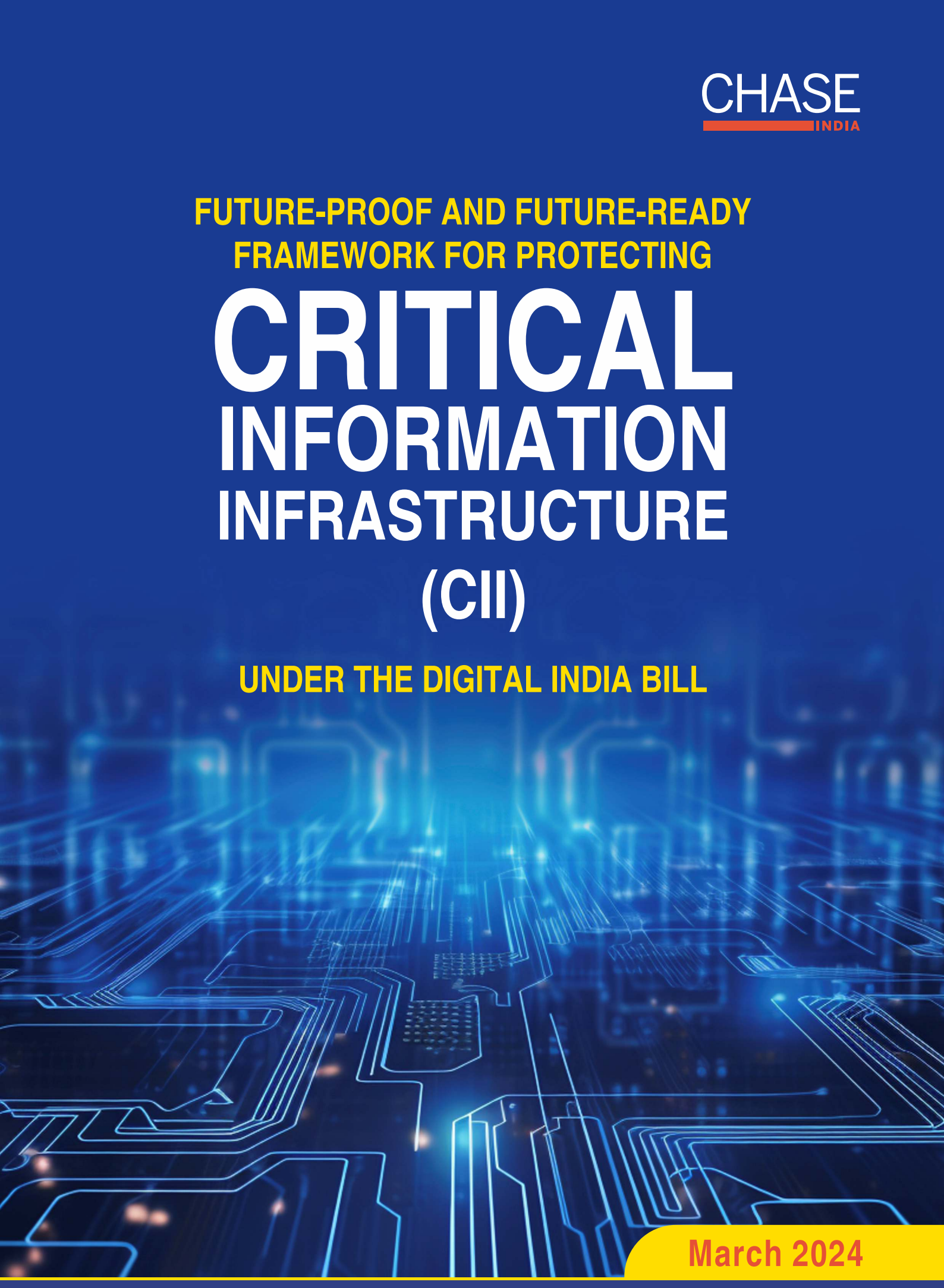
CHASE INDIA

FUTURE-PROOF AND FUTURE-READY FRAMEWORK FOR PROTECTING

CRITICAL INFORMATION INFRASTRUCTURE (CII)

UNDER THE DIGITAL INDIA BILL



March 2024

Introduction:

The Government has often indicated that the present Information Technology Act, 2000 will be revamped and replaced by the Digital India Act. March 2023 saw the first round of consultations for the much-awaited Digital India Bill. The consultations did not prescribe the exact provisions but focussed on the vision of the Government and sought suggestions from stakeholders like industry and civil society for achieving this vision. The vision for a cyber security stance as laid out during the discussion includes accelerating the growth of the innovation and technology ecosystem, accelerating the digitalisation initiatives of the Government, addressing technologies and risks and becoming future-proof and future-ready. The discussions also highlighted the lack of coordinated cyber security incident response mechanisms under the present Information Technology Act, 2000 ("IT Act"). To ensure that these goals are met, it is important to focus on the protection of Critical Infrastructure and Critical Information Infrastructure. In order to achieve the Government's vision of becoming a leader in the global cyber laws space through innovative law-making under the Digital India Bill, the protection of CII and its synchronisation with global best practices to ensure comprehensive protection is crucial. In today's times, no country can protect its CII/CI on its own. Therefore, coordinated efforts are required for effective protection. The presentation made by MoS, MeitY also shared a similar vision highlighting the need for global standard cyber laws[1].The presentation also highlighted the fact that the proposed Digital India Bill needs to ensure that Indian internet is open, safe, trusted and accountable. It should help towards accelerating growth and innovation, speeding up digitisation efforts of the Government, addressing emerging technologies and risks, and becoming future-proof and future-ready (an evolvable digital law). It should also help evolve a coordinated cyber security incident response mechanism, institutional mechanism for awareness creation etc. Recently, the Parliamentary Standing Committee on Finance in its report titled "Cyber Security and Rising Incidence of Cyber/White Collar Crimes" presented to the parliament on July 27 also suggested three options that may be evaluated from the perspective of cyber security. These options are as follows:

- Promulgating new rules
- Through amendment to Digital India legal framework to explicitly address cyber security matters
- By bringing an entirely new cyber security legislation.

