COUNTRY: **SWEDEN**

Sweden does not have a national cybersecurity strategy, but one is being developed. There are no laws in Sweden that specifically deal with cybersecurity.

Sweden does, however, have a functioning computer emergency response team, CERT-SE, which has jurisdiction over all Swedish networks. Furthermore, the Swedish Civil Contingencies Agency (MSB), which is the national authority in charge of information security, has helped Sweden establish a good reputation on cybersecurity. MSG is the centralised information security entity and has a prominent public presence.

	QUESTION	RESPONSE	EXPLANATORY TEXT
	LEGAL FOUNDATIONS		
1.	Is there a national cybersecurity strategy in place?	✖	According to the European Union Agency on Information Security (ENISA) <www.enisa.europa.eu>, Sweden is preparing a cybersecurity strategy. As of August 2014, the expected date of release is unknown. A high level Strategy for Information Security 2010-2015 has been published, but it does not address specific issues in cybersecurity or set out actions and responses.
2.	What year was the national cybersecurity strategy adopted?	–	
3.	Is there a critical infrastructure protection (CIP) strategy or plan in place?	✔	Sweden adopted the National Strategy for the Protection of Vital Societal Functions in 2014. The strategy was produced by the Swedish Civil Contingencies Agency (MSB). <www.msb.se>
4.	Is there legislation/policy that requires the establishment of a written information security plan?	✔	The Swedish Civil Contingencies Agency's Regulations on Government Agencies' Information Security 2009, pursuant to Regulation 2006:942 <riksdagen.se/sv/Dokument-Lagar/Lagar/Svenskforfattningssamling/Forordning-2006942-om-krisb_sfs-2006-942> compels each government agency to establish an information security policy sufficient for ensuring that agency's information security.
5.	Is there legislation/policy that requires an inventory of "systems" and the classification of data?	✔	The Armed Forces Regulation on Security 2203:77 outlines a four-tiered classification system. Under the system, data deemed to be in need of classification are assigned a classification level according 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 Public Access to Information and Secrecy Act 2009 sets out security practices for information mapped to the classification level assigned to it. The classification levels are set out in the Armed Forces Regulation on Security 2203:77 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?	✖	The Swedish Civil Contingencies Agency's Regulations on Government Agencies' Information Security 2009, pursuant to Regulation 2006:942 <riksdagen.se/sv/Dokument-Lagar/Lagar/Svenskforfattningssamling/Forordning-2006942-om-krisb_sfs-2006-942> support "regular" review and monitoring of incident response measures. This process is not required to be conducted according to 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 Sweden that requires a public report on cybersecurity capacity for the government. There is a government committee investigating Sweden's information security legislation and national defence framework that is expected to report in November 2014. <www.regeringen.se/sb/d/108/a/233522>
9.	Is there legislation/policy that requires each agency to have a chief information officer (CIO) or chief security officer (CSO)?	✔	The Swedish Civil Contingencies Agency's Regulations on Government Agencies' Information Security 2009, pursuant to Regulation 2006:942 <riksdagen.se/sv/Dokument-Lagar/Lagar/Svenskforfattningssamling/Forordning-2006942-om-krisb_sfs-2006-942> require each government agency to appoint one or more persons to direct and coordinate measures related to information security.
10.	Is there legislation/policy that requires mandatory reporting of cybersecurity incidents?	✖	The Swedish Civil Contingencies Agency (MSB) <www.msb.se> advises government agencies to report cybersecurity incidents, however, such reporting is not mandatory.
11.	Does legislation/policy include an appropriate definition for "critical infrastructure protection" (CIP)?	✔	The Swedish Civil Contingencies Agency (MSB) <www.msb.se> provides an appropriate definition for "critical infrastructure protection".

COUNTRY: SWEDEN

	QUESTION	RESPONSE	EXPLANATORY TEXT
12.	Are requirements for public and private procurement of cybersecurity solutions based on international accreditation or certification schemes, without additional local requirements?	✔	Swedish procurement processes recognise international security certifications, and although some local security guidelines have been developed, they do not require additional local certification or accreditation.
	OPERATIONAL ENTITIES		
1.	Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)?	✔	CERT-SE <www.cert.se> was established in 2003 and is responsible for coordinating incident response measures for both government institutions and private entities across all Swedish networks.
2.	What year was the computer emergency response team (CERT) established?	2003	
3.	Is there a national competent authority for network and information security (NIS)?	✔	The Swedish Civil Contingencies Agency (MSB) <www.msb.se>, in its role as protector of public safety, civil defence, and emergency management, acts as the agency responsible for network and information security.
4.	Is there an incident reporting platform for collecting cybersecurity incident data?	✔	CERT-SE <www.cert.se> is tasked with incident reporting and collecting information about cybersecurity incidents. They engage proactively by monitoring their constituency for cybersecurity incidents, and providing an email-based reporting structure to log cybersecurity incidents.
5.	Are national cybersecurity exercises conducted?	✔	Sweden conducted the National Cyber Security Exercise "NISÖ" in 2012. Sweden also participated in the multi-national International Watch and Warning Network Exercise 2013 organised by the United States.
6.	Is there a national incident management structure (NIMS) for responding to cybersecurity incidents?	◑	The Swedish Civil Contingencies Agency's Regulations on Government Agencies' Information Security 2009, pursuant to Regulation 2006:942 <riksdagen.se/sv/Dokument-Lagar/Lagar/Svenskforfattningssamling/Forordning-2006942-om-krisb_sfs-2006-942> compel each agency to develop its own information security management systems, based on standards supported by the Swedish Standards Institute.
	PUBLIC-PRIVATE PARTNERSHIPS		
1.	Is there a defined public-private partnership for cybersecurity?	◑	The National Telecommunications Coordination Group (NTSG) <www.pts.se/upload/Faktablad/En/facts-about-ntsg.pdf> is a public-private partnership in Sweden that is composed of representatives from entities engaged with electronic communications critical infrastructure. While not dedicated to cybersecurity, the group carries out coordinating and advising functions in the area of electronic communications.
2.	Is industry organised (i.e. business or industry cybersecurity councils)?	◑	While there is no industry-led cybersecurity-specific platform in Sweden, IT & Telekomforetagen <www.itotelekomforetagen.se>, a membership organisation for Swedish companies in the information technology and telecom sector, 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 Sweden.
	SECTOR-SPECIFIC CYBERSECURITY PLANS		
1.	Is there a joint public-private sector plan that addresses cybersecurity?	✖	Sweden 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?	✖	As of August 2014, Sweden is preparing a national cybersecurity strategy that may contain education commitments.