EXECUTIVE SUMMARY

With the advancement of convergent communication technologies and shared Information system in India, Critical Sectors are becoming more dependent on their Critical Information Infrastructures (CIIs). These CIIs are interconnected, interdependent, complex and distributed across various geographical locations. Various inherent threats exist to CIIs, ranging from terrorist attacks to organized crimes to espionage, malicious cyber activities, which are growing rapidly. Protection of CIIs and hence CIs of the nation is the one of the paramount concerns of the Government.

To this endeavor, Government of India, has designated 'National Critical Information Infrastructure Protection Centre' (NCIIPC) of National Technical Research Organisation (NTRO) as the nodal agency under Section 70A(1) of the Information Technology (Amendment) Act 2008 for taking all measures including associated Research and Development for the protection of CIIs in India.

NCIIPC is driven by its mission "To take all necessary measures to facilitate protection of Critical Information Infrastructure, from unauthorized access, modification, use, disclosure, disruption, incapacitation or destruction, through coherent coordination, synergy and raising information security awareness among all stakeholders" and with a vision "to facilitate safe, secure and resilient Information Infrastructure for Critical Sectors in the country".

This document presents forty controls and respective guiding principles for the protection of CIIs. These controls and guiding principles will help Critical Sectors to draw a CIIP roadmap to achieve safe, secure and resilient CII of the nation. The 'Guidelines for forty Critical Controls' is one of the significant milestones in our efforts for the protection of nation's critical information assets.

"Guidelines of protection of National Critical Information Infrastructure" is designed in active consultation with all stake holders with a holistic approach. Summary of stakeholder's recommendations and NCIIPC's remarks are in Annexure 'A'. Introductory part deals with the general organisational structure and potent threats to them along with need to insulate and evolve countermeasures.

CIIs shall not be seen in isolation rather vertical and horizontal interdependencies within and among organizations. The organisational structure required to devise, evolve and carryout plans, policies and programs are also discussed. Section 5 of the document provides vision, mission and guiding principles for NCIIPC to achieve its objective.

In section 6 on 'Best practices, Controls and Guidelines' <u>forty controls</u> are described, which are to be followed by CIIs. An attempt has been made to include all Critical Controls The controls are: (1) Identification of CIIs; (2) Vertical and Horizontal interdependencies; (3) Information Security Department; (4) Information Security Policy; (5) Training and Skill up gradation; (6) Data loss Prevention;(7) Access Control Policies; (8) Limiting Admin Privileges; (9) Perimeter

Protection; (10) Incident Response; (11) Risk Assessment Management; (12) Physical Security; (13) Identification and Authentication; (14) Maintenance Plan; (15) Maintaining Monitoring and Analysing logs; (16) Penetration Testing; (17) Data storage-Hashing and Encryption; (18) Feedback mechanism; (19) Security Certification; (20) Asset and Inventory Management; (21) Contingency Planning; (22) Disaster Recovery Site; (23) Predictable Failure Prevention; (24) Information/Data Leakage Protection;(25) DoS/DDoS Protection; (26) Wi-Fi Security; (27) Data Back-up plan; (28) Secure Architecture Deployment; (29) Web Application Security; (30) Testing and Evaluation of Hardware and Software; (31) Hardening of Hardware and Software; (32) Period Audit; (33) Compliance of Security Recommendations; (34) Checks and Balances for Negligence; (35) Advanced Persistent threats (APT) Protection; (36) Network Device Protection; (37) Cloud Security; (38) Outsourcing and Vendor Security; (39) Critical Information Disposal and Transfer; (40) Intranet security