These points, as highlighted during the consultation on the Digital India Bill and the parliamentary standing committee on Finance's report, were among those that we tried to address with respect to CII in our first report on Modernising Policy Framework for Protecting India's Critical Information Infrastructure (CII). In this report, we highlighted the need for a working group to conduct a comprehensive risk analysis of Critical Information Infrastructure (CII) in India and strengthen the protection accorded to CII in India. The report proposed that the working group should comprise cyber security experts from the central and state governments, industry, think tanks, emerging start-ups, and academia, to enable a comprehensive approach. The report also identified comprehensive recommendations for the working group to look at, in order to provide solutions to some of the problems highlighted above. The table below showcases the recommendations of our previous report and its alignment with the goals envisaged for the Digital India Bill:

[1]https://www.meity.gov.in/writereaddata/files/DIA_Presentation%2009.03.2023%20Final.pdf

Goals for Digital India Bill[2]	Recommendation [Modernising Policy Framework for Protecting India's Critical Information Infrastructure (CII)]
Global standard cyber laws	• **Adoption of Global Best Practices & Cross-Border Knowledge Sharing:** In today's connected world, no country can mitigate the cyber threats to CII effectively on its own. Hence, there is a need for building globally accepted standards of CII and implementing them at the national level. It is equally important to adopt global best practices in national laws and create a system for cross-border knowledge sharing. This will also be an essential step towards improving India's geo-political position.
An open, safe, trusted and accountable Internet	• **Risk Mitigation:** The focus of the CII framework should not be limited to cyber-attacks. A comprehensive framework should focus on ensuring the continuity of services during natural disasters, power outages, etc. An attack on one CII may likely have a domino effect on other CIIs as well. Therefore, the focus of the Government should be on ensuring continuity, irrespective of the cause. It must be ensured that there are appropriate safeguards which are built in as a risk mitigation approach.
Accelerate growth and innovation	• **MSSPs:** The working groups should focus on ways to encourage Managed Security Service Providers (MSSP)[3] and other similar service providers to provide requisite support to industry and for CII protection in India. This can be done by creating specific funds under the PPP scheme.
Accelerate digitisation efforts of the Government	• **Assessment of Cyber-Attacks on CII:** There is a need for autonomous Indian organisations to carry out independent analysis and trustworthy reporting of cyber-attacks on CII. As the Government accelerates its digitisation efforts independent assessment, analysis and reporting is key to frame its internal mechanisms to ensure cyber resilience.
Address emerging technologies and risks	• **Continuous Monitoring:** A more comprehensive framework for continuous monitoring should be built for the protection of technologies, including Cloud supporting CII. At present, as per the Meghraj 2.0 guidelines, the responsibility is on the user department and Communications Service Provider (CSP). Concerning CII, an inter-departmental committee should be set up, which can include members from NCIIPC, CERT-In, and Sectoral CERTs to evaluate the continuous monitoring process and responsibilities, so that effective remedial and anticipated action can be taken in response to emerging threats.
Future-Proof & Future-Ready	• **Comprehensive Risk Assessment:** With the rise in technology adoption, there is a need to have comprehensive risk assessment for studying cyber security controls that need to be applied. The risk assessment should also focus on the protection that is required to be provided to the physical critical infrastructure by law enforcement agencies which support the CII.

[2]https://www.meity.gov.in/writereaddata/files/DIA_Presentation%2009.03.2023%20Final.pdf
[3]An organization responsible for managing and delivering services to another organization as per their requirement is called a managed service provider (MSP). The services provided by an MSP typically are ongoing and remote. Here the focus is for providing cyber security services.

Coordinated cyber security incident response mechanism	• **Addressing Multiplicity of Regulations and Regulators:** Multiplicity of regulators and regulations governing the same field should be avoided. The multiple compliances, audits, forums, and information-sharing channels are time-consuming for organisations dealing with CII. The focus in such cases shifts from protection to compliance and information sharing. • **Providing Baseline Guidelines and Sector Specific Guidelines:** The baseline guidelines should be laid down by NCIIPC, which can be built upon by the sector-specific regulator based on the requirements of the sector concerned. It may however be noted that the same should not result in multiple regulations operating in the same space and creating multiple reporting channels. At present, the NCIIPC has provided some baseline guidelines for the protection of CII, such as cyber security audit baseline requirements, etc. It has been observed that, at times, other regulators operating in the same sphere, issue guidelines rather than building upon it. • **Establishing the Government's Internal Communication Channels:** There is a need to reassess the multiple notification requirements by multiple regulators in the CII framework. There is a need to reconcile the duplicative and conflicting notification obligations. The Government should implement an information-sharing system so that all relevant regulators are informed when the primary regulator, e.g. NCIIPC, is informed by the regulated entities. The obligation of the critical sector enterprise organisations should only be to inform the primary regulator and the Government should establish its internal communication channels. This is to say that a single interface between the Government and the Critical Sector Enterprise should be created which links all the regulators at the backend.
Institutional mechanism for awareness creation	• **Public-Private Capacity Building:** There is a need for enhanced government-industry partnerships focusing on reinvigorating strategies, improving coordination, designing best practices, and capacity building.

With increased digitisation and online governance, cyber security has become an integral part of governance. The vulnerabilities of the systems are often exploited to attack the systems. Cyber security therefore needs to be a continuous focus of the Government to enhance its digitalisation efforts. With the developments mentioned above on the proposed Digital India Bill front, it is imperative that these recommendations are incorporated through national laws and policies which have been discussed in our present report. We endeavour to identify and draft the legislative and policy provisions for effective protection of Critical Infrastructure and Critical Information Infrastructure to assist in defining a clear roadmap for the upcoming Digital India Act and National Cyber Security Policy. To identify these provisions, we also look at global best practices and prevailing best practices in India.

Global Practices:

The protection of Critical Infrastructure and Critical Information Infrastructure is important for every country. It has gained even more significance after the pandemic, which saw rapid digitalisation across countries, sectors of the economy and different sections of society. This is the reason that many countries, including India, are in the process of rethinking their cyber security strategy. At the international level too, cooperation for the protection of Critical Infrastructure and Critical Information Infrastructure is necessary for effective protection and enforcement.

'The protection of Critical Infrastructures against terrorist attacks: Compendium of good practices[4]' highlighted that the difference between infrastructure and information infrastructure is becoming irrelevant. This is the approach that most of the countries are taking in their national laws as well. The table below shows the treatment of Critical Infrastructure and Critical Information Infrastructure in various countries and multilateral organisations. Most countries have a single specialised policy/law dealing with Critical Information Infrastructure/Critical Infrastructure, as compared to India's unified approach in dealing with all aspects relating to cyber space under a common law i.e. the IT Act, 2000 at present and the proposed Digital India Bill which will replace the IT Act, 2000.

Sl.No.	Country	Law	Critical Sectors	Definition
1	Australia	*Security of Critical Infrastructure Act, 2018*[5]	1. Communication (a critical telecommunications asset, a critical broadcasting asset, a critical domain name system) 2. Data Storage or Processing 3. Defence (a critical defence industry asset) 4. Energy (a critical electricity asset, a critical gas asset, a critical energy market operator asset, a critical liquid fuel asset) 5. Financial Services and Markets (a critical banking asset, a critical superannuation asset, a critical insurance asset, a critical financial market infrastructure asset) 6. Food and Grocery (a critical food and grocery asset) 7. Health Care and Medical (a critical hospital) 8. Higher Education and Research (a critical education asset) 9. Space Technology, Transport (a critical port, a critical freight infrastructure asset, a critical freight services asset, a critical public transport asset, a critical aviation asset) 10. Water and Sewerage (a critical water asset)	The term "asset" in the Security of Critical Infrastructure Act, 2018 has been defined broadly and includes both critical information infrastructure and physical infrastructure.

