COUNTRY: **FRANCE**

France has had a national cybersecurity strategy in place since 2011, although it has a strong focus on defence and national security issues. The National Agency for the Security of Information Systems (ANSSI) is a well-established authority dedicated to information security and is integrated with the country's computer emergency response team, CERT-FR. The cybersecurity strategy contains recommendations for closer cooperation with the private sector, but this has not been significantly developed. ANSSI has published sector-specific security measures, making France one of the few EU countries to adopt such a targeted approach to managing cybersecurity.

	QUESTION	RESPONSE	EXPLANATORY TEXT
	LEGAL FOUNDATIONS		
1.	Is there a national cybersecurity strategy in place?	✔	The Information Systems, Defence and Security Strategy was adopted in 2011. <www.ssi.gouv.fr/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf> The strategy has a condensed set of objectives and subsequent action items.
2.	What year was the national cybersecurity strategy adopted?	2011	
3.	Is there a critical infrastructure protection (CIP) strategy or plan in place?	✖	There is no discrete critical infrastructure plan in place in France. The responsibility for critical infrastructure protection is spread across government departments, but is coordinated by the General Secretariat for Defence and National Security (SGDSN). <www.sgdsn.gouv.fr>
4.	Is there legislation/policy that requires the establishment of a written information security plan?	✖	There is no legislation or policy in place in France 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 French Penal Code <www.legifrance.gouv.fr/content/download/1957/13715/version/4/file/Code_33.pdf> requires data, of which disclosure may cause a threat to the national defence, to be classified. The French Defence Code outlines a primary three-tiered system of classification levels, with an additional seven special categories that can be applied. The specifics of the classifications levels are set out in the Decree of 30 November 2011 on the Protection of National Defence Secrets. <www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000024892134&fastPos=1&fastReqId=275001272&categorieLien=cid&oldAction=rechTexte> This decree mandates that classification levels are to be assigned according to the level of risk to national defence involved in disclosing classified information. The Recommendation for Information Systems Relating to Non-Defence Classified Sensitive Information <www.ssi.gouv.fr/IMG/pdf/1994_03_02_901_protection_systemes_d_information.pdf> deals with sensitive data, of which disclosure may not cause a threat to national security in particular, but may still be deemed sensitive to public or private interests. It does not require this data to be classified.

COUNTRY: FRANCE

	QUESTION	RESPONSE	EXPLANATORY TEXT
6.	Is there legislation/policy that requires security practices/ requirements to be mapped to risk levels?	✔	The French Defence Code compels the French Prime Minister to determine the appropriate requirements for the protection of classified information, according to "government priorities". Ministers then carry out security practices in their department based on the requirements of the Prime Minister. The current requirements are set out in the Decree of 30 November 2011 on the Protection of National Defence Secrets <www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000024892134&fastPos=1&fastReqId=275001272&categorieLien=cid&oldAction=rechTexte> and these dictate security procedures that map to risk levels. The Recommendation for Information Systems Relating to Non-Defence Classified Sensitive Information <www.ssi.gouv.fr/IMG/pdf/1994_03_02_901_protection_systemes_d_information.pdf> and the Protection of Non-Defence Sensitive Information: Recommendations for Computer Work Stations 1993 <www.ssi.gouv.fr/IMG/pdf/1993_03_01_600_Protection_des_informations_sensibles_ne_relevant_pas_du_secret_de_defense_-_Recommandation_pour_les_postes_de_travail_informatiques.pdf> deal with sensitive data whose disclosure may not cause a particular threat to national security. It details recommended security procedures pertaining to such information.
7.	Is there legislation/policy that requires (at least) an annual cybersecurity audit?	✖	There is no legislation or policy in place in France that requires at least an annual cybersecurity audit. The Decree of 30 November 2011 on the Protection of National Defence Secrets <www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000024892134&fastPos=1&fastReqId=275001272&categorieLien=cid&oldAction=rechTexte> requires security audits to be part of the operation of the information security process in general, but does not dictate any requirements in terms of timing or scope.
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 France that requires a public report on cybersecurity capacity for the government. The Decree No. 2009-834 of 7 July establishing the National Agency for the Security of Information Systems <www.legifrance.gouv.fr/jopdf/common/jo_pdf.jsp?numJO=0&dateJO=20090708&numTexte=3&pageDebut=&pageFin=> makes it the agency responsible for conducting inspections of information security systems. This process is not elaborated upon however. The decree does not mention cybersecurity in particular.
9.	Is there legislation/policy that requires each agency to have a chief information officer (CIO) or chief security officer (CSO)?	✔	The Decree of 30 November 2011 on the Protection of National Defence Secrets <www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000024892134&fastPos=1&fastReqId=275001272&categorieLien=cid&oldAction=rechTexte> requires each department in possession of classified information, which pertains to national defence to appoint a central security officer, whose position is connected to the Department of Defence.
10.	Is there legislation/policy that requires mandatory reporting of cybersecurity incidents?	✖	There is no legislation or policy in place in France that requires mandatory reporting of cybersecurity incidents.
11.	Does legislation/policy include an appropriate definition for "critical infrastructure protection" (CIP)?	✖	French legislation or policy does not have 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?	◑	The National Agency of Information Systems' Security (ANSSI) <www.ssi.gouv.fr> promotes specific local requirements for the security of information systems (the PASSI standard). This standard is often applied to public authorities in terms of information systems' security, in addition to international standards such as the Common Criteria. However, application of the standard is not mandatory.
	OPERATIONAL ENTITIES		
1.	Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)?	✔	CERT-FR <www.cert.ssi.gouv.fr>, formerly CERTA, was established in 2008. It is responsible for coordinating incident response measures for both government institutions and entities engaged with critical infrastructure.
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 National Agency for the Security of Information Systems (ANSSI) <www.ssi.gouv.fr> acts as France's national competent authority for network and information security.

