CHASE INDIA

Modernising policy framework for Protecting India's Critical Information Infrastructure(CII)

November 2022

Executive Summary:

There has been an overall rise in cyber security incidents in India in recent years, as also incidents concerning Critical Information Infrastructure(CII). The CII framework in India is broadly covered under the Information Technology Act, 2000, and the rules made thereunder. There are a few sectoral guidelines issued by organisations such as Cert-Power, for which power is drawn through their parent Electricity Act, 2003. With the advancesin technology and emerging threats, there is a need to revamp the protection accorded to CII in India. Towards this report, we recommend the creation of a working group to conduct a comprehensive risk analysis of CII in India and strengthen the protection affordedto CII in India. The proposed working group should comprise cyber security experts from the Central & State Government, Industry, think tanks, emerging start-ups and academia for a comprehensive approach. The working group may look at the following aspects:

- **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[1]; 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 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.

1.https://nciipc.gov.in/

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 needs to be further evolved.

➔ **Adoption of Global Best Practices & Cross Border Knowledge Sharing**: In today's connected world, no country can mitigate the cyber threats to CII effectively by itself. 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 important step towards improving India's geo-political position.

➔ **Comprehensive Risk Assessment**: With the increase 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.

➔ **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.

➔ **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 regulator issue guidelines operating in the same sphere rather than building upon it.

➔ **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 at the backend links all the regulators.

➔ **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 It must be ensured that there are appropriate safeguards which are built in as a risk mitigation approach.

➔ **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.

➔ **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[2], 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.

➔ **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.

➔ **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 fund under PPP scheme.

2.https://www.meity.gov.in/writereaddata/files/Guidelines_Procurement_Cloud%20Services_v2.2.pdf

Introduction

The Indian government reported a total of 394499, 1158208, 1402809, and 674021 cyber security incidents during the years 2019, 2020, 2021, and 2022 (up to June), respectively.[3] These figures show an increasing trend in cyber security incidents in general. The graph of cyber security incidents concerning Critical Information Infrastructure (CII) also shows an upward trend. As per a report by cybersecurity company Trellix, cyber-attacks on critical infrastructure by nation-states and bad actors have increased significantly, and India observed a 70 percent increase in ransomware activity in the fourth quarter (Q4) of 2021.[4] Cyber security incidents on the country's CII and disruptions caused thereby can have wide and extreme ramifications on the country. Through this discussion paper, we seek to analyse the existing legal and policy ecosystem which protects CII nationally and internationally, to answer the following broad questions:

1. Whether the existing framework can efficiently manage cyber risk to CII in India

2. Whether the existing framework is adequate and updated considering the advancement in technology, its adoption, and the increasing sophistication of cyber-attacks

3. What critical components in the existing legal and regulatory framework require a change

To arrive at answers to these questions, we examined the present protection structure and the regulatory ecosystem surrounding CII in India, the associated challenges, and international best practices in protecting CII. Based on our findings explained in detail below, we recommend the creation of a working group to conduct a comprehensive risk analysis of CII in India and revamp the protection afforded to CII in India.

3.http://164.100.47.194/Loksabha/Questions/QResult15.aspx?qref=39267&lsno=17

4.htt://www.business-standard.com/article/technology/india-sees-70-spike-in-ransomware-attacks-on-critical-infrastructure-122042700442_1.html

CII Protection Structure

The overarching principles for the identification of CII have been laid down in the Information Technology Act, 2000 (IT Act). Critical Information Infrastructure is defined in the explanation of Section 70(1) of the IT Act. 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.

National Critical Information Infrastructure Protection Centre (NCIIPC) under the National Technical Research Organisation (NTRO) has been designated as the nodal body for the protection of CII.[5] The enforceable guidelines/directions for the protection of CII are scattered across the rules made under the IT Act[6] and directions given by NCIIPC, Cert-IN[7] , and Sectoral Certs.

The Cyber Security Policy, 2013 provides a broad framework and vision relating to protection of CII among other things[8].One of its objectives is to enhance the protection and resilience of the nation's CII by operating a 24x7 National Critical Information Infrastructure Protection Centre (NCIIPC) and mandating security practices related to the design, acquisition, development, use, and operation of information resources. The National Cyber Security Policy mandates creating mechanisms for dialogue related to technical and operational aspects with industry, to facilitate efforts in the recovery and resilience of systems including CII. The National Cyber Security Policy further mandates NCIIPC to develop a plan for the protection of CII and ensure its implementation and integration with a business plan at the entity level. The plans shall include establishing mechanisms for secure information flow (while in process, handling, storage and transit), guidelines and standards, a crisis management plan, proactive security posture assessment, and forensically

---

5.Section 70A of the IT Act, 2000 read with Rule 3 of the Information Technology (National Critical Information Infrastructure Protection Centre and Manner of Performing Functions and Duties) Rules, 2013

6.Information Technology (National Critical information Infrastructure Protection Centre and Manner of Performing Functions and Duties) Rules, 2013 & Information Technology (Information Security Practices and Procedures for Protected System) Rules, 2018.

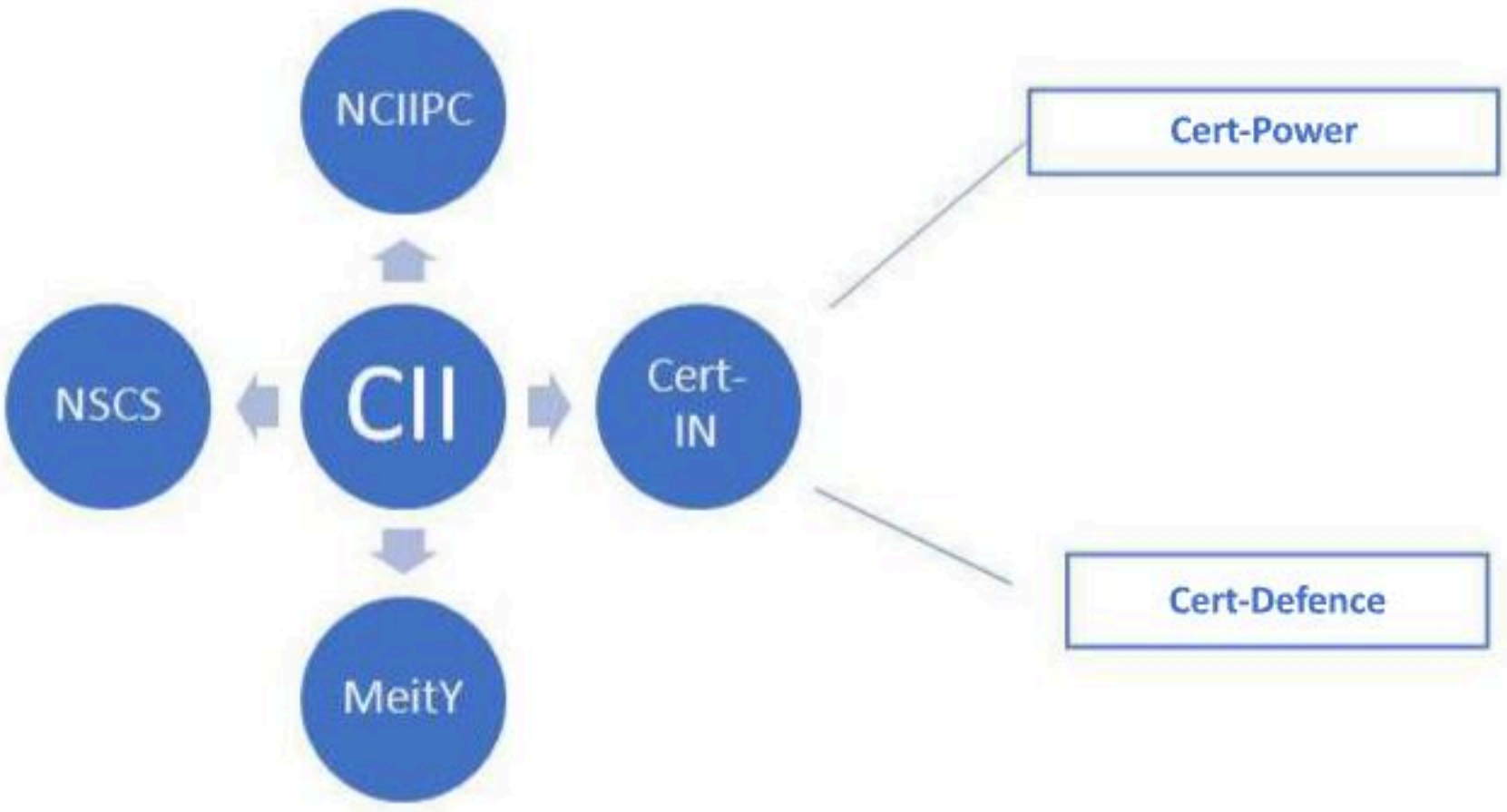
7.Section 70B of the IT Act, 2000 empowers CERT-In to call for information or issue directions on prevention, response, reporting etc. of cyber security incidents. Non-compliance of these directions is punishable with imprisonment for a term which may extend to one year or with fine which may extend to one lakh rupees or with both.