[4]https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/compendium_of_good_practices_eng.pdf

[5]The Security of Critical Infrastructure Act 2018 (Cth) (the SOCI Act) provides a framework for managing risks relating to Australia's critical infrastructure, including national security risks of espionage, sabotage, and foreign interference. On 2 April 2022, the Security Legislation Amendment (Critical Infrastructure Protection) Act 2022 (Cth) (the SLACIP Act) came into effect. The SLACIP Act amends the SOCI Act and builds on the amendments of the Security Legislation Amendment (Critical Infrastructure) Act 2021 (Cth) that came into effect on 2 December 2022

Sl.No.	Country	Law	Critical Sectors	Definition
2	UK	The Security of Network & Information Systems Regulations, 2018 (NIS Regulations)	1. Chemicals 2. Civil Nuclear 3. Communications 4. Defence 5. Emergency Services 6. Energy 7. Finance 8. Food 9. Government 10. Health 11. Space 12. Transport 13. Water	Those critical elements of Infrastructure (facilities, systems, sites, property, information, people, networks and processes), the loss or compromise of which would result in a major detrimental impact on the availability, delivery or integrity of essential services, leading to severe economic or social consequences or to loss of life.
3	Cina[6]	Regulations on Critical Information Infrastructure (CII) Security Protection (CII Regulation)	1. Public Communications and Information Services 2. Energy 3. Transport 4. Hydraulic Engineering 5. Finance 6. Public Services 7. E-government 8. Defence Technology Industry *Note: The definition is broad and other industries can be covered if they fall within the definition of CII*	CII is defined as the important network infrastructure and information system, the destruction, loss of function or data leakage of which could seriously harm the state security, national economy, people's livelihood and public interest.[7]
4	Canada	*The National Strategy & The Action Plan*	1. Energy and Utilities 2. Finance 3. Food 4. Transportation 5. Government 6. Information and Communication Technology 7. Health 8. Water 9. Safety 10. Manufacturing	Critical Infrastructure refers to processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government. Critical Infrastructure can be stand-alone or interconnected and interdependent within and across provinces, territories and national borders. Disruptions of Critical Infrastructure could result in catastrophic loss of life, adverse economic effects, and significant harm to public confidence.[8]
5	France[9]	Security of Activities of Vital Importance	Security of Activities of Vital Importance 1. Food 2. Health 3. Water 4. Telecom & Broadcasting 5. Space & Research 6. Industry 7. Energy 8. Transport 9. Finance 10. Civilian administration 11. Military activities and Justice	Critical Information systems are those which are supporting vital functions of the operators and "whose unavailability could strongly threaten the economical or military potential, the security or the resilience of the Nation".

[6]https://www.twobirds.com/en/insights/2021/china/china-released-regulation-on-critical-information-infrastructure
[7]https://www.twobirds.com/en/insights/2021/china/china-released-regulation-on-critical-information-infrastructure
[8]https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/cci-iec-en.aspx
[9]https://www.ssi.gouv.fr/en/cybersecurity-in-france/ciip-in-france/faq/

Sl.No.	Country	Law	Critical Sectors	Definition
6	Germany	National Strategy for Critical Infrastructure Protection	As per the national strategy, the Critical Infrastructures can be classified into technical basic infrastructure, and socio-economic services infrastructure. These include : Technical Basic Infrastructure: 1. Power supply 2. Information and communications Technology 3. Transport/Transportation 4. (Drinking) Water Supply and Sewage Disposal Socio-economic services infrastructure: 1. Public Health 2. Food 3. Emergency and rescue services; disaster control and management 4. Parliament; Government; Public Administration; Law Enforcement Agencies 5. Finance; Insurance Business 6. Media; and Cultural Objects (cultural heritage items)	Critical infrastructures (CI) are organisational and physical structures and facilities of such vital importance to a nation's society and economy that their failure or degradation would result in sustained supply shortages, significant disruption of public safety and security, or other dramatic consequences.[10] The criteria laid down for assessing criticality in the National Strategy is a "relative measure of the importance of a given infrastructure in terms of the impact of its disruption or functional failure on the security of supply, i.e. providing society with important goods and services." [11]
7	Japan[12]	*The Cybersecurity Policy for Critical Infrastructure Protection*	1. ICT 2. Finance 3. Aviation 4. Airports 5. Railways 6. Electricity power supply services 7. Gases supply services 8. Governmental services 9. Health care 10. Water 11. Logistics 12. Chemicals 13. Credit card services 14. Petroleum industries	CI refers to sectors that comprise the backbone of national life and economic activities formed by businesses providing services that are extremely difficult to be substituted; if the function of the services is suspended or deteriorates, it could have a significant impact on national life and economic activities.
8	South Africa	Critical Infrastructure Protection Act[13]	The basic public services identified under the group are: 1. Communication 2. Energy 3. Health 4. Sanitation 5.Transport 6. Water	Under the Act, Critical Infrastructure is defined as— (a) The functioning of such infrastructure is essential for the economy, national security, public safety and the continuous provision of basic public services; and (b) the loss, damage, disruption or immobilisation of such infrastructure may severely prejudice— (I) the functioning or stability of the Republic; (ii) the public interest with regard to safety and the maintenance of law and order; and (iii) national security

[10]https://www.bmi.bund.de/SharedDocs/downloads/EN/publikationen/2009/kritis_englisch.pdf?__blob=publicationFile&v=2
[11]https://www.bmi.bund.de/SharedDocs/downloads/EN/publikationen/2009/kritis_englisch.pdf?__blob=publicationFile&v=2
[12]https://www.nisc.go.jp/eng/pdf/cs_policy_cip_eng_v4.pdf
[13]https://www.gov.za/sites/default/files/gcis_document/201911/4286628-11act8of2019criticalinfraprotectact.pdf

Sl.No.	Country	Law	Critical Sectors	Definition
9	US[14]	Presidential Policy Directive 21 (PPD-21)	1. Chemical Sector 2. Commercial Facilities Sector 3. Communication Sector 4. Critical Manufacturing Sector 5. Dams Sector 6. Defence Industrial Base Sector 7. Emergency Services Sector 8. Energy Sector 9. Financial Services Sector 10. Food & Agricultural Sector 11. Government Facilities Sector 12. Healthcare & Public Healthcare Sector 13. Information Technology Sector 14. Nuclear reactors, Material & Waste Sector 15. Transport System Sector 16. Water & Waste Water Systems Sector	Critical Infrastructure sectors are those whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.
10	EU	European Programme for Critical Infrastructure Protection[15] & COUNCIL DIRECTIVE 2008/114/EC of 8 December, 2008 on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection[16]	1. Energy 2. ICT 3. Water 4. Food 5. Health 6. Financial 7. Public & Legal Order and Safety 8. Chemical and Nuclear Industry 9. Space and Research 10. Transport	'Critical Infrastructure' means an asset, system or part thereof located in the Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions; European Critical Infrastructures constitute those designated critical infrastructures which are of the highest importance for the Community and which, if disrupted or destroyed, would affect two or more MS, or a single Member State if the critical infrastructure is located in another Member State. This includes transboundary effects resulting from interdependencies between interconnected infrastructures across various sectors. 'Sensitive Critical Infrastructure protection related information' means facts about critical infrastructure, which if disclosed could be used to plan and act with a view tocausing disruption or destruction of critical infrastructure installations;

