KARNATAKA CYBER SECURITY VISION 2025

PREPARED BY KJA TASK GROUP

Karnataka Jnana Aayoga
(Karnataka Knowledge Commission)
Government of Karnataka

AUGUST 2019
Karnataka Cyber Security Vision 2025
AUGUST 2019

Karnataka Jnana Aayoga
(Karnataka Knowledge Commission)
Government of Karnataka
Dr. K Kasturirangan  
Chairman, KJA

MESSAGE

We are witnessing a period of dramatic digitalization of human activity - where vast amount of data is being systematically sensed/measured, collected/archived and is becoming part of a large system of data of human activity. The growth in internet connectivity, the expansion in the number of connected digital devices and the rapid developments in big data, cloud computing, data analytics, machine learning, advanced robotics and artificial intelligence are changing the way society develops - in terms of citizen activity, industrial processes, education systems, governance systems and the "thinking" of human beings. On the flip side, the vast network of connected systems and digitalization - especially in mission-critical, financial, national security and other system, the emerging threats of cyber-attacks has been growing and is a major concern for various nations. Even as technology is making the digitalization process simple and easy, the sophistication in cyber-attacks and cyber-crime is rapidly growing.

Karnataka has been the leading state in the IT domain and is in vanguard position to address cyber-security in a holistic manner and must take up responsible action in developing a vision for cyber-security - which can not only help the state but also the nation, at large. The state needs to assume responsibility for the "holistic security", including cyber-security - apart from citizen welfare, economic growth, public health, excelling education systems and a range of other activities that are fundamental to the prosperity and well-being of the state's citizenry. The internet has become such a pervasive part of public and private life that it is now a vital component of Governance and Citizen lives - bearing tremendous responsibilities on the Government and individual citizens to "collaborate" for security of cyber systems - be they individual citizen devices/systems OR government systems of total governance and development.

Cyber-security policies and legislation are required and need to evolve - backed by well-tested norms/practices and standards - that become practical do's and don’ts for cyber-security. Constant training, orientation, awareness in cyber-security and its developments is yet another step that is required. It is also essential to promote advanced research and technology development in the field of soft- and hard-cyber-security systems. Home-grown technology from industries and utilization is yet another critical step so that Indian industries can offer state-of-art solutions to the national needs of cyber-security.
It is against this backdrop that the Aayoga took up the task of preparing a vision and action plan for Cybersecurity in the state and invited a set of best experts in the country to draft a vision and strategy plan. The group was chaired by the eminent expert-Prof N Balakrishnan, Emeritus Professor of IISc and had Members from the state and the nation. The group developed this Cybersecurity Vision for the State of Karnataka and mapped out best practices and required action – including, cybersecurity regulations/policies, establishing an apex and expert State Cybersecurity Council as a single-point technology agency, immediate need for cybersecurity education and research in the state, promoting indigenous technology and products development and an eco-system for industrial development and for a critical advanced cybersecurity infrastructure in the state governance systems. The Aayoga has considered the report of the expert group in its 8th meeting and developed the KJA Recommendation on Cybersecurity Vision for the State of Karnataka. I am happy that the recommendation is being submitted to the Government.

I urge the Government to consider these recommendations and take up necessary steps for its implementation through the governmental system. I am confident that the Karnataka Cybersecurity Vision would help the government to bring in a set of action which will bring benefits to the state and its own vision of development of digital government functioning and operations.

I thank the Members of TG especially Prof. Balakrishnan, Co-Chair of the Task Group and Prof. Sridhar, Member-Secretary of the Task Group for their excellent and diligent work in drafting the vision document.

I also would like to express my gratitude to the Members of the Aayoga, especially Dr. Mukund Rao for guiding and steering the activities of this Task Group and for adopting the recommendation.

On behalf of the KJA, I am extremely happy to submit the KJA Recommendation on Karnataka Cybersecurity Vision to Government of Karnataka for consideration and effective implementation.