8.National Cyber Security Policy (1).pdf (meity.gov.in)

enabled information infrastructure. NCIIPC is also required to facilitate the organisations responsible for CII in the identification, prioritisation, assessment, remediation, and protection of CII and key resources based on the plan for the protection of CII. The cyber security policy mandates the implementation of global best practices and the use of validated and certified IT products. It prescribes periodic audits and certification of CII.

Sectoral Certs in Defence & Power are in force apart from Cert-In. Information Sharing and Analysis Centre (ISAC-Power) is the common platform for the six Sectoral CERTs under the Ministry of Power. The ISAC-Power focuses on the Central Information Resource pooling and sharing platform. It is a central coordinating agency to share and analyse various cyber security incidents in the Power Sector. The sector Certs such as CERT-Thermal, CERT-Hydro, CERT-Transmission, CERT-Distribution, CERT-Grid Operation, and CERT-Renewable Energy are under NTPC, NHPC, Powergrid, DP&T Division, CEA, NLDC, and MNRE/SECI, respectively.

Cert-Fin,acting as an umbrella CERT for the financial sector and reporting to CERT-In at the national level by the IT Act and Rules, was recommended by the Working Group for Setting Up of Computer Emergency Response Team in The Financial Sector (CERT-Fin) in 2017.[9] However, the recommendations have not been implemented yet.



9.https://dea.gov.in/sites/default/files/Press-CERT-Fin%20Report.pdf

Definition of Critical Information Infrastructure

Information Infrastructure is used to define the totality of interconnected computers and networks, and the information flowing through them.[10] Critical Information Infrastructure (CII) is defined under explanation to Section 70(1) of the IT Act as any computer resource, the incapacitation or destruction of which, shall have a debilitating impact on national security, economy, public health, or safety. The term computer resource has been defined under Section 2(k) of the IT Act as a computer, computer system, computer network, data, computer database, or software. The term computer system has further been defined[11] as *"a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programs, electronic instructions, input data, and output data, that performs logic, arithmetic, data storage, and retrieval, communication control, and other functions."*

It can therefore be seen that CII has been broadly defined in the IT Act and would include both interconnected hardware and software components if its breakdown impacts national security, economy, public health, or safety.

10.Guidelines for protection of Critical Information Infrastructure by National Critical Information Infrastructure Protection Centre released on 16th January 2015

11.Section 2(1)(l), Information Technology Act, 2000

Identification of Critical Information Infrastructure

The element of 'criticality' in CII is a lack of alternate options in case of disruption causing an impact on a nation's critical sectors and thereby affecting the public at large. With the advances in technologies and design, technical strides are being made to ensure the availability of the services under all circumstances and reduce the time for restoration to normalcy. The NCIIPC[12] is the nodal agency[13] for CII, and it assesses the criticality of the functions and services provided by the organisation / entity and the magnitude of impact on National Security, National Economy, Public Health, or Public Safety[14] in case of incapacitation/destruction of its ICT infrastructure based on the following parameters[15]:

(a) Impact on Customers, Business & Government functions based on the value of all types of transactions per day, total number of transactions per day, number of connected Devices and Network size, and number of Customers of different categories.

(b) Timeframe (hours/days/weeks) after which the impact level of non-availability of the ICT infrastructure will be very significant for National Security, National Economy, Public Health, Public Safety, Customers, Business, and Government (shorter timeframe indicates more critical).

(c) Timeframe (hours/days/weeks) after which the impact level of non-availability of the Business / Industrial Process will be very significant for National Security, National Economy, Public Health, Public Safety, Customers, Business, and Government (shorter timeframe indicates more critical).

(d) Level of Dependency is determined based on the impact of non-availability of Business / Industrial processes due to incapacitation or destruction of the underlying ICT infrastructure and degradation on other Critical Sectors and dependence of the Business / Industrial Process on other critical sectors/sub-sectors.

12.Organisation under NTRO

13.Vide Rule 3 of the Information Technology (National Critical Information Infrastructure Protection Centre and Manner of Performing of Functions and Duties) Rules, 2013

14.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.

15.https://nciipc.gov.in/documents/Guidelines_for_Identification_of_CII.pdf

If the above assessment indicates that functions and services of the organisation/entity have a significant impact nationally, there is a need to evaluate various Business and/or Industrial Processes of the organisation/entity from the point of view of identifying those computer resources, the incapacitation or destruction of which may have a debilitating impact on National Security, National Economy, Public Health or Public. The following parameters can be considered for the identification of critical business and/ or industrial processes of the organisation:

(a) Size & Economic Value of the Business /Industrial Process based on the value of all types of transactions processed per day, total number of transactions processed per day, number of connected Devices and Network size of the Business /Industrial Process, and number of Customers of different categories serviced.

(b) Criticality of the Business Process and estimated magnitude of impact on National Security, National Economy, Public Health, Public Safety, Customers, Business, and Government in case of incapacitation/ destruction of the underlying ICT infrastructure.

(c) Timeframe (hours/days/weeks) after which the impact level of non-availability of the Business / Industrial Process will be very significant for National Security, National Economy, Public Health, Public Safety, Customers, Business, and Government (shorter timeframe indicates more critical).

(d) Level of Dependency is determined based on the impact of non-availability of Business / Industrial processes due to incapacitation or destruction of the underlying ICT infrastructure and degradation on other Critical Sectors and dependence of the Business / Industrial Process on other critical sectors/sub-sectors.

Based on expert judgment and 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 to be CII. The appropriate government may, in consultation with NCIIPC, declare the identified CII of the concerned organisation through an 'Office Memorandum'. If needed, it may further choose to declare any computer resource which directly or indirectly affects the facility of CII, to be a 'Protected System'[16] through a notification in the Official Gazette.

16.Dealt with under Section 70 of the IT Act. The appropriate Government may, by notification in the Official Gazette, declare any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure, to be a protected system. Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.