COUNTRY: FRANCE

	QUESTION	RESPONSE	EXPLANATORY TEXT
4.	Is there an incident reporting platform for collecting cybersecurity incident data?	✔	CERT-FR <www.cert.ssi.gouv.fr> is tasked with collecting information about cybersecurity incidents. They engage proactively by monitoring their constituency for cybersecurity incidents, as well as having in place an email-based reporting structure to log cybersecurity incidents.
5.	Are national cybersecurity exercises conducted?	✔	France conducted the national cybersecurity exercise Piranet in 2010 and 2012. France has also taken part in multi-national exercises organised by the European Union and NATO.
6.	Is there a national incident management structure (NIMS) for responding to cybersecurity incidents?	✖	A national incident management structure for responding to cybersecurity incidents, if it exists, is not publicly available.
	PUBLIC-PRIVATE PARTNERSHIPS		
1.	Is there a defined public-private partnership for cybersecurity?	✖	The French Cybersecurity Strategy (Information Systems, Defence and Security: France's Strategy <www.ssi.gouv.fr/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf>) calls for the establishment of a public-private partnership to assist in the detection of threats and ensure the protection of national critical infrastructure. The status of the public-private partnership is unclear.
2.	Is industry organised (i.e. business or industry cybersecurity councils)?	✖	There is no apparent significant industry-led association for cybersecurity in France.
3.	Are new public-private partnerships in planning or underway (if so, which focus area)?	◑	The French Cybersecurity Strategy (Information Systems, Defence and Security: France's Strategy <www.ssi.gouv.fr/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf>) calls for the establishment of a public-private partnership to assist in the detection of threats and ensure the protection of national critical infrastructure. The status of the public-private partnership is unclear.
	SECTOR-SPECIFIC CYBERSECURITY PLANS		
1.	Is there a joint public-private sector plan that addresses cybersecurity?	✔	The National Agency for the Security of Information Systems (ANSSI) <www.ssi.gouv.fr> has published proposed cybersecurity measures for sectors engaged with critical infrastructure, which cover identification of critical infrastructure and the application of security rules. These rules apply to both public and private entities within each sector.
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?	✔	The French Cybersecurity Strategy <www.ssi.gouv.fr/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf> includes a long-term objective to "raise citizens' awareness of cybersecurity issues during the education process". The Strategy includes a commitment to implement an active governmental communication policy and states that "appropriate communication campaigns will be conducted by National Agency for the Security of Information Systems (ANSSI) targeting the general public and companies".