[14]Critical Infrastructure Sectors | CISA
[15]https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF
[16]https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

Sl.No.	Country	Law	Critical Sectors	Definition
11	OECD[17]	Recommendation of the Council on Protection of Critical Information Infrastructures	• Health, • Safety • Security • Economic well-being of citizens • Government • Economy To identify CII, the document lists the following: • Information components supporting Critical Infrastructures • Information Infrastructures supporting essential components of government business • Information Infrastructures essential to the national economy	CII is defined as referring to those interconnected information systems and networks, the disruption or destruction of which would have a serious impact on the health, safety, security, or economic well-being of citizens, or the effective functioning of the government or the economy.
12	Un[18]	The protection of Critical Infrastructures against terrorist attacks: Compendium of good practices[19]		The document refers to the OECD definition and highlights that we may be nearing a point where the distinction between infrastructure and information infrastructure may be irrelevant, as the two merge into one ever-expanding circle.

[17]https://legalinstruments.oecd.org/public/doc/121/121.en.pdf
[18]https://press.un.org/en/2017/sc12714.doc.htm
[19]https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/compendium_ of_good_ practices_eng.pdf

CII Practices in India

In our previous report on **Modernising Policy Framework for Protecting India's Critical Information Infrastructure (CII),** we had dealt with the existing practices for protecting Critical Information Infrastructure across sectors in detail. For the sake of brevity and ease of understanding, the prevailing practices are recapped in this section.

Critical Infrastructure is defined under Section 70 of the Information Technology Act, 2000 as a computer resource, the incapacitation or destruction of which shall have a debilitating impact on national security, economy, public health or safety. The Information Technology (National Critical Information Infrastructure Protection Centre and Manner of Performing Functions and Duties) Rules, 2013 further define "Critical Sector" as sectors, which are critical to the nation and whose incapacitation or destruction will have a debilitating impact on national security, economy, public health, or safety. National Critical Information Infrastructure Protection Centre (NCIIPC) has been designated as the national nodal agency for CII Protection. Section 66F(1)(A) of the IT Act categorises an attack on CII as cyber terrorism, which is punishable with imprisonment that may extend to imprisonment for life. Section 70(1) of the IT Act provides that the appropriate government can notify any computer resource which directly or indirectly affects the facility of CII to be a protected system. Section 70(3) of the IT Act provides punishment for securing unauthorised access to a protected system for a term that may extend to 10 years, along with a fine.

The National Cyber Security Policy, 2013[20] also deals with the protection of CII with one of its objectives being the enhancement of the protection and resilience of CII by operating a 24x7 NCIIPC and mandating security practices related to the design, acquisition, development, use and operation of information resources. The National Cyber Security Policy also mandates creating mechanisms for dialogue related to technical and operational aspects with industry to facilitate efforts in recovery and resilience of systems, including CII.

NCIIPC has issued guidelines for the identification and assessment of Critical Sectors.[21] NCIIPC first assesses the criticality of the functions and services and their impact. The criticality and impact are examined on parameters such as the impact on customers and Government functions, the timeframe after which the impact level of non-availability of the ICT infrastructure will be very significant (shorter timeframe indicates higher criticality), geographical or environmental impact and level of dependency. If the above assessment indicates a significant impact nationally, the business/ industrial processes of the organisation/entity are evaluated. This assessment is made on parameters such as the size and economic value of the business /industrial process, the criticality of the business process and the estimated magnitude of impact in case of incapacitation/ destruction of the underlying ICT infrastructure timeframe, after which the impact level of non-availability of the ICT infrastructure will be very significant (shorter timeframe indicates higher criticality), geographical or environmental impact and level of dependency. A detailed explanation of the parameters is provided in the guidelines for the identification of CII. Based on the estimation of the above parameters, various business and/or industrial processes are then grouped as critical or non-critical. Consequently, the underlying computer resources of critical processes along with their interconnected dependencies will be categorised as CII.

The Information Security Practices and Procedures for Protected System Rules, 2018[22] provide for security practices to be adopted by the organisation and its responsibility towards NCIIPC for information

[20] https://www.meity.gov.in/writereaddata/files/downloads/National_cyber_security_policy-2013%281%29.pdf
[21] https://nciipc.gov.in/documents/Guidelines_for_Identification_of_CII.pdf
[22] https://www.meity.gov.in/writereaddata/files/NCIIPC-Rules-notification.pdf

sharing and enforcing guidelines. With respect to CII, NCIIPC has also issued guidelines for the Cyber Security Audit baseline document,[23] a guidance note on building resilience against cyberattacks during the COVID-19 crisis[24], suggested roles and responsibilities of CISO[25], guidelines for the protection of CII[26] Framework for Evaluating Cyber Security[27], SOP for incident response28[28], and SOP for auditing CII[29]. CERT-In has issued Information Security Policy for Protection of CII[30] and Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet [31]. The Cyber Security Policy also deals with CII among other things[32]. MeitY has also issued top best practices for CISOs for a safe and secure Cyber Environment[33], as well as Key Roles and Responsibilities of Chief Information Security Officers (CISOs) in Ministries/Departments and Organisations managing ICT operations.[34] CERT-In has also recently released guidelines on information security practices[35]. These guidelines have been issued under section 70B of the Information Technology Act, 2000 and apply to all Ministries, Departments, Secretariats, and Offices. These guidelines include aspects such as security domains such as network security, identity and access management, application security, data security, third-party outsourcing, hardening procedures, security monitoring, incident management, and security auditing.The above-mentioned rules, policies, guidelines, and directions cover the overall protection of CII. These guidelines are built upon by the sectoral regulators such as Power, Telecom, Finance, etc.