Once a computer system is declared as a protected system, then any unauthorised access to such system is punishable by imprisonment for a term of up to ten years and shall also be liable to a fine. The Protected Systems are governed by Information Technology (Information Security Practices and Procedures for Protected System) Rules, 2018. These rules prescribe security practices to be adopted and the organisation's responsibility towards CII for information sharing and enforcing guidelines. Under these rules also, multiple procedural requirements focus on compliance and documentation rather than mechanisms to improve the cyber security posture. For example, Information Security Policies of the "Protected System" shall be approved by Information Security Steering Committee, a mechanism to report a cyber security incident to Information Security Steering Committee. Such provisions shift the focus and divert more resources to compliance.

Treatment of CII under the IT Act

While there may be overlapping aspects, the guidelines relating to CII can broadly be categorised into guidelines relating to the protection of CII, audit of CII, and incident reporting and management.

Protection of CII: In 2015, NCIIPC notified its guidelines for the Protection of CII.[17] Under these guidelines, the controls have been divided into five families represented in the diagram below. The detailed description of the controls is annexed in Annexure-1.

NCIIPC has also notified guidelines for evaluating cyber security in CII.[18] The implementation of these guidelines has been divided into four phases, which are as follows:

- **Phase-1 - Identifying Infrastructure and Existing Security Controls**: Under this, the organisation is expected to identify critical business processes, cyber security reporting structure, systems, related processes, existing security controls, Supervisory Control and Data Acquisition (SCADA), networks; and Security Controls applied for protection of all data that leaves or enters the local computer or local server from a network, services: services being used, and the services being

17.https://nciipc.gov.in/documents/NCIIPC_Guidelines_V2.pdf

18.https://nciipc.gov.in/documents/Evaluating_Cyber_Security_Framework.pdf

provided, along with existing cyber security controls, criticalities of their CII and Interdependencies on other organisations, i.e., the risk associated, and security control considered, asset owners-associated processes, risks, and security considered.

➔ **Phase-2 - Assess/Evaluate Vulnerabilities/Threats/Risks**: In this phase, the organisation needs to carry out an assessment/evaluation of the security controls (technological and/or procedural) identified in Phase 1. The evaluation covers Vulnerability-Threat-Risk assessments, Network architecture (with security devices in place), International Standards Applied, Organisational Policies, Human Resource Management Policies Specific to Cyber Security Controls, Compliance practices and correctness, and Consistency, and completeness of their security procedures.

➔ **Phase-3 -Implementation of Security Controls**: In this phase, the organisation operating CII is expected to accurately assess its findings of the assessment with NCIIPC and develop and implement an appropriate cyber security posture.

➔ **Phase-4 -Verify the implementation of Security Controls**: Under this phase, a cyber security audit must be conducted to assess the effectiveness of the cyber security controls implemented in Phase-3. The findings of the audit are expected to be shared with NCIIPC.

➔ **Phase-5 - Ensure Compliance to Audit**: The compliance report is required to be shared with NCIIPC. The residual risks must be signed off by senior management. Cert-IN has also issued a similar Information Security Policy for Protection of CII.[19] Under these guidelines, the Critical Sector organisation has required the organisations operating CII to identify senior management personnel as CISOs. In brief, the CISO will be responsible for the following:

- Be a point of contact for coordinating policy compliance efforts
- Regularly interact with Cert-In
- Prepare an information security plan and implement relevant security controls
- Carry out periodic IT security risk assessments and determine acceptable levels of risk consistent with the criticality of business requirements

---

19.https://mapit.gov.in/securityaudit/downloads/CERT-In%20Info_Sec_Policy.pdf

20.The requirement to undertake a regular and on-demand software asset management, cyber-risk analysis of your network, network resources and critical assets, threats and vulnerabilities, including audit of IT suppliers and vendors. Vulnerability Assessment & Penetration Testing (VAPT) of all websites and portals on quarterly basis at a minimum.Web Application Security Assessment (WASA) annually. This has been prescribed for CISOs in Ministry of Electronics and Information Technology vide D.O. No 5(4)/2016-ESD dated 19/5/2017 issued Key Roles and Responsibilities of Chief Information Security Officers (CISOs) in Ministries/Departments and Organisations managing ICT operations. Available at https://www.meity.gov.in/writereaddata/files/cisos_top_best_practices_guidelines.pdf

- Periodically test and evaluate the adequacy of technical security controls through Penetration Testing, Vulnerability Assessment, Application Security Testing, and Web Security Testing[20]

- Carry out an audit of information infrastructure on an annual basis and when there is a major upgradation in the Information Technology Infrastructure by an independent IT Security Auditing Organisation

- Report to Cert-IN the cyber security incidents as and when they occur, and the status of cyber security periodically, etc.

In the telecom sector, which is another crucial sector from a National Security perspective, guidelines have been laid down for sourcing telecom products and services on 16.12.2020, effective from 15.06.2021.[21] Under these guidelines, the Government notified that it will declare a list of Trusted Source/ Trusted Products for the benefit of TSPs. TSPs were required to connect new devices which are designated as 'Trusted Products'. NCSC is to make its determination based on the approval of a committee headed by the Deputy NSA. The Committee consists of members from the relevant department/ministry, industry, and an independent expert.

Audit of CII: Under the Cyber Security Audit baseline document for CII[22], the NSCS mandates baseline Requirements (CSA-BR) for CII. These baseline requirements act as a minimum, common, and harmonised criterion for cyber security audits. While the guidelines are to be mandatorily followed by all organisations with critical information infrastructure, NCIIPC encourages other public and private sector organisations to follow the baseline requirements. Under these guidelines, the organisation must define the criticality of the asset based on the risk assessment conducted and accordingly define the exposure level of any given infrastructure along with the scope and granularity of the markers. The management is responsible for defining the risk appetite during this process and the consequences thereof. As per the guidelines, an organisation's Cyber Infrastructure is classified into three risk profiles -

- High-Risk Information Infrastructure: Such infrastructures are those where the cyber-attack/ disruption will have an impact on CII.

- Medium Risk Infrastructure: In this infrastructure, the cyber-attack or disruption's impact will be limited within the organisation, but essential services of the organisation will be affected.

- Low-Risk Infrastructure: In this, cyber-attack/disruption will have minimal impact on the functions of the organisation.

21.https://www.trustedtelecom.gov.in/

22.https://cert-in.org.in/PDF/CyberSecurityAuditbaseline.pdf

Based on this classification, NSCS has defined the audit markers and baseline security requirements which have been detailed in Annexure-2.

In its SOP for auditing CII, NCIIPC has specified that certain CII of strategic importance can only be audited by Government organisations.[23] The SOP[24] categorises CII into two categories -

- Report to Cert-IN the cyber security incidents as and when they occur, and the status of cyber security periodically, etc.

- Critical Segment Category–I: Critical Segment Category-I consists of network segments in a CII/ Protected System with the classification 'Secret'[25] or 'Top Secret'[26] . A cyber security audit of a 'Critical Segment Category-I' must be carried out by a government auditor. The auditors must be working as permanent employees in a government organisation and must have served at least 4 years for the Government of India. Government auditors like STQC or any other government agency empaneled by CERT-In may be considered for conducting an audit of 'Critical Segment Category-I'.

- Critical Segment Category-II: Network segments in a CII/Protected System with a classification not greater[27] than 'Confidential'[28] would fall under the category Critical Segment Category-II. A cyber security audit of a 'Critical Segment Category-II' may be carried out by a private auditor.

Under the SOP[29] , following types of audits are required for CII:

a. **Internal Audit**: An internal audit is carried out by the Information Security team of the organisation who are part of the Information Security Group within the organisation. The members of an internal audit team must be a group of people with working knowledge of

---

23.https://nciipc.gov.in/documents/SOP-CII_Audit.pdf

24.Ibid

25.Information, unauthorised disclosure of which could be expected to cause serious damage to the national security or national interest or cause serious embarrassment in its functioning. This classification should be used for highly important information.

