COUNTRY: **INDIA**

Legal Foundations: India's National Cyber Security Policy was adopted in 2013. It is a detailed plan that includes both high-level principles and targeted objectives and proposals. However, the plan has not been fully implemented and the legal framework supporting cybersecurity remains weak.

Operational Entities: CERT-In, the national CERT, is involved in high-level policy discussions related to information security.

Public-Private Partnerships: Private-sector representative bodies in India are well developed and proactive with regard to cybersecurity. CERT-In also liaises with the private sector; however, there is no dedicated public-private partnership.

Sector-Specific Cybersecurity Plans: There is no joint public-private sector plan that addresses cybersecurity in India. A Joint Working Group has been established to discuss and present recommendations on public-private partnerships in cybersecurity. The working group includes industry representatives.

Education: Creating a culture of cybersecurity awareness through a series of promotional activities and education initiatives is one objective of the Indian National Cyber Security Policy 2013, which also includes a commitment to a comprehensive national awareness raising campaign on cybersecurity.

Additional Cyberlaw Indicators: India has avoided several legal and policy burdens on cybersecurity providers, but it continue to impose local testing requirements in addition to international testing regimes.

	QUESTION	RESPONSE	EXPLANATORY TEXT
	LEGAL FOUNDATIONS		
1.	Is there a national cybersecurity strategy in place?	✔	The Indian government released the National Cyber Security Policy <deity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20(1).pdf> in 2013. It is a detailed plan that includes both high-level principles and targeted objectives and proposals.
2.	What year was the national cybersecurity strategy adopted?	2013	
3.	Is there a critical infrastructure protection (CIP) strategy or plan in place?	✔	The Guidelines for Protection of National Critical Information Infrastructure <csoforum.in/whitepapers/41312/guidelines-for-protection-of-national-critical-information-infrastructure>, a critical information infrastructure plan, has been in place in India since June 2013.
4.	Is there legislation/policy that requires the establishment of a written information security plan?	✖	There is no legislation in place in India 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 Official Secrets Act 1923 <www.archive.india.gov.in/allimpfrms/allacts/3314.pdf> provides a definition for official information but does not provide a system of classification or classification levels. In practice, India uses a four-tier system of classification for sensitive government information.
6.	Is there legislation/policy that requires security practices/requirements to be mapped to risk levels?	◑	The Official Secrets Act 1923 <www.archive.india.gov.in/allimpfrms/allacts/3314.pdf> details security practices and requirements for official information in general, but does not map these to specific risk levels.
7.	Is there legislation/policy that requires (at least) an annual cybersecurity audit?	✖	There is no legislation in place in India that requires at least an annual cybersecurity audit. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 include annual audit requirements for organizations who have obtained a security certification, but these rules only apply to sensitive data. The National Cyber Security Policy highlights the need for a monitoring process to be implemented, but does not require the establishment of a cybersecurity auditing process in particular.

COUNTRY: INDIA

	QUESTION	RESPONSE	EXPLANATORY TEXT
8.	Is there legislation/policy that requires a public report on cybersecurity capacity for the government?	◑	There is no legislation in place in India that requires a public report on cybersecurity capacity for the government. However, the Inter-Departmental Information Security Task Force (ISTF) was set up, in part, to assess India's cybersecurity capacity and it has submitted multiple reports to government on this issue. These reports are not publicly available.
9.	Is there legislation/policy that requires each agency to have a chief information officer (CIO) or chief security officer (CSO)?	◑	While India does have ministerial level chief information officers, there is no legal requirement for each agency to have a chief information officer or chief security officer.
10.	Is there legislation/policy that requires mandatory reporting of cybersecurity incidents?	✔	In January 2014 the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 were released. These include mandatory incident reporting for a wide range of cybersecurity incidents listed in the Annex to the rules <deity.gov.in/sites/upload_files/dit/files/G_S_R%2020%20(E)2.pdf>.
11.	Does legislation/policy include an appropriate definition for "critical infrastructure protection" (CIP)?	✔	The Guidelines for Protection of National Critical Information Infrastructure <csoforum.in/whitepapers/41312/guidelines-for-protection-of-national-critical-information-infrastructure> include 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 Indian National Cyber Security Policy 2013 provides mixed messages on the promotion of international standards, certification and accreditation. On one hand, the Strategy encourages organizations to adopt guidelines for procurement of trustworthy ICT products that "provide for procurement of indigenously developed security technologies." On the other hand, the Strategy promotes the adoption of ISO 27001 and other international security best practices. It will be important to assess how these competing objectives are implemented in practice.
	OPERATIONAL ENTITIES		
1.	Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)?	✔	CERT-In <www.cert-in.org.in> was established in 2004. It is tasked with incident protection and the coordination of incident response procedures across all Indian networks.
2.	What year was the computer emergency response team (CERT) established?	2004	
3.	Is there a national competent authority for network and information security (NIS)?	✔	The Indian government has set up a cybersecurity expert study group, operating under the Ministry of Home Affairs. This group is responsible for reviewing domestic cybersecurity and for developing further policy <articles.economictimes.indiatimes.com/2014-12-24/news/57376238_1_cyber-crimes-expert-group-home-minister-rajnath-singh>. The Inter Departmental Information Security Task Force (ISTF) was set up under the National Security Council to be a national authority responsible for information security. The ISTF has issued substantial recommendations to the government on issues that include critical information infrastructure protection, improving the legal framework surrounding information, and the implementation of best practices. The long-term status of the task force is unclear.
4.	Is there an incident-reporting platform for collecting cybersecurity incident data?	✔	CERT-In <www.cert-in.org.in> is tasked with collecting information about cybersecurity incidents. It proactively conducts research and profiling of attackers, and has an online incident and vulnerability reporting structure in place to log cybersecurity incidents.
5.	Are national cybersecurity exercises conducted?	✔	India carries out cybersecurity exercises on its own and in partnership with countries like the United States and Asian countries.