In the Power Sector[36], Sectoral CERT has been identified for Thermal, Hydro, Transmission, Distribution, Grid Operations and Renewable Energy. The CERTs identified are NTPC, NHPC, Powergrid, DP&T Division, CEA, NLDC and MNRE/SECI, respectively. Information Sharing and Analysis Centre (ISAC-Power) is the common platform for the six Sectoral CERTs under the Ministry of Power. The ISAC-Power is the central coordinating agency to share and analyse various cyber security incidents in the Power Sector. Cert-Power issued the CEA (Cyber Security in Power Sector) Guidelines, 2021. The guidelines focus on the protection and resilience of Critical Information Infrastructure. The CISO under these guidelines is required to submit to NCIIPC within 24 hours of occurrence, the report on every sabotage classified as cyber incidents(s) on Protected System. Apart from this, under these guidelines, the Responsible Entity shall submit to NCIIPC through Sectoral CERT, details of Cyber Assets that use a routable protocol to communicate outside the Electronic Security Perimeter drawn by the Responsible Entity or a routable protocol within a control centre and dial-up accessible Cyber Assets, within 30 days from the date of their commissioning in the System. The Responsible Entity is required to review their declared/notified CIIs at least once a year to examine changes, if any, in the functional dependencies, protocols, and technologies or upon any change in security architecture. In case the NCIIPC has directed the Responsible Entity to constitute an Information Security Steering Committee, it shall review their declared/notified CIIs once every 6 months. The Responsible Entity is mandated to submit details of Critical Business Processes and underlying information infrastructure along with mapped impact and risk profile to NCIIPC and shall get their CIIs identified in consultation with NCIIPC. All cyber assets of identified/notified CIIs are recorded in the asset register and are considered for risk assessment as well as for finalisation of controls in the statement of applicability. All ICT-based equipment/systems deployed in CII are to be sourced from the

[23]https://nciipc.gov.in/documents/CyberSecurityAuditbaseline.pdf
[24]https://nciipc.gov.in/documents/NCIIPC_COVID19_Guidelines.pdf
[25]https://nciipc.gov.in/documents/Roles_Responsibilities-CISO.pdf
[26]https://nciipc.gov.in/documents/NCIIPC_Guidelines_V2.pdf
[27]https://nciipc.gov.in/documents/Evaluating_Cyber_Security_Framework.pdf
[28]https://nciipc.gov.in/documents/SOP-Incident_Response.pdf
[29]https://nciipc.gov.in/documents/SOP-CII_Audit.pdf
[30]https://mapit.gov.in/securityaudit/downloads/CERT-In%20Info_Sec_Policy.pdf
[31]https://cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf
[32]https://nciipc.gov.in/documents/National_Cyber_Security_Policy-2013.pdf
[33]https://www.meity.gov.in/writereaddata/files/cisos_top_best_practices_guidelines.pdf
[34]https://www.meity.gov.in/writereaddata/files/CISO_Roles_Responsibilities.pdf
[35]https://www.cert-in.org.in/PDF/guidelinesgovtentities.pdf
[36]https://cea.nic.in/power-sector-information-sharing-and-analysis-center-isac-power/?lang=en

list of the 'Trusted Sources' as and when drawn by MoP/CEA.

In the Telecom Sector, National Security Council Secretariat came out with a directive for sourcing telecom products and services.[37] The directives are effective from 15 June,2021. As per the directives, the Government will declare a list of Trusted Source/ Trusted Product for the benefit of Telecom Service Providers (TSPs). NCSC will make its determination on the list of Trusted Products based on approval of the National Security Committee on Telecom (NSCT) headed by Deputy NSA. The Committee consists of members from the relevant department/ministry and will also have 2 members from the industry and an independent expert. In 2020, the Department of Telecommunication also came out with best practices relating to cyber security. These practices catered to organisation level and user level.[38]

In the Finance Sector,[39] the Working Group for Setting Up of Computer Emergency Response Team in The Financial Sector (CERT-Fin), 2017 recommended the creation of CERT-Fin to act as an umbrella CERT for the financial sector and report to CERT-In. Apart from this, the Reserve Bank of India (RBI) has continuously focused on ensuring a resilient cybersecurity framework. In 2016, the RBI had come out with a cyber security framework for banks[40] which, inter alia, required banks to come out with a cyber security policy which is distinct from the IT Policy/IS policy. Further, on October 19, 2018 the RBI issued basic cyber security guidelines applicable to all Urban Co-operative Banks (UCBs). However, any UCB, depending on its self-risk assessment, the complexity of its Information Technology (IT)/ Information Security (IS) systems, the nature of digital products offered, and others, is free to adopt advanced cyber security norms as decided by their Boards. It is observed that the level of technology adoption is also different across the banks in this sector – some banks offer state-of-the-art digital products to their customers and some banks maintain their books of account in a standalone computer and use e-mail for communicating with their customers/supervisors/ other banks.[41] The RBI has recently also released its Draft Master Directions on Cyber Resilience and Digital Payment Security Controls for Payment System Operators[42] for public consultations, covering aspects related to robust governance mechanisms for identification, assessment, monitoring and management of these risks. The Parliamentary Standing Committee on Finance in its report titled "Cyber Security and Rising Incidence of Cyber/White Collar Crimes" also recommended that there is a need to collaborate closely with financial institutions to improve uptime and address recurring downtime in critical payment systems through investments in robust infrastructure, conducting regular security assessments and establishing effective incident response mechanism.

From the above, it can be understood that India is continuously trying to improve the resilience of its Critical Information Infrastructure. With the ongoing discussion on the Digital India Bill and the National Cyber Security Policy, it is the right time to revamp the protection of CII to cater to present-day needs.

While India's focus has been to continuously to improve its cyber security posture, a need for coordinated effort has been felt[43]. There is a need to build effective inter-governmental communication channels to ensure that work is not being done in silos. For achieving this, a common set of principles for the protection of CII & CI should be laid down under the Digital India Bill, which can be further built upon by the sectoral regulators. The reporting channels for CII/CI should however be through a single window with inbuilt transfer of information to relevant authorities. The Digital India Bill as dealt with in the previous sections, seeks to build a future-ready and future-proof framework for Digital India.

[37] https://www.trustedtelecom.gov.in/
[38] https://dot.gov.in/sites/default/files/2020_07_09%20Cybersec%20SA.pdf
[39] https://dea.gov.in/sites/default/files/Press-CERT-Fin%20Report.pdf
[40] https://www.rbi.org.in/commonperson/English/Scripts/Notification.aspx?Id=1721
[41] https://www.rbi.org.in/scripts/PublicationsView.aspx?Id=18717
[42] https://www.rbi.org.in/Scripts/bs_viewcontent.aspx?Id=4267
[43] https://www.meity.gov.in/writereaddata/files/DIA_Presentation%2009.03.2023%20Final.pdf

Regulatory Framework for India

As stated above, in our previous reports, we had identified 10 recommendations which need to be considered for a resilient CII. In this section, we would identify the mechanism of their implementation through policies and law.

Towards this end, we recommend that a separate policy on the protection of Critical Infrastructure and the present treatment of Critical Information Infrastructure may also be enhanced and included in the Digital India Act or a separate Act for the protection of Critical Information Infrastructure be enacted.