26.Information, unauthorised disclosure of which could be expected to cause exceptionally grave damage to the national security or national interest. This category is reserved for nation's closest secrets and is to be used with great reserve.

27.This would cover Confidential Information, Restricted Information (Information, which is essentially meant for official use only and which would not be published or communicated to anyone except for official purpose) and unclassified information (Information that requires no protection against disclosure e.g. Public releases.)

28.Information, unauthorised disclosure of which could be expected to cause damage to the security of the organisation or could be prejudicial to the interest of the organisation, or could affect the organisation in its functioning.

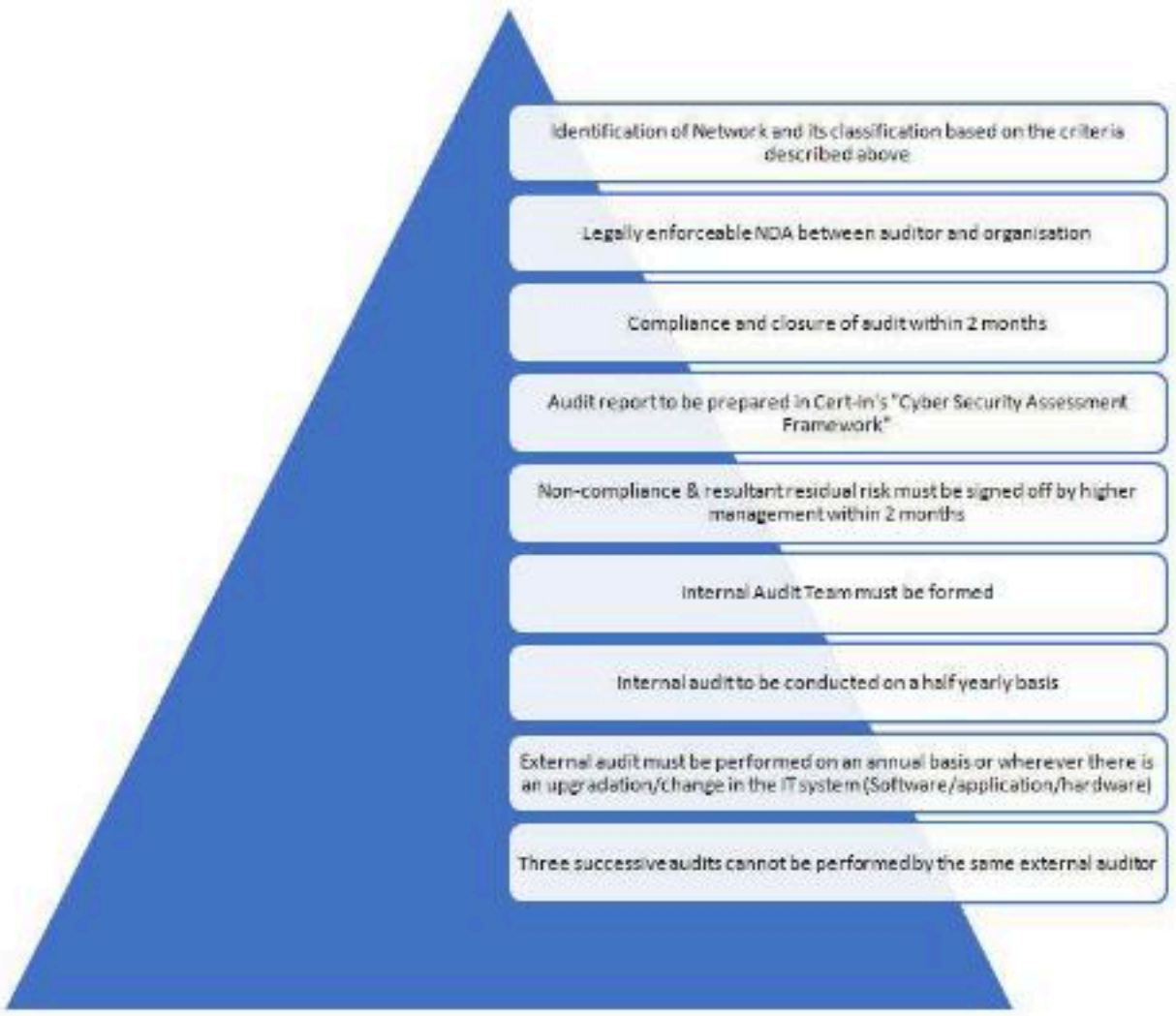
29.https://nciipc.gov.in/documents/SOP-CII_Audit.pdf

Information Security and operational technology used within the organisation. They must however, not be a part of the operational team.

b. **External Audit**: An external party audit can be carried out by any of the private/public auditors empaneled by the Government of India and/or recognised by popular international standards as recognised by the Government of India such as ISO27001, National Information Security Policy, and Guidelines, etc.

c. **Special Audit**: Specially formed group of auditors chosen from various government establishments for carrying out an audit of a CII/Protected System on a special requirement. The group of auditors may be chosen from the pool of auditors available in the Information Security Group of various CIIs/Protected Systems. This group may be constituted by picking expertise from various government establishments considering the types of technologies to be audited. Any group member of a special audit team shall not be chosen from the CII/protected system being audited, to ensure a transparent and fair audit. Indicative conditions for special audits are the Effectiveness of ISMS in a CII/Protected system is doubtable or request from the top management of a CII/Protected system to carry out a special audit for them etc.

The process of audit as defined in the SOP[30] is as follows:



30.https://nciipc.gov.in/documents/SOP-CII_Audit.pdf

Incident Response & Reporting: Cert-In has recently issued directions relating to information security practices, procedures, prevention, response, and reporting of cyber incidents for Safe & Trusted Internet, focusing on CII.[31] CERT-In has asked all government and private agencies, including internet service providers, social media platforms, and data centres to mandatorily report cyber security breach[32] incidents listed in Annexure-1 within six hours of noticing them. Incidents Concerning CII referred to in Annexure-1 are targeted scanning/probing of critical networks/ systems[33], Compromise of critical systems/information[34], and Attacks on Critical infrastructure.[35] Regarding these guidelines, multiple industry stakeholders had raised concerns that the time period of six hours is inconsistent with international norms. One of the primary concerns of the stakeholders was that such onerous obligations could contribute to the worst security position overall, as it would result in resources being diverted to ensure compliance with these directions rather than obtaining information and managing or mitigating the effects of the security incidents.

NCIIPC too has established protocols for responding to cyber security incidents impacting CII.[36] Under this, an NCIIPC Incident Response ('NCIIPC IR') team is constituted, comprising Team Lead / Incident Response Coordinator / Alternate Team Lead (to be nominated on a rotational basis, every quarter), Sectoral Coordinator (of the sectorconcerned), Domain Experts (Technology Specific / Vulnerability Analyst), Domain Expert (Live/Dead Forensics), Domain Expert (Network Forensics). The NCIIPC IR team is expected to be prepared with forensic accessories and if required, they may help the impacted CII organisation with collecting logs/mirror images. The SOP establishes two

---

31.htt://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf

32. Cyber security breach refers to unauthorised use of data by a person or an entity that compromises the confidentiality, integrity or availability of information maintained in a computer resource. This has been defined under Rule 2(i) of the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013.

33.As per FAQs issued by Cert-In on the directions dated 28.04.2022, targeted network scanning/probing refers to the action of gathering information regarding critical computing systems and networks, thus, impacting the confidentiality of the systems. It is used by adversaries to identify available network hosts, services and applications, presence of security devices as well as known vulnerabilities to plan attack strategies.