July 24, 2019

(K. Kasturirangan)
Chairman, KJA
KARNATAKA CYBER SECURITY VISION 2025

FOREWORD

Karnataka Jnana Aayoga (KJA) is a recommendatory body established by the Government of Karnataka, under the Chairmanship of Dr K Kasturirangan with experts and professionals in various fields as Members - who, together, bring a wealth of knowledge and expertise through new ideation, undertake extensive brain-storming and wide consultations on extremely important and relevant issues for the state’s development. KJA has already recommended various policy, technology and innovative knowledge interventions/studies addressing various problems of governance and of society.

One of the areas that KJA has recognized as critical and important is Cybersecurity. Cybersecurity is the suite of technologies, processes and practices that are designed and implemented to protect networks, computers, programs and data from attack, damage or unauthorized access. Cybersecurity would include Application security, Information security, Network security, Disaster recovery / business continuity planning, Operational security etc. Cyber security, therefore, is highly relevant across various government, industries, academia – State Data Centres, e-gov services, K-GIS, IT companies, Bio-technology, Aerospace, Retail, Healthcare, Intelligence, Hospitality, Banking and Finance, Military etc. The growing importance of Cybersecurity is also due to the increasing reliance of citizens and society on computer systems and digitalization, the wide usage of Internet for exchange of services and information, access to wireless networks that provide the channels for information flow, the growth of "smart" devices that link up users and services, including smartphones, televisions and many tiny devices as part of the Internet of Things (IoT). Apart from these, more disruptive developments of Bots, Malware, Bitcoins, Darknet, DeepWeb, Ransomware and large-scale usage of Big data, Cloud technology, Robotics, Blockchain etc are posing innumerable challenges.

In Karnataka (and the nation), government, industry, society, academia and even individuals are conducting large and many transactions through the internet and thus can be exposed to potential threats to both hardware and software and their digital assets. Citizens and individuals access most services – banking, postal, e-commerce, travel, hospitality, health, schooling and many other services on the net. In fact, citizens have a lot of their personal data on the networks and internet through emails, records, family history and images and many other personal materials on internet. Thus, securing and protecting the cyber eco-system becomes critical and important.

Karnataka is an established leader of e-Governance and leading the country in m-governance and g-governance – number of government services are online; Aadhar data is critical for services; banking
platforms are large; insurance systems are intensively sued; manufacturing and education services are wide and important. Karnataka is having the right eco-system for being at the front and leading Cybersecurity actions in India – with the large IT eco-system and also a progressive IT-oriented government in the state. Hence, it is only obvious for Karnataka to develop a comprehensive and in-depth cyber security policy, provide impetus to cybersecurity technology and applications development and enabling state-wide security of our cyber eco-system.

KJA in its 7th meeting held on September 7, 2017 discussed on the importance and relevance of cybersecurity for Karnataka and its associated issues and challenges. As an outcome of this discussion, an expert Task Group on Karnataka Cybersecurity Vision was constituted by KJA to prepare the Karnataka Cybersecurity Vision by addressing all aspects of data, systems, network, services and so on.

Over the past 12 months, the TG has had large number of consultations - with the departments, in particular with Principal Secretary, Dept. of IT/BT; various industry groups; academic institutions and central agencies to obtain ideations and suggestions on need for Cybersecurity programmes. Along with this TG had extensive meetings with Data Security Council of India to explore cyber security initiatives taken up by them; consultations were conducted with IIT-Madras, C-DAC, Hyderabad and Cybercrime Research and Training Institute (CCRTI), CID HQ, Bengaluru. The TG has made specific recommendations across 7 areas– Protection and Enforcement actions; Competency and Skill Development in education and research systems; Product Testing and Certification for quality cybersecurity products; Business Promotion for industrial development; Research and Development for advanced home-grown technology; best of Policies and Regulations and Outreach Programmes and Awareness building.

