COUNTRY: **FINLAND**

Finland published a comprehensive cybersecurity strategy. It is complemented by a strong overall legal framework encompassing a range of important cybersecurity issues. The national authority responsible for cybersecurity in Finland is in transition, involving the amalgamation of two government computer emergency response teams (CERTs) and the creation of the Cyber Security Centre.

	QUESTION	RESPONSE	EXPLANATORY TEXT
	LEGAL FOUNDATIONS		
1.	Is there a national cybersecurity strategy in place?	✔	Finland's Cyber Security Strategy <www.defmin.fi/en/publications/strategy_documents/Finland_s_cyber_security_strategy> was adopted in 2013. The strategy is composed of two sections: • The first includes the overall approach to cybersecurity and dedicated cybersecurity goals, while • The second is a background dossier which includes the underlying principles of the strategy as well as an implementation plan.
2.	What year was the national cybersecurity strategy adopted?	2013	
3.	Is there a critical infrastructure protection (CIP) strategy or plan in place?	✔	The Government Decision on the Security of Supply 2008 <www.finlex.fi/fi/laki/ajantasa/2008/20080539> is the latest set of official goals and standards relating to the protection of critical infrastructure. Section 2.2 of the decree addresses critical information technology infrastructure in particular. The decree is based is on the policies and systems defined in the Security of Supply Act 1992. <www.finlex.fi/fi/laki/ajantasa/1992/19921390>
4.	Is there legislation/policy that requires the establishment of a written information security plan?	◑	While there is no legislation or policy in place in Finland that requires the establishment of a written information security plan, the Ministry of Finance established Government Information Security Management Board (VAHTI) <www.vm.fi/vm/en/16_ict/03_information_security/index.jsp> and published the Government Information Security Guideline in 2009. <www.vm.fi/vm/en/04_publications_and_documents/01_publications/05_government_information_management/20090629Effect/name.jsp>. It contains security requirements expected of government organisations, including required handling and storage procedures.
5.	Is there legislation/policy that requires an inventory of "systems" and the classification of data?	✔	Under the Government Decree on Information Security in Central Government 2010 <www.finlex.fi/en/laki/kaannokset/2010/en20100681.pdf>, each government institution or authority must decide whether and when to introduce classification. Documents are classified against a four-tier classification "protection level" system. These "protection levels" are based on the security requirement to be complied with in handling them, as specified in Section 9 of the decree. The decree does require central government documents deemed secret to be classified. Documents are deemed secret by the Act on the Openness of Government Activities 1999 <www.finlex.fi/en/laki/kaannokset/1999/en19990621.pdf> or any other act. The decree works in conjunction with the Act on the Openness of Government Activities 1999.
6.	Is there legislation/policy that requires security practices/requirements to be mapped to risk levels?	✔	The Government Decree on Information Security In Central Government 2010 <www.finlex.fi/en/laki/kaannokset/2010/en20100681.pdf> requires classification levels to be applied to information, which is a reflection of both the risk level involved in disclosing the information and the necessary security requirements to be complied with in handling the information.
7.	Is there legislation/policy that requires (at least) an annual cybersecurity audit?	✔	The Instructions on Implementing the Decree on Information Security in Central Government <www.finlex.fi/en/laki/kaannokset/2010/en20100681.pdf> outlines "regular" auditing as part of the implementation and monitoring process of the Government Decree on Information Security in Central Government 2010 <www.finlex.fi/en/laki/kaannokset/2010/en20100681.pdf>, though the requirement is not in the decree itself. The Finnish National Security Authority has published the National Security Auditing Criteria, which covers "information assurance" in detail.