34.As per FAQs issued by Cert-In, gaining control of computer resource without permission typically through exploitation ofvulnerabilities. Attack methods for compromise may include "shoulder surfing", "social engineering", "exploitation of software vulnerability", "sophisticated malware" etc. Compromise of critical systems/information may impact all core aspects of cyber security viz. confidentiality, integrity and availability.

35.As per FAQs issued by Cert-In, SCADA systems are used for monitoring, and remotely controlling, geographically widely distributed processes from a centralised location. They have been incorporated for operational purposes in most of the critical infrastructure. Sophisticated malware are used by threat actors to target SCADA systems. The effect of these attacks can range from espionage to cause disruption of essential services. This type of incident impacts all core aspects of cyber security viz. confidentiality, integrity and availability.

36.https://nciipc.gov.in/documents/SOP-Incident_Response.pdf

incident reporting mechanisms, i.e., within the organisation dealing with CII and one from the impacted organisation to NCIIPC. The NCIIPC IR team, upon receipt of information, will assist the impacted organisation in mitigation of the cyber security incident, and disseminate information to other CII in close coordination with Cert-In. While the SOP provides for the steps for response by NCIIPC, it is silent on the procedure the impacted organisation may take to mitigate risks associated with cyber security incidents. A robust SOP must define the baseline parameters which are required to be followed by the impacted organisation for dealing with a cyber security incident.

Similarly, Cert-Power issued the CEA (Cyber Security in Power Sector) Guidelines, 2021[37]. 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.[38] Apart from this, under these guidelines, the Responsible Entity[39] shall submit to NCIIPC through Sectoral CERT, details of Cyber Assets[40] 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 is to be sourced from the list of the 'Trusted Sources' as and when drawn by MoP/CEA.[41]

The present CII framework has multiple duplicative and inconsistent obligations to report to multiple regulators, which adds to the compliance costs of critical entities. The focus should

37.https://cea.nic.in/wp-content/uploads/notification/2021/10/Guidelines_on_Cyber_Security_in_Power_Sector_2021-2.pdf

38.Article 12, CEA (Cyber Security in Power Sector) Guidelines, 2021

39.The term Responsible entities mean all Transmission Utilities as well as Transmission Licensees, Load despatch centres (State, Regional and National), Generation utilities (Hydro, Thermal, Nuclear, RE), Distribution Utilities Generation Aggregators, Trading Exchanges, Regional Power Committees, and Regulatory Commissions.

40.shall mean the programmable electronic devices, including the hardware, software and data in those devices that are connected over a network, such as LAN, WAN and HAN.

41.Article 1(vi), CEA (Cyber Security in Power Sector) Guidelines, 2021

instead be on improving cyber security posture. Multiple compliances alsoresult in diverting money to compliance that could otherwise be spent on security; and in adding to the burden of IT specialists, whose focus should be on responding to and mitigating the effects of the incident. It should however be noted that the federated cybersecurity ecosystem in India with multiple regulators, each working on similar aspects but with differentiated objectives, is resilient. A single overarching body may not be able to do justice to all the complexities of CII and regulate it comprehensively. However, to ensure that compliance costs of critical entities are reduced, and the focus is on cyber security rather than compliance, it is necessary to set up a mechanism for these national bodies to establish an automated information sharing and collaboration network. Such a network can harmonise the cyber security obligations of critical sector enterprises and reduce the cost of compliance.

Interdependencies between Public & Private Sector for protecting CII

In India, the majority of CII is owned, operated, and managed by the government. In rare cases, CII is being operated by the private sector, for example, the GST System, NPCI which was notified as a protected system by the Ministry of Finance. At that time, the system was being operated and managed by Goods and Services Tax Network, which had not been taken over by the Central Government. The private entity in such cases is required to follow strict compliance norms as prescribed above. Understanding interdependencies between the public and private sectors is fundamental to protecting CII. Even a government-owned CII will have associated IT infrastructure where private players will be involved. One of the important examples of this is adoption and usage of cloud computing. The CII may be owned by the government or its agencies. However, in case the CII is integrated with the cloud, the government and the cloud service provider will have shared responsibilities concerning securing the CII. For example, the cloud service provider will be responsible for securing the cloud platform and the government will be responsible for configuring its tenant to apply appropriate authentication controls.

Technology Modernisation

Technology modernisation is a priority for the government sector, which is evident from its focus on emerging technologies like GIS, AI and blockchain, and to ensure business continuity. The private sector also relies on technology to ensure business continuity. Cloud as IaaS solution helps businesses and governments to reduce maintenance of on-premises data centres, save money on hardware costs, give the flexibility to scale IT resources up and down with demand, and reduce security risk by leveraging the security updates,as well as research and development undertaken by cloud service providers. This model helps in the quick provisioning of new applications and increases the reliability of underlying infrastructure and has been implemented by organisations such as SEBI. Cloud in the Software as a Service (SaaS) model allows users to connect to and use cloud-based apps over the Internet, and leverage machine learning to identify and present common threat vectors. Common examples are email, calendar, and office tools, including tools that warn users that an unsolicited email might be a phishing attempt. This has been fundamental in ensuring continuity of operations during the COVID-19 related lockdowns. Under the Cloud Platform as a Service (PaaS) model, there is complete development and deployment environment in the cloud. PaaS model includes infrastructure—servers, storage, and networking—but also middleware, development tools, Business Intelligence (BI) services, database management systems, and more. PaaS is designed to support the complete web application lifecycle: building, testing, deploying, managing, and updating. Recognising the reliance on the cloud, the Central Government and some State Governments are adopting a cloud-first approach following the guidelines laid down in Meghraj 2.0. The cloud services for government projects are either provided by NIC or the empanelled cloud services providers, which at present include 18 private players.[42] Cloud in India is not treated separately as a CII, however, if it forms part of the network associated with protected systems, it falls within the definition of CII. Therefore, PPP in protecting CII is fundamental for an effective regime.

42.http://www.meity.gov.in/content/gi-cloud-meghraj

Protecting Cloud

Cloud computing is fast becoming the preferred way of ensuring continuity and running operations globally, specially concerning CII. The inherent advantages of the cloud - investment in security, more data on international malicious activity, greater resilience and redundancy with multiple data centre backups and rapid ability to deploy virtual machines, security, and privacy by design architecture, less need to devote financial resources to the maintenance of on-prem servers -make it an ideal choice for ensuring continuity of CII. While there are extreme benefits of cloud adoption, it does have its new age risks to consider, such as the need for the customer to cede control of some aspects of its operations. The cloud service provider users need to undertake risk assessments and balance the risks of moving to the cloud against the risks of keeping data in on-prem servers.India is fast moving towards a Digital India 2.0 with federated digital identities.It is understood that a cloud-first approach is the way forward to truly reap the benefits of digitisation.

From a CII perspective, cloud computing services can be critical in two ways -these services can be critical in themselves, or such services can be critical in their support of another critical service.[44] The special nature of cloud computing plays a role here. It is inherent to the cloud computing model that hardware and software are shared between multiple tenants. This is exactly what creates a benefit when it comes to withstanding DDoS attacks or peak loads. At the same time, this complexity in dependencies can create strange side effects. Outages at an underlying IaaS or PaaS provider can affect a range of (otherwise unrelated) services across society.[45] However, simply defining cloud as CII is also not the correct way forward. There is a need to determine what should be deemed 'critical'—the entire sector, a provider, a service, a particular function, a data centre, etc. The criteria regulators employ will determine the types and numbers of entities affected and raise jurisdictional issues.[46]

Globally, a trend is being seen where Cloud Service Providers are being held against the same standards for CII.[47] In India, wherever a cloud is associated with a CII or a protected system, the

---

43.Microsoft Word - InDEA 2.0 Report Draft V6 24 Jan 22_Rev.docx (mygov.in)

44.Critical Cloud Computing:A CIIP perspective on cloud computing services,European Network and Information Security Agency Version 1,0, December 2012

45.Critical Cloud Computing: A CIIP perspective on cloud computing services, European Network and Information Security Agency Version 1,0, December 2012

46.Working Paper on Cloud Governance Challenges: A Survey of Policy and Regulatory Issues, Ariel E. Levite and Gaurav Kalwani, Carnegie Endowment for International Peace.