The TG report was considered by the Aayoga in its 8th meeting held on June 21, 2019 and various suggestions for crystallised actions and roadmap were made. These suggestions have been included and the Aayoga has endorsed and approved this KJA Recommendation on Karnataka Cybersecurity Vision - a comprehensive short- and long-term action plan on Cybersecurity and has defined a roadmap of technological development, systems implementation and applications development, policies, education and research and citizen awareness in the state. As part of this vision, the Aayoga recommends for implementation of a fully operational State Cyber Command Centre – to make Cybersecurity a top-attention and bring mission orientation. The Vision can be easily implemented by Government of Karnataka involving industries, academia and civil society.
On behalf of the Aayoga, I would like to acknowledge the yeomen contributions of the KJA Task Group on KCSV - in particular the eminent Prof. Balakrishnan, who was ably supported by Prof. Sridhar of IIIT-B and many expert members - specifically, Dr. Sanjay Bahl, Mr. Preet Paramjit Singh, Mr. Sanjiv and Prof. Raghunath and all others for their intense discussions, technological analysis and tireless efforts in drafting the TG report. I would also like to express gratitude and thanks to Principal Secretary, Dept. of IT/BT for all his support and invaluable suggestions and in engaging with KJA.

I also take this opportunity to thank all the KJA Members - who provided the guidance and direction for the TG and in finalizing these recommendations of the Aayoga. The leadership provided by Dr K Kasturirangan has been the driving force for the KJA and also in finalizing these recommendations. He has provided the vision direction and a deeper systemic understanding for cybersecurity and societal interface - thanks and respectful gratitude to Dr Kasturirangan - the leading light for KJA.

The KJA Secretariat, in particular Dr Jayashri has played all the background and nitty-gritty role of linking/stitching together all the various notes/discussions/ideas and helping in drafting the report - not once but many times over. Dr Jayashri has supported the TG and the KJA in making these Recommendations to reality - thanks to her.

I am happy that the KJA Recommendation on Cybersecurity Vision is being submitted to Government and I am confident that the Recommendation would be considered by the government and appropriately taken up for implementation. KJA is confident that the Vision will provide useful operational and strategic actions to cyber security issues and to various stakeholders across the state. KJA would like to see Karnataka emerge as the "Cybersecurity Power" of the nation and of the world!!

July 24, 2019

(Mukund Kadursrinivas Rao)
Member-Secretary
Mukund.k.rao@gmail.com
KARNATAKA CYBER SECURITY VISION 2025

PREFACE

Karnataka Jnana Aayoga constituted a Task Group on Karnataka Cyber Security Vision (TG-KCSV) to develop a comprehensive and in-depth cyber security policy and define a roadmap of technological development, systems implementation and applications development, education and research and citizen awareness in the state. The members of the TG were experts in various domains of the Cyber landscape, who brought their vast experience into the preparation of the report.

In recent times, technology, particularly cyber technology has become an integral part of every one’s life. This has created a techno-social world wherein all the good and bad activities one witnessed in the real social world have found their place albeit at a faster pace and enhanced anonymity. The bad side of this cyber world manifest in the form of cybercrime, cyber frauds and attacks on the individual’s privacy and the nation’s digital and financial assets. Fintech, which is an integral part of common man’s life, has become the biggest and easy target for criminals.

With the massive growth in the usage of social networks such as Facebook, Twitter, WhatsApp, etc. it has also become necessary for the users to realise about protecting their identity from being stolen, and also the ability to detect fake and terrorists related news as well as the ability to use these media responsibly. It has also become necessary in today’s world to identify the misuse of the social media by others, avoid and shun them if needed.

On the national front, all our critical, financial as well as citizen-related information are available and accessible through the Internet. It is an important role of the Government to protect these information infrastructures against attacks by adversaries who may range from script-kiddies to state actors. Internet has also been off-late used for terror related anti-national activities. Protecting our cyber networks from being used against the nation is also one of the paramount duties of the Government.

The good side of the cyber expansion is that it also presents a great opportunity for the states and the country in terms of increased business case through new IT challenges. India has well chalked out plans for its cyber policies, awareness creation, IT and Information Infrastructure protection and the business growth both within India and globally.

Karnataka is a pioneer in IT and in using It for the delivery of citizen centric services and inter-government business. It also has the largest IT industry which must be concerned about its own cyber security and the possible business opportunities.

World over, state governments have been working on their own framework for cyber security, well aligned with the country’s plans in protecting the cyber space and give assurance to its citizens and business that the cyber space is indeed a very safe one. This is a great challenge given the fact that cyber is extremely fast changing world and newer forms of threats from script kiddies, to organized international criminals, to state actors emerge almost every day.