COUNTRY: INDIA

	QUESTION	RESPONSE	EXPLANATORY TEXT
6.	Is there a national incident management structure (NIMS) for responding to cybersecurity incidents?	◑	While India does have an early warning system and a national computer emergency response team, there is no clear national incident management structure for responding to cybersecurity incidents. The National Cyber Security Policy 2013 <deity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20(1).pdf> details the introduction of a National Cyber Alert System (NCAS) which would be an expansion of the current early warning system. The function of such a system would be to maintain the integrity of information networks during a cyberattack, and to restore a network as quickly as possible. In doing so, the system intends to improve coordination and information sharing with entities engaged with critical infrastructure and other public and private agencies. A Joint Working Group has been established to discuss and present recommendations on public-private partnerships in cybersecurity.
	PUBLIC-PRIVATE PARTNERSHIPS		
1.	Is there a defined public-private partnership (PPP) for cybersecurity?	◑	While there is not a defined public-private partnership for cybersecurity in India, CERT-In <www.cert-in.org.in>, engages with the private sector in the course of its incident response duties. Furthermore, the National Cyber Security Policy 2013 <deity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20(1).pdf> considers developing effective public-private partnerships as a key strategy. A Joint Working Group has been established to discuss and present recommendations on public-private partnerships in cybersecurity.
2.	Is industry organized (i.e., business or industry cybersecurity councils)?	✔	The Data Security Council of India (DSCI) <www.dsci.in> is an industry organization founded to promote data protection, and to develop and implement security and privacy best practices for all Indian industries that operate information systems. DSCI was established by the National Association of Software and Services Companies (NASSCOM) <www.nasscom.in>, a trade association covering the Indian information technology and business process outsourcing industries.
3.	Are new public-private partnerships in planning or underway (if so, which focus area)?	◑	The National Cyber Security Policy 2013 <deity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20(1).pdf> lists developing effective public-private partnerships as a key strategy. Furthermore, Section 3 of the Cyber Security Policy proposes the establishment of a think tank to facilitate discussion and deliberation on cybersecurity policy. As of May 2015, the status of such an organization is unclear.
	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 India that addresses cybersecurity. A Joint Working Group has been established to discuss and present recommendations on public-private partnerships in cybersecurity. The working group includes industry representatives.
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, as of May 2015.
3.	Have any sector cybersecurity risk assessments been conducted?	✖	Sector cybersecurity risk assessments have not been conducted in India.
	EDUCATION		
1.	Is there an education strategy to enhance cybersecurity knowledge and increase cybersecurity awareness of the public from a young age?	✔	Objective 12 of the Indian National Cyber Security Policy 2013 <deity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20(1).pdf> is to create a culture of cybersecurity awareness through a series of promotional activities and education initiatives and includes a commitment to a comprehensive national awareness-raising campaign on cybersecurity.

COUNTRY: INDIA

	QUESTION	RESPONSE	EXPLANATORY TEXT
	ADDITIONAL CYBERLAW INDICATORS		
1.	Are cybersecurity services able to operate free from laws that discriminate based on the nationality of the vendor?	◑	There are multiple and complex layers of government procurement in India. Many of the state and local procurement practices do give preferences to local suppliers (although these may not necessarily be relevant to cybersecurity). India is an observer, but not a member, of the WTO plurilateral Agreement on Government Procurement.
2.	Are cybersecurity services able to operate free from laws or policies that mandate the use of specific technologies?	✔	Although the Indian government has generally taken a technology-neutral approach, it is important to note that the 2008 amendments to the Information Technology Act included a provision that would allow the government to determine what modes of encryption companies and individuals may use: Section 84A: The Government may, for secure use of the electronic medium and for promotion of e-governance and e-commerce, prescribe the modes or methods for encryption. As of May 2015, no rules have been issued under Section 84A.
3.	Are cybersecurity services able to operate free from additional local testing requirements that go beyond international testing requirements?	✖	India imposes some local testing requirements in addition to international testing requirements. These local testing arrangements have been the subject of criticism by India's trading partners, including the European Union <madb.europa.eu/madb/barriers_details.htm?barrier_id=115396&version=3>.
4.	Are cybersecurity services able to operate free from laws or policies that mandate the submission of source code or other proprietary information?	✔	A source code submission proposal was raised in India in 2013, but was withdrawn following international criticism, madb.europa.eu/madb/barriers_details.htm?barrier_id=115396&version=3
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 India that require service providers to locate their servers inside the country.
6.	Are cybersecurity services able to operate free from unnecessary restrictions on cross-border data flows (such as registration requirements)?	✔	India has no registration requirements for any parties under the Information Technology Act 2000. However, there are some rules in place for the transfer of sensitive data offshore. It can only be transferred to a country where it is clear that the sensitive data will be adequately protected — Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011. Sensitive data is defined under the 2011 Rules as information relating to a data subject's password; financial information; health; sexual orientation; medical records and biometric information. Overall these rules appear reasonable.