47.Working Paper on Cloud Governance Challenges: A Survey of Policy and Regulatory Issues, Ariel E. Levite and Gaurav Kalwani, Carnegie Endowment for International Peace.

standards of CII apply to clouds too. Meghraj 2.0 also places strict compliance obligations on the empaneled cloud service provider for cyber security and disaster recovery, among other things. The Cert-In guidelines, 2022 inter-alia place obligations concerning cyber security and incident reporting on cloud service providers, while these guidelines are not restricted to only cloud service providers. NCIIPC in its Guidelines for the Protection of National Critical Information Infrastructure[48], has provided best practices for the cloud. These guidelines include using strong encryption methods, onus on the enterprise to manage data backup on its own, barriers to keep critical information separate from other information and organisations, securing cloud-organisation and cloud-cloud interlinkages, maintaining logs, securing access to critical information, network services, operation system, application and system, adequate authentication mechanism, risk management strategy, breach reporting mechanism, regular updating, and patching.

The multiple guidelines ensure that a CII protection plan for the cloud should be able to address cyber disruptions and cyber-attacks. Cyber disruption means the loss of cloud services which adversely impacts the users of CII. These disruptions could be because of natural disasters, power outages, etc. Cyber-attacks would include attacks such as DDoS etc. With the concentration of cloud services in major players, any impact through cyber disruption or attack is likely to have a large impact. Therefore, there is a need to proceed with care in general and especially when it comes to critical infrastructure.

It may, however, be noted that the cloud, thanks to its design cloud infrastructure, is more resilient to DDoS attacks and disruptions due to natural disasters, as compared to on-premises solutions. On-premise, solutions are also capital intensive and come with the constant need to maintain the continuity of technical human resource to ensure smooth operations and security of the solution. The government, therefore, needs to focus on cyber security, minimise the risk of disruptions in CII and ensure robust disaster recovery and drill, privacy, and compliance frameworks.

Cloud Service Providers are already applying some of the best practices to ensure cyber security. These include defense-in-depth, cybersecurity approach, and implementing secure operation practices such as deny-by-default, zero-trust architecture, least privilege, and multifactor authentication. This should be the key focus of organisations operating and maintaining CII[49]. This approach helps in eliminating risks attached to cyber attackers gaining control of IT systems and attacking the system from inside. Cloud Service providers also provide end-to-end backup and disaster recovery solutions that are simple, secure, scalable, and cost-effective, thus reducing recovery time. This is achieved through a centralised management interface which makes it easy to

48.https://www.asianlaws.org/gcld/cyberlawdb/IN/guidelines/NCIIPC_Guidelines_V2.pdf

49.https://azure.microsoft.com/mediahandler/files/resourcefiles/build-the-critical-infrastructure-services-of-the-future-with-microsoft-azure/Critical%20Infrastructure%20whitepaper%20Oct%202021.pdf

protect, monitor, and manage enterprise workloads across cloud-hybrid, private, public, and community[50].Configuring virtual machines (VMs) to failover to the cloud or between cloud data centres helps in protecting data from deletion and ransomware. Granular visibility and control coupled with segmentation capabilities prevent unauthorised deployments and allow blocking of suspicious activity. Encrypting all traffic and deploying machine learning-based threat protection and deeper micro-segmentation keeps the network protected at all edges. Data is encrypted at rest and in transit.[51] Smart machine-learning models can better classify data, a cloud-security policy engine can govern access decisions, and data loss prevention (DLP) policies secure sharing with encryption and tracking.[52] Clouds with broad compliance coverage and the ability to respond and rapidly build and deploy specific solutions to comply with country-specific and new regulations should be preferred for CII.

50.https://azure.microsoft.com/mediahandler/files/resourcefiles/build-the-critical-infrastructure-services-of-the-future-with-microsoft-azure/Critical%20Infrastructure%20whitepaper%20Oct%202021.pdf

51.https://cloudblogs.microsoft.com/industry-blog/government/2021/10/25/the-future-of-critical-infrastructure-is-in-the-cloud/

52.https://azure.microsoft.com/mediahandler/files/resourcefiles/build-the-critical-infrastructure-services-of-the-future-with-microsoft-azure/Critical%20Infrastructure%20whitepaper%20Oct%202021.pdf

Managed Security Service Providers (MSSPs)

Service providers such as MSSPs, threat intelligence, and analytics, cybersecurity architects, consultants, etc play a pivotal role in cyber security. They address the cyber security needs of organisations that do not have the capacity or expertise to have a dedicated security operations team. For more mature organisations, these service providers provide an independent outlook to review the cyber security alerts. These organisations should be encouraged to provide value-added services to the critical sector enterprises as they would also help in mitigating difficulties faced by Critical Sector Enterprises in hiring and retaining skilled cyber security professionals.

Such specialised services also help in reducing the cost, time, and effort spent by critical sector enterprises in compliance and use cloud services to scale up their capabilities. Their importance is evident in government and autonomous organisations procuring Governance Risk Compliance & Performance ('GRCP-SP'). GRCP-SP has a very important role in governing the security of ecosystem and ensuring a robust security governance programme. The scope of these service providers, interalia, includes information and cyber security for the internal ecosystem, field Information Security Assessment of all external ecosystem partners, fraud and forensics checking, and detection of any unauthorised activity related to the system on the internet.

An impetus to the abovementioned services under the would also provide a stimulus to CII protection in the country. This can be done by creating specific fund under PPP scheme.

International Perspective

There is no globally shared definition of Critical Information Infrastructure (CII). The principles of protecting CII are however similar. In this section, we cover some of the major international principles protecting CII. In 2003, G8 countries adopted 'Principles for Protecting Critical Information Infrastructures'[53]. These principles provide as follows:

i. Countries should have emergency warning networks regarding cyber vulnerabilities, threats, and incidents.

ii. Countries should raise awareness to facilitate stakeholders' understanding of the nature and extent of their critical information infrastructures, and the role each must play in protecting them.

iii. Countries should examine their infrastructures and identify interdependencies among them, thereby enhancing the protection of such infrastructures.

iv. Countries should promote partnerships among stakeholders, both public and private, to share and analyse critical infrastructure information to prevent, investigate, and respond to damage to, or attacks on such infrastructures.

v. Countries should create and maintain crisis communication networks and test them to ensure that they will remain secure and stable in emergencies.

vi. Countries should ensure that data availability policies consider the need to protect critical information infrastructures.

vii. Countries should facilitate tracing attacks on critical information infrastructures and, where appropriate, the disclosure of tracing information to other countries.

viii. Countries should conduct training and exercises to enhance their response capabilities and test continuity and contingency plans in the event of an information infrastructure attack and should encourage stakeholders to engage in similar activities.

ix. Countries should ensure that they have adequate substantive and procedural laws, such as those outlined in the Council of Europe Cybercrime Convention of 23 November 2001, and trained personnel to enable them to investigate and prosecute attacks on critical information infrastructures, and to coordinate such investigations with other countries as appropriate.

x. Countries should engage in international cooperation, when appropriate, to secure critical

53.http://www.cybersecuritycooperation.org/documents/G8_CIIP_Principles.pdf

information infrastructure, including by developing and coordinating emergency warning systems, sharing and analysing information regarding vulnerabilities, threats, and incidents, and coordinating investigations of attacks on such infrastructure by domestic laws.

xi. Countries should promote national and international research and development and encourage the application of security technologies that are certified according to international standards.