Realising the importance of cyber security, Karnataka Government- a visionary one as always had through the KJA commissioned this report. In this report the experts have given an over view of the Nations plans and actions in cyber security and state of such cyber preparedness elsewhere in the world. The Task Group has also come up with plans of action that call for leveraging on the nation’s plans and had recommended a few unique actions of relevance to Karnataka. Critically, this Vision Report recommends plans to help

...
for Karnataka to take responsibility for its own cybersecurity, especially with regards to essential infrastructure and governance. On the flip side – and as one of the fastest growth industries at national level – developing our own cybersecurity industry is also an opportunity for economic growth, job creation and education – ensuring Karnataka is well positioned for a future as a digitally advanced nation. Our aim is that this document provides an informative primer on the relevant issues facing Karnataka in relation to cybersecurity, to generate discussion and debate, and to raise awareness with regards to a fundamental building block of the technologically-dependent society which we have already become. As you will read in the following pages, cybersecurity is not optional. It must form part of the design of every product, of every database, of every electronic communication. And – through education, awareness and proactive change – we can all play a part in securing our future.

TG defined cyber security for the State, explained its risks and challenges in relation to the digital economy and its global connectivity and discussed how the risks could be managed effectively. Examples and case studies are used to expound on the risks and challenges of cyber security. Ideas and suggestions on appropriate cyber security policy, procedures and controls as well as cyber security analytics for predicting probability of cyber-attacks are also deliberated extensively in the report. Laws concerning cyber security and legal protection are clearly highlighted. An effective security architecture is also suggested at state level. This architecture is structured, coordinated and activity consisting of processes and tools that will work together to secure state resources and rely on the continuous flow of information. The security architecture driven by policy indicated how the architecture to be implemented and how they will be enforced which enables the architecture to guide the State so that decisions are aligned and consistent throughout the entire IT landscape. The architecture of the report is strategic and structured in a way to looked at both security aspects and privacy assessment. Efforts are made in the report to ensure tightened rules on handling of personal data not to deter the disclosure or flow of necessary information in the name of privacy protection.

I would like to express my thanks to all the members of TG-KCSV for their ideas and involvement, Prof. Sridhar the Member-Secretary of TG-KCSV for leading the consultation and drafting process. Mr. Gaurav Gupta, Principle Secretary, IT/BT Dept of GoK has given valuable inputs and suggestion without which the report would not have had any practical utility. Dr. Mukund K. Rao, Member Secretary KJA was always there with his extremely useful inputs. Dr. Jayashri took the brunt of the attack and was extremely meticulous in the conduct of the meetings and preparation of the minutes – her contributions to the TG are noteworthy of mention. The visionary son of India, Dr. K. Kasturirangan was highly supportive of this work, gave critical inputs and suggestions to improve the draft versions and in fact the originator of the idea of the preparation of a report on Cyber security for Karnataka. We, the committee members are grateful to all of them. They in fact enhanced the quality of the report and made us feel satisfied that the report has in fact come out to be of good quality and practical utility.

They also led the creation of the thought process that was enshrined in this report with their total commitment and passion.

Sincerely

[Signature]

N Balakrishnan
Co-Chairs of TG:

- Prof. N. Balakrishnan, Honorary Professor, IISc & Chair, Task Group
- Prof. S. Sadagopan, Member, KJA; Director, IIIT-B & Co-Chair, Task Group

Member-Secretary of TG:

- Prof. V. Sridhar, Professor of Education, IIIT-B & Member-Secretary of Task Group

Members of TG:

- Dr. Sanjay Bahl, Director General, Indian Computer Emergency Response Team (CERT-In) & Member, Task Group
- Principal Secretary, IT/BT Department, GoK & Member, Task Group
- Dr. Mukund Rao, Member-Secretary, KJA & Member, Task Group
- Mr. Sanjiv K. R., Chief Technical Officer, Wipro & Member, Task Group
- Mr. Preet Paramjit Singh, Delivery Lead - Special Projects & Cyber Resilience, Cyber Security Practice, Tata Consultancy Services Limited & Member, Task Group
- Prof. S. Raghunath, Professor of Strategy, Chair, Centre for Corporate Governance and Citizenship, IIM-B & Member, Task Group
- Dr. T. Ramakrishna, Professor of Law, NLSIU & Member, Task Group

