires each agency to have a chief information officer or chief security officer.
10.	Is there legislation/policy that requires mandatory reporting of cybersecurity incidents?	✖	There is no legislation or policy in place in South Korea that requires mandatory reporting of cybersecurity incidents.
11.	Does legislation/policy include an appropriate definition for "critical infrastructure protection" (CIP)?	✔	The Information and Communication Infrastructure Protection Act 2001 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?	◑	There are no specific cybersecurity standards or certification requirements for procurement in South Korea, as of May 2015. Where general IT procurement requirements are in place, these requirements sometimes include unique local requirements. South Korea has also introduced some local testing requirements for products which have already received international accreditation. Although South Korea participates in the Common Criteria Recognition Arrangement (CCRA), in practice a combination of unique local requirements and additional local testing acts as a barrier to the proper implementation of the CCRA. The ITSCC <service1.nis.go.kr/eng/certify/mission.jsp> promotes the use of certified and validated IT security products and systems, but this approach has not yet been formalized in all government procurement policies.
	OPERATIONAL ENTITIES		
1.	Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)?	✔	South Korea has two computer emergency response teams that are engaged on a national level. • KrCERT/CC <eng.krcert.or.kr> was established in 1996. It is responsible for early detection systems and the coordination of incident response for non-government networks in South Korea. KrCERT/CC is the South Korean representative at the Asia Pacific Computer Emergency Response Team and represents South Korea in multi-national forums. • KN-CERT <service1.nis.go.kr> was established in 2004 to coordinate incident response across networks utilized by government organizations and agencies.
2.	What year was the computer emergency response team (CERT) established?	1996	
3.	Is there a national competent authority for network and information security (NIS)?	✔	The Korea Internet and Security Agency (KISA) <www.kisa.or.kr> acts as the national competent authority for network and information security in Korea. It is a sub-organization of the Korean Communications Commission <service1.nis.go.kr/eng/main.jsp>. In addition to this, the South Korean government announced in April 2015 the establishment of a new cybersecurity post under the President. The post is expected to be chiefly responsible for the strategy and management of cybersecurity as it related to South Korea' cyber defense and cyber offense capabilities <thediplomat.com/2015/04/south-korea-beefs-up-cyber-security-with-an-eye-on-north-korea>.
4.	Is there an incident-reporting platform for collecting cybersecurity incident data?	✔	KrCERT/CC <eng.krcert.or.kr> is tasked with the collection of cybersecurity incident data. Cyber incidents are detected by KrCERT/CC through its early warning systems, and incidents can also be reported directly by individuals and organizations.

COUNTRY: SOUTH KOREA

	QUESTION	RESPONSE	EXPLANATORY TEXT
5.	Are national cybersecurity exercises conducted?	✔	South Korea has conducted multiple national and bilateral cyber exercises — these have focused mainly on responding to military based cyber-aggression in a mock cyber warfare scenario.
6.	Is there a national incident management structure (NIMS) for responding to cybersecurity incidents?	◑	KrCERT/CC <eng.krcert.or.kr> has a network of response teams that engage in the event of a cybersecurity incident. These response teams, and KrCERT/CC, are required to liaise with relevant stakeholders as part of the response process, however there is not a clear national incident management structure for responding to cybersecurity incidents beyond this requirement.
	PUBLIC-PRIVATE PARTNERSHIPS		
1.	Is there a defined public-private partnership (PPP) for cybersecurity?	◑	South Korea does not have a defined public-private partnership for cybersecurity. KrCCERT/CC <eng.krcert.or.kr> collaborates closely with the private-sector in the running of its early warning system and when coordinating incident response procedures. KrCERT/CC also runs the "Cyber Emergency Shelter" program, which provides safe server space for small and medium-sized businesses if they are a target of a cybersecurity incident.
2.	Is industry organized (i.e., business or industry cybersecurity councils)?	◑	While there is no industry-led organization dedicated to cybersecurity, the National IT Industry Promotion Agency (NIPA) <www.nipa.kr> is a representative organization for the South Korean information technology sector.
3.	Are new public-private partnerships in planning or underway (if so, which focus area)?	✖	As of May 2015, there are no documented new public-private partnerships being planned in South Korea.
	SECTOR-SPECIFIC CYBERSECURITY PLANS		
1.	Is there a joint public-private sector plan that addresses cybersecurity?	✖	There is no joint public-private sector plan in Korea that addresses cybersecurity.
2.	Have sector-specific security priorities been defined?	✖	Sector-specific security priorities have not been publicly defined, nor has there been a proposal to define sector-specific security priorities in legislation or policy.
3.	Have any sector cybersecurity risk assessments been conducted?	✖	Sector cybersecurity risk assessments have not been conducted in South Korea.
	EDUCATION		
1.	Is there an education strategy to enhance cybersecurity knowledge and increase cybersecurity awareness of the public from a young age?	◑	The Korean Information Security Agency (KISA) <www.kisa.or.kr/eng/activities/internetpromotion.jsp> is responsible for promoting the responsible use of the internet amongst users, and they conduct a range of online and broadcast awareness-raising campaigns.
	ADDITIONAL CYBERLAW INDICATORS		
1.	Are cybersecurity services able to operate free from laws that discriminate based on the nationality of the vendor?	◑	South Korea is a member of the WTO plurilateral Agreement on Government Procurement (GPA), which includes rules guaranteeing fair and non-discriminatory conditions of international competition. These rules cover most large contracts. Some government procurement is still not covered by South Korea's commitments under the GPA — for example, procurement from SMEs. Some preference is given to local suppliers (in the form of extra evaluation points) for government procurement.
2.	Are cybersecurity services able to operate free from laws or policies that mandate the use of specific technologies?	✔	There are no specific mandatory technology requirements in laws or policies. South Korea does impose some local encryption standards in limited circumstances in the national security sector. These standards are not compatible with widely used international encryption standards.
3.	Are cybersecurity services able to operate free from additional local testing requirements that go beyond international testing requirements?	✖	The South Korean NIS has implemented additional security testing for networking products which have already been accredited and tested against the international common criteria (CC). Vendors must pass these additional local tests before the products can be procured by public sector customers.
4.	Are cybersecurity services able to operate free from laws or policies that mandate the submission of source code or other proprietary information?	✔	There are no requirements for cybersecurity services to submit source code, as of May 2015.

COUNTRY: SOUTH KOREA

	QUESTION	RESPONSE	EXPLANATORY TEXT
5.	Are cybersecurity services able to operate free from laws or policies that require service providers to locate their servers inside the subject country?	✓	There are no specific regulations in South Korea that require service providers to locate their servers inside the country. The recent Act on the Development of Cloud Computing and Protection of Users 2015 has the potential to create a more restrictive environment for cybersecurity services. Guidelines and regulations under the Act have not yet been developed.
6.	Are cybersecurity services able to operate free from unnecessary restrictions on cross-border data flows (such as registration requirements)?	◑	There are no registration requirements or other unnecessary restrictions on the majority of cross-border data flows in South Korea. However, registration is required for large data collections (more than 10,000 individual records) and there are also restrictions on transferring banking and credit card data outside South Korea.