The United Nations General Assembly resolution on the creation of a global culture of cybersecurity and the protection of critical information infrastructures[54] and OECD recommendation on the Protection of Critical Information Infrastructures are broadly similar to the G8 guidelines[55]. Additionally, the OECD[56] guidelines focus on cross-border knowledge sharing and cooperation between the public and private sectors for the protection of CII. These guidelines propose a broad framework to ensure cyber resiliency and mitigating impact through the adoption of risk assessment and adoption of best practices. Similarly, European Union also seeks to protect its CII from cyber-attacks, manmade technological threats, and disruptions from natural disasters to reduce vulnerabilities and increase resiliency.[57] The European Programme for Critical Infrastructure Protection (EPCIP) provides the overall framework for the protection of critical infrastructure in European Union Member States. Under the 2008 Directive on European Critical Infrastructures, a procedure for identifying and designating European Critical Infrastructures (ECI) is established. It also provides a common approach for assessing the need to improve CII's protection. The Directive has a sectoral scope, applying only to the energy and transport sectors.[58]

Internationally, the focus of protecting CII is through understanding the inter-dependencies and involving the private sector to protect them. In multilateral cooperative agreements, the need to maintain an internal posture is necessary. However, there is a need to share information and best practices with other countries. In today's extremely inter-connected world, one of the preferred ways to ensure the resilience of CII is through cooperation and learning from best practices.

54.https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf

55.https://www.oecd.org/digital/ieconomy/40825404.pdf

56.https://www.oecd.org/digital/ieconomy/40825404.pdf

57.critical infrastructure' means an asset, system or part thereof located in 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;

58.https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

Recommendations

Cyber security is the dominant posture when it comes to the protection of CII in India. In today's times, the CIIs are disrupted not only by cyber-attacks, but also because of natural disasters, company-related outages, pandemics, etc. While cyber-attacks are the most concerning cause while protecting CII, other aspects must also be considered. In doing so, the focus of the rules, directions, etc should be on ensuring resilience and mitigating the impact of disruptions through strong disaster recovery plans. With this in mind, we offer the following recommendations for building a more resilient framework. This brings us to answer the three questions we began our research with. A joint response to the above mentioned three questions is that, while the structure is adequate for dealing with well-established technologies, the framework to regulate and protect the interplay between emerging tech and CII needs to be more robust.

Reportedly, the Indian Government is planning to amend the 22-year-old IT Act with a more relevant Digital India Act. One of the important aspects for the government to consider while amending the IT Act is the protection of CII. This topic is fundamental for ensuring the government's vision of a safe, open, accountable Digital India. Therefore, we recommend the creation of a working group to conduct a comprehensive risk analysis of CII in India and revamp the protection afforded to CII in India. The working group should consist of cyber security experts from the Central Government & State before Government, Industry, think tanks, and academia for a comprehensive approach. The working group may look at the following aspects:

- **Expansion of Definition and Scope of CII**: Given the global trends and emerging technologies, the definition and protection of CII need to be enhanced. A definition like the EU & 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 the incapacitation or destruction of which 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 NCIIPC's website[59], and 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 as CIIs. There is also a need to define the non-IT Critical Infrastructure of these Critical Sector Enterprises as Critical Infrastructure.

59.https://nciipc.gov.in/

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 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.

➔ **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. Therefore, there is a need to build globally accepted standards of CII and implement 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 important step towards improving India's geo-political position.

➔ **Comprehensive Risk Assessment**: With the increase in technology adoption there is a need to have a comprehensive risk assessment for studying cyber security controls that need to be applied to emerging tech like 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.

➔ **Addressing Multiplicity of Regulation 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 in creating multiple reporting channels.

➔ **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 regulated entities. The obligation of the critical sector enterprise 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 at the backend links all the regulators.

➔ **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.

➔ **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.

➔ **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[60], the responsibility lieson the user department and CSP. Concerning CII, an inter-departmental committee should be set up, which includes 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.

➔ **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.

➔ **MSSPs**: The working group should focus on ways to encourage MSSPs and other similar service providers to provide requisite support to the industry and CII protection in India. This can be done by creating specific fund under PPP scheme.

In conclusion, we recommend the creation of a working group of cyber security experts to study, analyse and recommend the way forward for a robust ecosystem for protecting CII, to ensure that emerging challenges are addressed efficiently and in a timely manner. With Digital India 2.0 being the focus of the Government and the Parliamentarians. It is imperative that CII of the Digital India 2.0 is secure and robust to meet the necessary challenges especially in the light of recent incidents of hybrid war.

60.https://www.meity.gov.in/writereaddata/files/Guidelines_Procurement_Cloud%20Services_v2.2.pdf

Annexure-1

Controls for protection of CII as per NCIIPC's guidelines for Protection of CII

i. **Planning Controls**: This set of controls is assessed at the design stage to ensure that security is taken as a fundamental designing parameter for all new CII.

ii. **Implementation Controls**: These controls translate the design planning into actual system security configurations. These controls also come into play in case of retrofitting existing, unprotected/poorly protected CII.

iii. **Operational Controls**: To ensure that security postures are maintained in the operational environment. These controls also come into play in case of retrofitting existing, unprotected/poorly protected CII.

iv. **Disaster Recovery/Business Continuity Planning (BCP) Controls**: These controls are essential to ensure minimum downtime, as well as to ensure that the restoration process factors in, and overco mes the initial vulnerabilities, or isolates infrastructure compromised by attackers, to ensure graceful degradation / minimum maintenance of service provided by the CII.

v. **Reporting and Accountability Controls**: These controls ensure that adequate accountability and oversight are exercised by senior management and ensure communication channels with government agencies where required.

Planning Control	Disaster Recovery	Implementation Control	Reporting & Accountability	Operational Control
• PC1: Identification of CII • PC2: Vertical and Horizontal • Interdependencies • PC3: Information Security • Department • PC4: Information Security • Policy • PC5: Integration Control • PC6: VTR Assessment and • Mitigation Controls • PC7: Security Architecture Controls including Configuration Management and Mitigation controls • PC8: Redundancy Controls • PC9: Legacy System Integration • PC10: Supply Chain Management – NDAs, extensions and applicability • PC11: Security Certifications • PC12: Physical Security Controls	• DR1: Contingency Planning – graceful degradation • DR2: Data Back-up and Recovery Plan, Disaster Recovery Site • DR3: Secure and Resilient Architecture Deployment	• IC1: Asset and Inventory • Control • IC2: Access Control Policies • IC3: Identification and Authentication Control • IC4: Perimeter Protection • IC5: Physical and Environmental Security • IC6: Testing and Evaluation of Hardware and Software	• RA1: Mechanism for • threat reporting to Govt. Agencies • RA2: Periodic Audit and • Vulnerability Assessment • RA3: Compliance of security Recommendation	• OC1: Data storage: Hashing and Encryption • OC2: Incident Management – • Response • OC3: Training, Awareness • and Skill upgradation • OC4: Data Loss Prevention • OC5: Penetration Testing • OC6: Asset and Inventory • Management • OC7: Network Device • Protection • OC8: Cloud Protection • OC9: Critical Information • Disposal and Transfer • OC10: Intranet Security • OC11: APT protection