Recommendation	Implementation Mechanism	Details
Expansion of definition and scope of CII: Given the global trends and emerging technologies, the definition and protection accorded to CII need to be enhanced. A definition like that of the European Union (EU) and the Organisation for Economic Cooperation and Development (OECD) would be more appropriate in terms of the sectors covered. Critical Sectors in India have been defined under Section 2(e) of the Information Technology (National Critical Information Infrastructure Protection Centre and Manner of Performing Functions and Duties) Rules, 2013, as sectors that are critical to the nation, and incapacitation or destruction of these will have a debilitating impact on national security, economy, public health or safety. It is important to specify such critical sectors - e.g., communications, energy, banking, transport, etc. Some sectors are listed on the National Critical Information Infrastructure Protection Centre (NCIIPC) website; however, there is a need to include the same in the regulatory framework in the form of rules/regulations/directions to ensure clarity. High-impact entities in critical sectors should be defined as Critical Sector Entities. The Critical Information Infrastructure of these Critical Sector Enterprises should be evaluated and notified such as NPCI, LIC and CIIs. There is also a need to define the non-IT Critical Infrastructure of these Critical Sector Enterprises as Critical Infrastructure. The Board of Critical Sector Enterprises should be responsible for setting up the Information Security Governance framework for their respective entities, with support from national nodal bodies. An approach like the one specified by the Information Security Steering Committee (ISSC) for Protected Systems, as specified in the Information Technology (Information Security Practices and Procedures for Protected System) Rules, 2018 can be followed. Further, **there is a need to define the parameters for classifying Critical Information Infrastructure as a Protected System under Section 70(1) of the Information Technology Act, 2000.** The present NCIIPC guidelines do have guidelines to identify CII. However, the guidelines for classifying CII as a protected system need to be further evolved.	Legal & Policy	Broadening the definition: In India, there are 7 sectors that have been identified as critical sectors, with Health being the recent addition, post the AIIMS attack. We recommend the addition of Data Storage and Processing also as a critical sector. In the policy, there should also be a provision to update these sectors on a regular basis. The definition of Critical Information Infrastructure should be amended in the following manner: 'Critical Infrastructure' means an asset, system, network, facility, computer resource, computer system, premise and any other thing as may be prescribed, the incapacitation or destruction of which shall have a debilitating impact on national security, economy, public health, safety, economic and social wellbeing of its citizens. NCIIPC, in the Act, should be empowered to notify the mechanism for identifying high impact entities in critical sectors and identifying their Critical Infrastructure, and identifying protected system through notification/ directions. NCIIPC should maintain a comprehensive record of Critical Infrastructure Assets, containing information in relation to those assets. These records must not be made public and should be exempt from RTI disclosures. The requirements for notifying cyber security breaches, implementing directions by NCIIPC and civil penalties for enforcement of these should be defined in the Act.

Adoption of Global Best Practices & Cross-Border Knowledge Sharing: In today's connected world, no country can mitigate the cyber threats to CII effectively on its own. Hence, there is a need for building globally accepted standards of CII and implementing them at the national level. It is equally important to adopt global best practices in national laws and create a system for cross-border knowledge sharing. This will also be an essential step towards improving India's geo-political position.	Policy	The policy on Critical Information Infrastructure should, inter alia, list cross-border knowledge sharing as an objective. Further, there should be a specific provision for International Cooperation. Objective - *"To establish a mechanism for exchange of information and best practices and for co-ordinated protection of critical infrastructures."* International Cooperation: i. Support and device measures for minimising cross-border vulnerability (including vulnerability to natural disasters) of Critical Infrastructure. ii. Undertake expansion of existing initiatives and/or enter into new bilateral and multilateral agreements for information sharing, including but not limited to, best practices for the protection of Critical Infrastructure. *Note: The Parliamentary Standing Committee on Finance in its report titled "Cyber Security and Rising Incidence of Cyber/White Collar Crimes" presented to the parliament on July 27 also recommended a proactive global regulatory framework by encouraging information sharing and joint threat intelligence.*[44]
Comprehensive Risk Assessment: With the rise in technology adoption, there is a need to have a comprehensive risk assessment for studying cyber security controls that need to be applied to Cloud. The risk assessment should also focus on the protection that is required to be provided to the physical critical infrastructure by the law enforcement agencies which support the CII.	Legal	The following functions may be included in Rule 4 - Functions and Duties of the National Critical Information Infrastructure Protection Centre under the Information Technology (National Critical Information Infrastructure Protection Centre and Manner of Performing Duties) Rules, 2013: *I. The National Critical Information Protection Centre shall undertake a security and resilience risk assessment of Critical Infrastructure based on the framework decided and updated from time to time by NCIIPC, in consultation with the committee comprising NCIIPC, MeitY, NSCS, etc.* Provided that the organisations responsible for managing and operating Critical Infrastructure shall cooperate with the National Critical Information Protection Centre for conducting the security and resilience risk assessment of Critical Infrastructure. *ii. NCIIPC, in consultation with organisations responsible for managing and operating Critical Infrastructure, decide the components of the security and resilience risk assessment.*

[44] https://sansad.in/ls/committee/departmentally-related-standing-committees/12-finance-nameH=%E0%A4%B5%E0%A4%BF%E0%A4% A4%E0%A5%8D %E0%A4%A4

Addressing Multiplicity of Regulation & Regulators: Multiplicity of regulators and regulations governing the same field should be avoided. The multiple compliances, audits, forums, and information-sharing channels are time-consuming for organisations dealing with CII. The focus in such cases shifts from protection to compliance and information sharing.	Legal & Policy	There is a need to establish a central authority for cyber security. The Parliamentary Standing Committee on Finance in its report titled "Cyber Security and Rising Incidence of Cyber/White Collar Crimes" presented to the parliament on July 27 recommended that there is a need for centralized authority in ensuring cyber security particularly for the financial services ecosystem. The committee noted that while the National Cyber Security Coordinator (NSCS) is responsible for coordinating and overseeing and compliance of cyber security policies there is no central authority dedicated to cyber security. Committee was of the view that the existing decentralized approach disperses regulation and control and thus hinders unified direction and a proactive approach to combating cyber threats. The National Critical Information Protection Centre should continue to be the nodal agency with respect to Critical Infrastructure in accordance with the Gazette notification dated 16 January,2014.[45], read with Information Technology (National Critical Information Infrastructure Protection Centre and Manner of Performing Duties) Rules, 2013. In addition to the above, the Rule 4 - Functions and Duties of the National Critical Information Infrastructure Protection Centre under the Information Technology (National Critical Information Infrastructure Protection Centre and Manner of Performing Duties) Rules, 2013 may be amended as follows: 4(11) Issuing guidelines, advisories and vulnerabilities or audit notes etc. relating to the protection of Critical Information Infrastructure and practices, procedures, prevention and response in consultation with stakeholders, in close coordination with Indian Computer Emergency Response Team, Sectoral Computer Emergency Response Teams and other organisations working in the field and related fields. Provided that the organisations operating and managing Critical Infrastructures should be required to report to NCIIPC.
Providing Baseline Guidelines and Sector Specific Guidelines: The baseline guidelines should be laid down by NCIIPC, which can be built upon by the sector specific regulator, based on the requirements of the sector concerned. It may however be noted that the same should not result in multiple regulations operating in the same space and creating multiple reporting channels. At present, NCIIPC has provided some baseline guidelines for the protection of CII, such as cyber security audit baseline requirements, etc. It is seen that, at times, other regulators operating in the same sphere issue guidelines rather than building upon it.	Legal & Policy	For the implementation of this recommendation, we suggest amending Rule 4 of the Information Technology (National Critical Information Infrastructure Protection Centre and Manner of Performing Duties) Rules, 2013 in the following manner: "4(6) Assisting in development of appropriate plans, adoption of standards, sharing of best practices, refinement of procurement processes, issuing directions, guidelines in respect of protection of Critical Information Infrastructure." Clause 4 to Section 70A of the IT Act, 2000 should be added, which reads as follows: "Any service provider, intermediaries, data centres, body corporate or person managing or operating Critical Infrastructure, who fails to provide the information called for or comply with the direction under sub-section (6), shall be punishable with a fine which may extend to XXXX rupees."