Abbreviations

Sl. No.	Abbreviation	Full Form
1.	3G	3rd Generation
2.	AAA	Authentication, Authorization and Accounting
3.	ACL	Access Control List
4.	AMC	Annual Maintenance Contract
5.	API	Application Programming Interface
6.	APT	Advanced Persistent Threat
7.	BCP	Business Continuity Planning
8.	BDA	Breach Disclosure Agreement
9.	BYOD	Bring Your Own Device
10.	CCTV	Closed Circuit Television
11.	CD	Compact Disc
12.	CERT	Computer Emergency Response Team
13.	CISO	Chief Information Security Officer
14.	CII	Critical Information Infrastructure
15.	CIIs	Critical Information Infrastructures
16.	COTS	Commercial off-the-shelf
17.	CSD	Centre for Security Development
18.	CSRF	Cross Site Request Forgery
19.	DoS	Denial of Service
20.	DDoS	Distributed Denial of service
21.	DMZ	Demilitarized Zone
22.	DNS	Domain Name Server
23.	DR	Disaster Recovery
24.	DVD	Digital Video Disc
25.	FTP	File Transfer Protocol
26.	GPRS	General Packet Radio Service
27.	HaaS	Hardware as a Service
28.	HR	Human Resource
29.	HTTP	Hyper Text Transfer Protocol
30.	HTTPS	Secure HTTP
31.	IaaS	Infrastructure as a Service
32.	IP	Internet Protocol
33.	IDS	Intrusion Detection System

34.	IIT	Indian Institute of Technology
35.	IISc	Indian Institute of Sciences
36.	IODR	Insecure Direct object Reference
37.	IPS	Intrusion Prevention System
38.	IRM	Information Rights Management
39.	IS	Information Security
40.	ISD	Information Security Department
41.	ISMS	Information Security Management System
42.	ISO	International Standard Organisation
43.	ISPo	Information Security Policy
44.	ISP	Internet Service Provider
45.	IT	Information Technology
46.	LAN	Local Area Network
47.	LEA	Law Enforcement Agency
48.	MAC	Media Access Control
49.	MITM	Man-in-the-Middle
50.	MO	Mobiles
51.	MSS	Managed Security Services
52.	MTBF	Mean time between Failure
53.	MTTF	Mean Time to Failure
54.	NADS	Network Anomaly Detection System
55.	NBA	Network Behavioral Access
56.	NDA	Non Disclosure Agreement
57.	NCIIP	National Critical Information Infrastructure Protection
58.	NCIIPC	National Critical Information Infrastructure Protection Centre
59.	NIDS	Network Intrusion Detection System
60.	NIPS	Network Intrusion Prevention system
61.	NIT	National Institute of Technology
62.	NMS	Network Management System
63.	NOC	No Objection Certificate
64.	NTP	Network Time Protocol
65.	OEM	Original Equipment Manufacture
66.	OS	Operating System
67.	OWASP	Open Web Application Security Project
68.	P2P	Peer to peer
69.	PaaS	Platforms as a Service
70.	PDA	Personal Digital Assistant
71.	PKI	Public Key Infrastructure
72.	PPP	Public Private Partnership

73.	PSU	Public Sector Undertaking
74.	R&D	Research and Development
75.	RDP	Remote Desktop Protocol
76.	RPO	Recovery Point Objective
77.	RTO	Recovery Time Objective
78.	SaaS	Software as a Service
79.	SDLC	Secure Development Life cycle
80.	SCADA	Supervisory Control and Data Acquisition
81.	SIEM	Security Information and Event Management
82.	SLA	Service Level Agreement
83.	SNMP	Simple Network Management Protocol
84.	SOC	Service Operation Centre
85.	SQL	Structured Query Language
86.	SSH	Secure Shell
87.	SSID	Service Set Identifier
88.	SSL	Secure Sockets Layer
89.	TCP	Transport Control Protocol
90.	TLS	Transport Layer Security
91.	UDP	User Datagram Protocol
92.	UPS	Uninterrupted Power Supply
93.	URL	Uniform Resource Locator
94.	USB	Universal serial Bus
95.	VPN	Virtual Private Network
96.	WAN	Wide Area Network
97.	Wi-Fi	Wireless Fidelity
98.	WiMax	World Wide Inter-Operability for Microwave access
99.	WPA	Wi-Fi Protected Access
100.	XSS	Cross Site Scripting