COUNTRY: FINLAND

	QUESTION	RESPONSE	EXPLANATORY TEXT
8.	Is there legislation/policy that requires a public report on cybersecurity capacity for the government?	✔	Section 6.2 of Finland's Cyber Security Strategy <www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf> states that the Cyber Security Centre will prepare annual reports on cybersecurity incidents and the "lessons learnt" by government departments in handling them.
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 Finland 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 Finland that requires mandatory reporting of cybersecurity incidents.
11.	Does legislation/policy include an appropriate definition for "critical infrastructure protection" (CIP)?	✔	The terms "critical infrastructure" and "critical information infrastructure" are defined in the appendix of Finland's Cyber Security Strategy. <www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf>
12.	Are requirements for public and private procurement of cybersecurity solutions based on international accreditation or certification schemes, without additional local requirements?	✔	Finland has developed some specific security requirements for procurement related to critical infrastructure or the handling of classified information — The KATAKRI or National Security Auditing Criteria. <www.defmin.fi/?l=en&s=703> As of August 2014, it is unclear whether an organisation can rely on international certification or accreditation to demonstrate compliance with these criteria, although it appears likely that this will be the case.
	OPERATIONAL ENTITIES		
1.	Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)?	✔	The National Cyber Security Centre Finland (NCSC-FI) <www.viestintavirasto.fi/en/informationsecurity.html> was established in 2014 through a merger of CERT-FI and NCSA-FI. This body is responsible for the coordination of incident response and information security measures for both government institutions and the private sector.
2.	What year was the computer emergency response team (CERT) established?	2014	
3.	Is there a national competent authority for network and information security (NIS)?	✔	The National Cyber Security Centre Finland (NCSC-FI) <www.viestintavirasto.fi/en/informationsecurity.html>, which is a sub-agency of the Finnish Communications Regulatory Authority (FICORA) <www.viestintavirasto.fi/en>, acts as the national competent authority for network and information security.
4.	Is there an incident reporting platform for collecting cybersecurity incident data?	✔	While the National Cyber Security Centre Finland (NCSC-FI) is responsible for incident management, security incident reporting is managed by Finnish Communications Regulatory Authority (FICORA) <www.viestintavirasto.fi/en>, of which the NCSC-FI is a sub-agency. Incidents are logged through an online form on the FICORA website.
5.	Are national cybersecurity exercises conducted?	✔	According to the European Union Agency for Network and Information Security (ENISA) <www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-exercises/exercise-survey2012/at_download/fullReport>, Finland carries out national cyber exercises every half year. Finland has taken part in multi-national exercises organised by the European Union and NATO. Finland's Cyber Security Strategy acknowledges the role of training exercises as a measure to be adopted to increase competence in information security.
6.	Is there a national incident management structure (NIMS) for responding to cybersecurity incidents?	✖	There is no discrete national incident management structure for responding to cybersecurity incidents in place in Finland.
	PUBLIC-PRIVATE PARTNERSHIPS		
1.	Is there a defined public-private partnership for cybersecurity?	◑	The National Emergency Supply organisation (NESO) <www.nesa.fi/organisation> is a network of multiple public-private partnership initiatives whose objectives are related to the security of supply. NESO is responsible for measures related to developing and maintaining the security of supply.
2.	Is industry organised (i.e. business or industry cybersecurity councils)?	✔	The Finnish Information Security Cluster (FISC) <fisc.fi> is an association of Finnish information security companies. Their role is primarily business advocacy, however in representing the information security sector, FISC is significantly engaged with Finnish cybersecurity.
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 Finland.

COUNTRY: FINLAND

	QUESTION	RESPONSE	EXPLANATORY TEXT
	SECTOR-SPECIFIC CYBERSECURITY PLANS		
1.	Is there a joint public-private sector plan that addresses cybersecurity?	◑	The Government Decision on the Security of Supply 2008 <www.finlex.fi/fi/laki/ajantasa/2008/20080539> addresses, in part, cybersecurity as it relates to sector-specific critical infrastructure. Finland, however, 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?	✔	Finland's Cyber Security Strategy 2013 <www.defmin.fi/en/publications/strategy_documents/Finland_s_cyber_security_strategy> includes a detailed commitment to cybersecurity education. It states that: "the study of basic cyber security skills must be included at all levels of education. The learning requirements of cybersecurity must be included on the curricula of basic education (comprehensive school), vocational upper secondary education, general upper secondary education and higher education". As of August 2014, the Strategy is recent and is yet to be fully implemented.