[45]https://www.meity.gov.in/writereaddata/files/S_O_18%28E%29_0.pdf

		Further, Section 70A(2) be amended in the following manner: "The national nodal agency designated under sub-section (1) shall be responsible for all measures including Research and Development relating to the protection of Critical Information Infrastructure and defining baseline guidelines. Provided that the nodal agency shall, in defining these baseline guidelines, work in close coordination with Indian Computer Emergency Response Team, Sectoral Computer Emergency Response Teams and other organisations working in the field and related fields, and these organisations shall be free to further develop on these baseline guidelines for their respective sectors and arrive at sector specific plans or guidelines."
Establishing Government's Internal Communication Channels: There is a need to reassess the multiple notification requirements by multiple regulators in the CII framework. There is a need to reconcile the duplicative and conflicting notification obligations. The Government should implement an information sharing system so that all relevant regulators are informed when the primary regulator, e.g. NCIIPC, is informed by the regulated entities. The obligation of the critical sector enterprise organisations should only be to inform the primary regulator and the Government should establish its internal communication channels. This is to say that a single interface between the Government and the Critical Sector Enterprise should be created which links all the regulators at the backend.	Legal	Rule 4- Functions and Duties of the National Critical Information Infrastructure Protection Centre under the Information Technology (National Critical Information Infrastructure Protection Centre and Manner of Performing Duties) Rules, 2013 may be amended as follows: "National Critical Information Protection Centre shall devise appropriate mechanisms and channels for inter-government communication channels for coordinated action relating to Critical Infrastructure in consultation with Indian Computer Emergency Response Team, Sectoral Computer Emergency Response Teams and other organisations working in the field and related fields."
Risk Mitigation: The focus of the CII framework should not be limited to cyber attacks. A comprehensive framework should focus on ensuring continuity of services during natural disasters, power outages, etc. An attack on one CII may likely have a domino effect on other CIIs as well. Therefore, the focus of the Government should be on ensuring continuity, irrespective of the cause. It must be ensured that there are appropriate safeguards which are built in, as a risk mitigation approach.	Policy	The policy for the protection of Critical Information Infrastructure should define risk in a manner that consists of natural events, technical failures, human errors, cyber security incidents, and cyber attacks.
Public Private Capacity Building: There is a need for enhanced government-industry partnership focusing on reinvigorating strategies, improving coordination, designing best practices, and capacity building.	Policy	The policy on Critical Infrastructure may consider adding a clause on Building Cooperation: Building Cooperation: *Comprehensive protection of Critical Information Infrastructure requires coordinated efforts by Government, industry, academia and subject matter experts. Therefore, NCIIPC will endeavour to work closely with such above mentioned organisations with an aim to reinvigorate strategies, improve coordination, design best practices and continuously undertake capacity building efforts.* Similar provisions already exist in Rule 7 of the Information Technology (National Critical Information Infrastructure Protection Centre and Manner of Performing Duties) Rules, 2013.

Continuous Monitoring: A more comprehensive framework for continuous monitoring should be built for the protection of technologies including Cloud supporting CII. At present, as per the Meghraj 2.0 guidelines, the responsibility is on the user department and Communications Service Provider (CSP). Concerning CII, an inter-departmental committee should be set up, which can include members from NCIIPC, CERT-In, and Sectoral CERTs to evaluate the continuous monitoring process and responsibilities, so that effective remedial and anticipated action can be taken in response to emerging threats.	Policy	Rule 4(5) of the Information Technology (National Critical Information Infrastructure Protection Centre and Manner of Performing Duties) Rules, 2013 already lists monitoring as one of the functions of NCIIPC. In the policy for the protection of Critical Infrastructure, a sub-committee of the advisory committee set up under Rule 6 of the Information Technology (National Critical Information Infrastructure Protection Centre and Manner of Performing Duties) Rules, 2013 should review the monitoring process. As per Rule 6(d), the advisory committee may constitute sub-committees to address any specific issue relating to the functioning of NCIIPC. Therefore, a sub-committee should be formed for the purpose of regular assessment which consists of the following members: • Centralised cyber security authority • MHA • NSCS • NCIIPC • MeitY • CERT-In • Sectoral CERT, Regulator, Ministry. (Special Invitees) • Domain Experts (Special Invitees) • Representatives of Protected Systems (Special Invitees) • Industry Representatives (Special Invitees) 2)The sub-committee should evaluate assess and monitor responsibilities so that effective remedial and anticipated action can be taken in response to emerging threats. One of the points of the Parliamentary Standing Committee on Finance in its report titled “Cyber Security and Rising Incidence of Cyber/White Collar Crimes” presented to the parliament on July 27 recommended the Government to consistently evaluate the impact of AI tools along with periodic assessment to monitor the effectiveness of potential drawbacks of AI tools. Accountability standards should be set in this regard for all concerned entities. Establishing such a committee would help in such evaluation and future evaluations for emerging tech. This activity may also be covered by the empowered committee with overall responsibility of the Central Authority for cyber security. In addition, the Central Authority may also undertake dummy exercises to assess preparedness for a cyber-attack.
Assessment of Cyber Attacks on CII: There is a need for autonomous Indian organisations to carry out independent analysis and trustworthy reporting of cyber attacks on CII.	Law	Rule 4- Functions and Duties of the National Critical Information Infrastructure Protection Centre under the Information Technology (National Critical Information Infrastructure Protection Centre and Manner of Performing Duties) Rules, 2013 may be amended as follows: “National Critical Information Infrastructure Protection Centre shall be responsible for carrying out independent and trustworthy analysis of cyberattacks on CII every XXX months/years”.