Convenor of TG:

- Dr. Jayashri, Sr. Research Associate, KJA
ACKNOWLEDGEMENTS

In preparation of this Task Group report TG has taken tremendously help from the following and extremely grateful to:

- Shri. Gaurav Gupta, Principal Secretary to the Government, Department of IT/BT and ST, GoK
- Ms. Rama Vedashree, CEO, DSCI
- Prof. Kamakoti, Professor, IIT Madras
- Mr. Venkatesh Murthy, Deputy Director, Cyber Lab, DSCI
- Ms. Kumudha Rani, Scientist, CFS, Forensics Sciences Lab, Bengaluru
- Ms. Priya Madhavan. Director, Industry Development, DSCI
- Ms. Moneesha Shrivastav, Regional Lead-Karnataka, NASSCOM IT-ITeS Sector Skills Council
- Shri. I.L. Narasimha Rao, Director, CDAC-Hyderabad
- Shri. R.K. Srivastava, Advisor (Former), Department of IT/BT and ST, GoK
- Members of the Task Group on Karnataka Cybersecurity Vision
- KJA Secretariat for overall coordination
KARNATAKA CYBER SECURITY VISION 2025

CONTENTS

MESSAGE
FOREWORD
PREFACE
TASK GROUP – KARNATAKA CYBER SECURITY VISION
ACKNOWLEDGEMENTS

EXECUTIVE SUMMARY ................................................................................................................................. 1
Key Cyber Security Goals for the State of Karnataka ................................................................................ 1
Key Recommendations ............................................................................................................................. 2

1. INTRODUCTION ........................................................................................................................................ 3
1.1 Cyber Security Initiatives by the Government of India ................................................................................. 4
1.2 Cyber Security Framework for the State of Karnataka ................................................................................... 5

2. PILLAR – 1: Protection and Enforcement .................................................................................................. 7
2.1 Incidence Resilience and Crisis Management............................................................................................... 7
2.2 State Cyber Crime Cells and Forensic Labs ................................................................................................ 9
  2.2.1 Cyber Forensic Section at Bengaluru ................................................................................................. 9
2.3 Cyber Secure Critical Information Infrastructure ...................................................................................... 11
2.4 Cyber Security Administration .............................................................................................................. 13

3. PILLAR-2: COMPETENCY AND SKILL DEVELOPMENT ............................................................................ 15
3.1 Cyber Security Competency Development Initiatives of the Government of India .................................... 16
3.2 Promote “Security Aware Culture” for the Citizens and Society ................................................................. 18
  3.2.1. Cyber security awareness programme of CDAC Hyderabad ............................................................ 18
3.3 “Train the Trainer” approach for teaching cybersecurity in Educational Institutes .................................. 18
  3.3.1. Information security courses for students in colleges and universities ........................................... 19
  3.3.2. Initiatives of CDAC-H on cyber security awareness programmes for school students .................. 19
  3.3.3. Cyber security Qualification Packages developed by DSCI ............................................................ 20
3.4 Cyber Security Competency Development for Government, Enterprises and Small Businesses ............. 21
  3.4.1. Yuva Yuga Scheme ......................................................................................................................... 22
  3.4.2. Cybersecurity upskilling scheme for Women ................................................................................. 22
  3.4.3. Future of Skills programme of NASSCOM ...................................................................................... 23
  3.4.4. Certificate Programmes ............................................................................................................... 24
3.4.5. Training in Cybersecurity Governance ................................................................. 24
3.5. Vocational Education in Cyber Security ................................................................. 25
   3.5.1. Vocational Education and Training ................................................................. 25
3.6. Cyber Security Training for Law Enforcement Agencies (LEAs) ............................ 27
   3.6.1. Cyber Forensics Training Lab at Bengaluru ....................................................... 27
   3.6.2. Cyber Forensics Training for LEAs by Academic Institutions ......................... 28
3.7. Competency Development for State Legislatures and Policy Makers .................... 29
3.8. Estimation of skill requirement in Cyber Security in Karnataka ............................ 30