Annexure-2

NSCS's Cyber Security Audit Baseline Requirements

Risk Profile	Category Controls	Mandatory Markers	Recommended Markers
High-Risk Information Infrastructure	Management	All Markers are Mandatory	Not Applicable
	Protection	All Markers are Mandatory	Not Applicable
	Detection	All Markers are Mandatory	Not Applicable
	Response	All Markers are Mandatory	Not Applicable
	Recovery	All Markers are Mandatory	Not Applicable
	Lessons learned & Improvements	All Markers are Mandatory	Not Applicable
Medium Risk Information Infrastructure	Management	All Markers are Mandatory	Not Applicable
	Protection	All Markers are Mandatory except for Recommended Section	pro.12, pro.13, pro.20
	Detection	All Markers are Mandatory except for Recommended Section	det.3
	Response	All Markers are Mandatory except for Recommended Section	res.1, res.8
	Recovery	All Markers are Mandatory	Not applicable
	Lessons learned & Improvements	All Markers are Mandatory	Not applicable
Low-Risk Information Infrastructure	Management	All Markers are mandatory except for Recommended Section	csm.11, csm.12, csm.14, csm.15
	Protection	All Markers are Mandatory except for Recommended Section	pro.12, pro.13, pro.16, pro.20, pro.21
	Detection	All Markers are Mandatory except for Recommended Section	det.3, det.4, det.7, det.9
	Response	All Markers are Mandatory except for Recommended Section	res.1, res.8, res.9
	Recovery	All Markers are Mandatory	Not Applicable
	Lessons learned & Improvements	All Markers are Mandatory except for Recommended Section	imp.4, imp.5

Baseline security controls

Control Category	Markers	Marker Identifier
Management	Organisation Information Security Policy and Audit Process is defined and established	csm[61].1
	Frameworks, standards, and/or best practices are	csm.2

61.Cyber Security Management

	adopted for cyber security	
	The commitment of Senior Management is ensured	csm.3
	Components of the infrastructure are identified and prioritised based on the criticality	csm.5
	Classification of Infrastructure as High, Medium, and Low Risk is aligned to business process, classification affirmed during the audit process	csm.6
	Components (hardware, software, systems, applications, networking components) of the organisation's information infrastructure are inventoried	csm.7
	Threats, vulnerabilities, likelihoods, and impacts are identified	csm.8
	Cyber Security Risks are identified	csm.9
	The Risk Management approach is effective and aligned with the business process	csm.10
	Risk Treatment Plan is established and accepted/residual risks are in tune with the criticality of related function	csm.11
	Critical Functions Continuity Plan /Business Continuity Plan which addresses the resilience of minimum-security controls is defined and implemented	csm.12
	Information/Cyber Security roles & responsibilities are defined and informed and trained upon	csm.13
	Adequate manpower and resources for Cyber Security function aredefined and provisioned	csm.14
	Cyber Security Crisis Management Plan is developed, implemented, and exercised by the organisation	csm.15
	The cyber security management approach addresses any legal, regulatory, or sector-specific compliance related to cyber security, and the same is adhered to by the organisation	csm.16
	Compliance with Audit Reports is ensured by the Management	csm.17
	Data is identified, labeled and its owner, custodians, and users are made aware and responsible	csm.18
	Access Control - Administrative, Physical and Technical controls, and their control model are identified	csm.19
Protection	Physical security controls for critical assets are implemented and managed	pro[62].1
	Access control – Identified controls are implemented in the specified model	pro.2
	Remote access and teleworking are controlled	pro.3
	Controls for Malware Protections are implemented, and effectiveness is ensured	pro.4
	The vulnerability and Patch Management process is implemented effectively	pro.5
	Controls for Removable Media and BYOD/BYOT are implemented	pro.6
	Wireless network security controls are implemented	pro.7
	Secure configuration for hardware, software, industrial	pro.8

62.Protective Controls

	control systems, network components, and applications are implemented and managed	
	Secure software development lifecycle is ensured (in-house as well as outsourced)	pro.9
	Perimeter security devices like Firewall, IDS/IPS, network monitoring, etc. are deployed in the organisation and they are monitored continuously	pro.10
	Vulnerability Assessment (VA) and implementation of corrective actions are done by the organisation continuously (VA by the internal team as well as empaneled Third-Party)	pro.11
	The scope of Penetration Testing Exercises is defined and its periodic conduct is ensured	pro.12
	Periodic Participation of organisation in national/ sectoral/ organisational Cyber Security Exercises is ensured	pro.13
	Role-based Cyber Security Training and awareness programs are conducted periodically for all employees and associated external entities	pro.14
	Content of cyber security training is appropriate	pro.15
	BCP and Disaster management plans are tested periodically, and continuity of security controls is tested	pro.16
	Data protection (-in-transit, at-rest) controls are implemented effectively	pro.17
	Data retention and destruction policies are defined and implemented	pro.18
	Change Control policy and practices are defined and implemented	pro.19
	Mapping and Securing Supply Chain including baseline compliance by vendors is ensured	pro.20
	Secure Disposal of IT Equipment is ensured	pro.21
Detection	Scope, mechanism, and frequency of log collection is defined and implemented	det[63].1
	Mechanisms for regularly analysing the alert/log data collected from different security devices is ensured	det.2
	Daily Log analysis of the critical services is maintained	det.3
	Monitoring of accounts and access is implemented	det.4
	Network Monitoring is implemented	det.5
	Physical security controls are monitored for possible cyber security incidents	det.6
	Adequate resources for log and alert analysis are available and roles andresponsibilities are clearly defined	det.7
	Synchronisation with a singular time source is ensured	det.8
	Detected incidents are analysed technically to determine cause, impact, attacker methodology	det.9
Response	Cyber Crisis Management Plan, in line with National Cyber Crisis Management Plan, is prepared and established	res[64].1
	Incident Response Plan is implemented	res.2

63.Detection Controls

64.Incident Response

	Roles and responsibilities for Incident Response are clearly defined	res.3
	The Incident Escalation matrix is defined	res.4
	The communication mechanism within the organisation is clearly defined for incident resolution	res.5
	The communication mechanism with stakeholders and agencies is clearly defined for incident resolution	res.6
	Contact details of ministries, stakeholders, vendors, and agencies like NCIIPC andCERT-In for incident resolutions are up to date and documented	res.7
	Incident/abuse reporting channel and mechanism is defined and implemented	res.8
	Information sharing mechanisms with external entities are clearly defined and implemented	res.9
	Incidents are recorded and investigated in terms of impact, the vulnerability exploited or attempted to exploit, attacker methodology, and attack source	res.10
	Incidents are contained and mitigated	res.11
Recovery	A recovery plan is defined and implemented	rec[65].1
	Resources are available for the recovery of critical functions	rec.2
	The recovery plan should incorporate lessons learned from crisis/incident	rec.3
Lesson Learnt & Improvement	Lessons learned from incidents and cyber exercises are incorporated into the response plan	imp.[66]1
	Lessons learned and improvement plans are documented, and commitment of management is ensured	imp.2
	CCMP and incident handling procedures/response plan are improved and updated	imp.3
	Organisation'sCyber Security posture is improved as compared to the last reference point (last assessment, last year, etc)	imp.4
	Organisation's performance is improved in successive Cyber Security exercises and training	imp.5

65.Recovery Controls

66.Improvement

About Authors

Srishti Saxena

Senior Manager
ssaxena@chaseindia.com

Kaushal Mahan

Vice President
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**

Acknowledgment

Chase India would like to acknowledge the valuable insights and inputs received from Industry experts, former goverment officials etc and experts who helped give shape to this report

Disclaimer