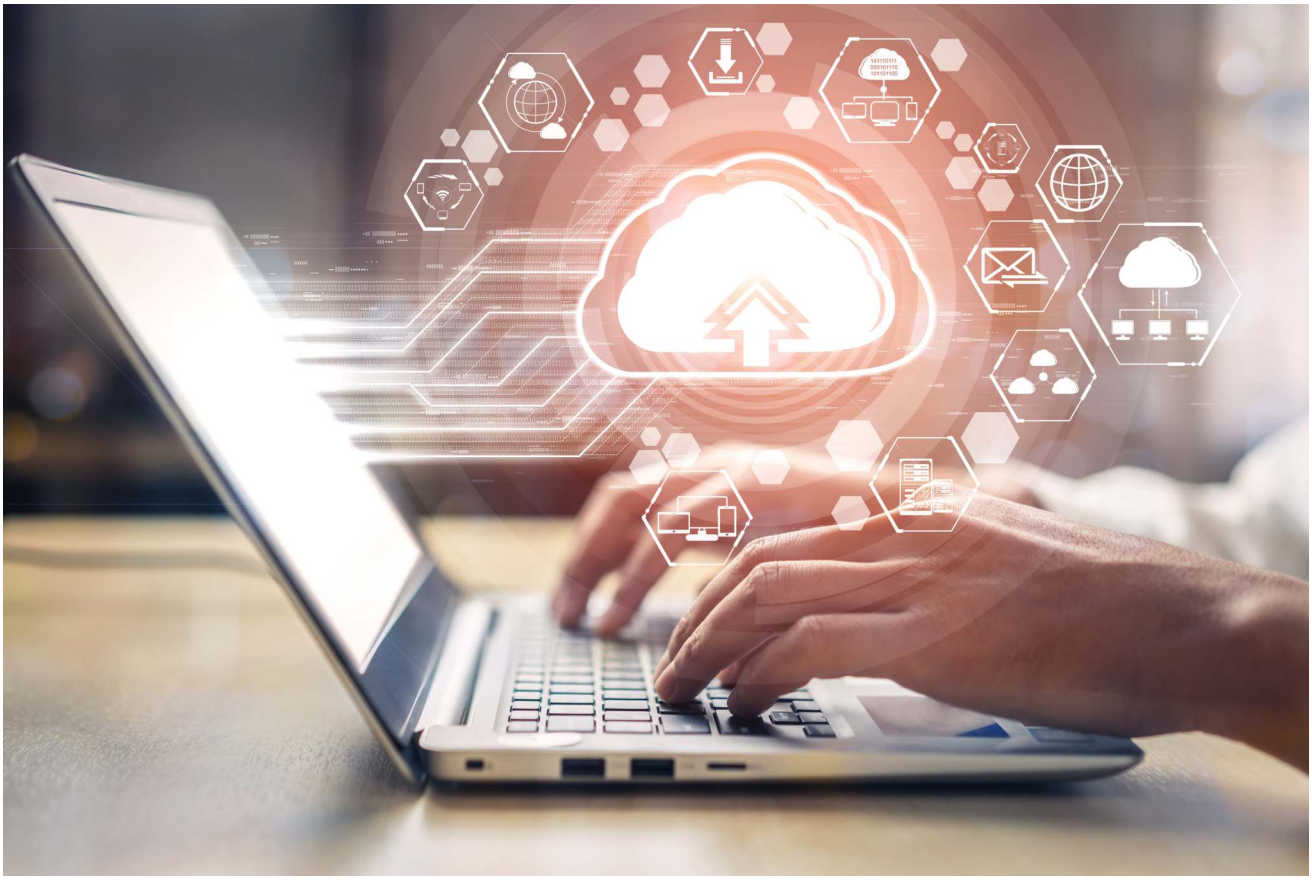
MSSPs: The working groups should focus on ways to encourage Managed Security Service Providers (MSSP) and other similar service providers to provide requisite support to the industry and for CII protection in India. This can be done by creating specific funds under PPP scheme.	Policy	The policy for the protection of Critical Infrastructure should contain the following clause with respect to Managed Security Service Providers and it can be added to the objective of the policy- "To encourage an ecosystem of cyber security professionals, especially with regard to Managed Security Service Providers (MSSP) and other similar service providers, and to provide requisite support to the industry and for CII protection in India." "Strengthening the Cyber Security Ecosystem: The advisory committee set up under Rule 6 of the Information Technology (National Critical Information Infrastructure Protection Centre and Manner of Performing Duties) Rules, 2013 will be empowered to take necessary measures for promoting the ecosystem and unlocking new capabilities in India."

Note: The above table represents the modifications/ additions required under the law/policy against each of the recommendations in our earlier report. The structure of the Policy, Rules, Acts, etc. would be different.

Findings & Way Forward

In view of the above discussion and findings, we recommend the formulation of a separate policy for protecting Critical Infrastructure and amendments to the IT Act to broaden the protection of Critical Infrastructure. This can be done through the creation of a working group to conduct a comprehensive risk analysis of CII in India and to revamp the protection afforded to CII in India. The working group should comprise cyber security experts from the Central Government and State Governments, industry, think tanks, and academia for a comprehensive approach.

Further, we recommend that the advisory committee as already formed under Rule 6 of the Information Technology (National Critical Information Infrastructure Protection Centre and Manner of Performing Duties) Rules, 2013 should review and monitor the implementation of the law and policy periodically for bringing necessary amendments in the same, to ensure a robust and updated ecosystem. The scope of the advisory committee should be enhanced in the Rules to include such activities and the same should be adopted by the Digital India Act. For a future-ready and future-proof framework for Digital India, focusing on an agile framework for CI/CII is imperative. Through these provisions, we hope to create such an agile framework.



CHASE INDIA

About Authors :

Srishti Saxena,
Former Account Director, Chase India,
ssaxena@chase-india.com

Dr. Dhawal Gupta
Group Business Director, Chase India,
dhawalg@chase-india.com

Kaushal Mahan
Vice President – Public Policy, Chase India,
kaushal@chase-india.com

About Chase India :

Founded in 2011, Chase India is a leading public policy research and advisory firm with growing practices in Technology & Fintech, Transport & Infrastructure, Healthcare & Life Sciences, Development and Sustainability. We provide consultancy services to organizations for mitigating business risks through insight-based policy advocacy. Over the years, Chase India has collaboratively worked with multiple stakeholders such as government, parliamentarians, civil society organizations, academia and corporates on several policy issues of critical importance. Chase India is committed to using its knowledge, high-ethical standards and result-oriented approach to drive positive action for our partners. Chase India has pan India presence with offices in New Delhi, Mumbai, Pune, Hyderabad, Chennai and Bengaluru and is a part of the WE Communications Group worldwide.

For more information, please visit www.chase-india.com

First Floor, 74, Link Road, Lajpat Nagar III, New Delhi – 110024, India.