4. PILLAR-3: PRODUCT TESTING AND CERTIFICATION ....................................... 32
   4.1. India Common Criteria Certification Scheme (IC3S) ....................................... 32
      4.1.1. Common Criteria Evaluation and Certification ......................................... 33
   4.2. State Advisory Committee for Cyber Security Assurance (SAC-CSA) .............. 34

5. PILLAR-4: BUSINESS PROMOTION ........................................................................ 36
   5.2. Promotion of Local Security Industry ............................................................... 38
      5.2.1. Venture Capital activity in cyber security startups ...................................... 38
      5.2.2. Role of Start-up Accelerators ................................................................. 39
   5.3. Public Procurement and Make in India ............................................................ 40
   5.4. Developing indigenous Cyber Security Products ............................................. 41
      5.4.1. Use Case Clearing House ........................................................................ 42
   5.5. Effective Public-Private Partnerships ............................................................... 42

6. PILLAR-5: CYBER SECURITY: RESEARCH & DEVELOPMENT ............................ 44
   6.1. Karnataka Cyber Security – Centre of Excellence ........................................... 45
   6.2. Institutional Collaborations ............................................................................... 47

7. PILLAR-6: STATE POLICIES AND REGULATION .................................................. 48
   7.1. Cyber Security Council of Karnataka (CSC-K) .............................................. 48
   7.2. Cyber Security Legal and Policy Think Tank (CS-LPTT) .................................. 49

8. PILLAR-7: OUTREACH PROGRAMMES .................................................................. 50

9. INTERNATIONAL PRACTICES OF CYBER SECURITY GOVERNANCE .................. 52

10. METHODOLOGY ..................................................................................................... 54
    10.1 Secondary Data Sources .................................................................................. 54
    10.2 Inputs from Experts and Members of the Task Group ........................................ 54
10.3 Inputs from Other Key Stakeholders .............................................................................................. 54

11. KARNATAKA CYBER SECURITY VISION 2025: SUMMARY OF RECOMMENDATIONS AND KEY GOALS .................................................................................................................................................................... 57

11.1. Key Cyber Security Goals ............................................................................................................... 57

11.2. Key Performance Indicators and Targets ....................................................................................... 61

11.3. Proposed Government Budget ...................................................................................................... 64

References .................................................................................................................................................. 67

Appendix-1. The Oversee and Governance Job Categories ................................................................. 69

Appendix-2. Cyber Security Governance Principles for Corporate Directors .................................... 70

Appendix-3. Model Cybersecurity training curriculum ........................................................................... 71

Appendix-4. India based Cyber Security Start-ups and associated Funding ........................................ 72

Appendix-5. Current and Expected outcomes of CS-CoE .................................................................... 73

Appendix-6. GO on Karnataka Jnana Aayoga ......................................................................................... 74
LIST OF FIGURES

FIGURE 1. EXISTING CYBER SECURITY INITIATIVES IN INDIA 5
FIGURE 2. KARNATAKA CYBER SECURITY FRAMEWORK (KCSF) 6
FIGURE 3. KCSF PILLAR 1: PROTECTION AND ENFORCEMENT 7
FIGURE 4. SECTORAL ADOPTION OF CYBER SECURITY 13
FIGURE 5. THE WORKFORCE CATEGORIZATION FOR “CYBERSECURITY OVERSEE AND GOVERN” 14
FIGURE 6. KCSF PILLAR 2: CYBER SECURITY COMPETENCE DEVELOPMENT MODEL 16
FIGURE 7. CYBERSECURITY SKILL UPGRADE PROGRAMMES 30
FIGURE 8. KCSF PILLAR 3: BUSINESS PROMOTION 38
FIGURE 9. KCSF PILLAR 4: FRAMEWORK FOR R&D IN CYBERSECURITY 45
FIGURE 10. CYBER SECURITY – CENTRE OF EXCELLENCE FRAMEWORK OF THE GOVERNMENT OF KARNATAKA 45
FIGURE 11. KCSF PILLAR 6: STATE CYBER LAWS AND REGULATION 48
FIGURE 12. KCSF PILLAR 7: OUTREACH PROGRAMMES 51
FIGURE 13. METHODOLOGY USED IN THE STUDY 54

LIST OF TABLES

KJA RECOMMENDATION 1
TABLE 1. CERTIFIED CYBER SECURITY PROFESSIONALS 31
TABLE 2. ESTIMATE OF CYBER SECURITY PROFESSIONALS REQUIRED IN THE STATE 31
TABLE 3. HIGHLIGHTS OF THE IT SECTOR IN KARNATAKA 37
TABLE 4. FUNDING DETAILS OF CYBER SECURITY START-UPS 39
TABLE 5. KARNATAKA STATE CYBER SECURITY 2025 KEY GOALS 53
TABLE 6. KARNATAKA STATE CYBER SECURITY 2025 KEY GOALS 57
TABLE 7. KEY PERFORMANCE INDICATORS AND TARGETS 61
TABLE 8. PROPOSED GOVERNMENT BUDGET FOR THE CYBER SECURITY PROGRAMME 64
### ABBREVIATIONS AND KEYWORDS

<table>
<thead>
<tr>
<th>Abbreviation/ Keyword</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>AI</td>
<td>Artificial Intelligence</td>
</tr>
<tr>
<td>CERT</td>
<td>Computer Emergency Response Team</td>
</tr>
<tr>
<td>CDAC</td>
<td>Centre for Development of Advanced Computing</td>
</tr>
<tr>
<td>CFS</td>
<td>Cyber Forensics Section, Forensics Services Lab</td>
</tr>
<tr>
<td>CID</td>
<td>Crime Investigation Department</td>
</tr>
<tr>
<td>CCRA</td>
<td>Common Criteria Recognition Arrangement</td>
</tr>
<tr>
<td>CCTL</td>
<td>Common Criteria Test Laboratory</td>
</tr>
<tr>
<td>CS-CoE</td>
<td>Cyber Security - Centre of Excellence</td>
</tr>
<tr>
<td>DAE</td>
<td>Department of Atomic Energy</td>
</tr>
<tr>
<td>DRDO</td>
<td>Defence Research and Development Organization</td>
</tr>
<tr>
<td>GoK</td>
<td>Government of Karnataka</td>
</tr>
<tr>
<td>GoI</td>
<td>Government of India</td>
</tr>
<tr>
<td>DSCI</td>
<td>Data Security Council of India</td>
</tr>
<tr>
<td>ICT</td>
<td>Information &amp; Communication Technologies</td>
</tr>
<tr>
<td>IC3S</td>
<td>India Common Criteria Certification Scheme</td>
</tr>
<tr>
<td>IIsc</td>
<td>Indian Institute of Science</td>
</tr>
<tr>
<td>IIT</td>
<td>Indian Institute of Technology</td>
</tr>
<tr>
<td>IIIT-B</td>
<td>International Institute of Information Technology Bangalore</td>
</tr>
<tr>
<td>IIMB</td>
<td>Indian Institute of Management Bangalore</td>
</tr>
<tr>
<td>IoT</td>
<td>Internet of Things that includes machine-to-machine communication</td>
</tr>
<tr>
<td>ISO</td>
<td>International Standards Organization</td>
</tr>
<tr>
<td>ISRO</td>
<td>Indian Space Research Organization</td>
</tr>
<tr>
<td>IT Act</td>
<td>Information Technology Act</td>
</tr>
<tr>
<td>IT-BT-ST</td>
<td>Information Technology – Bio Technology – Science &amp; Technology</td>
</tr>
<tr>
<td>IT / ITES</td>
<td>Information Technology / IT Enabled Services</td>
</tr>
<tr>
<td>KBITS</td>
<td>Karnataka Biotechnology and Information Technology Services</td>
</tr>
<tr>
<td>KCSF</td>
<td>Karnataka Cyber Security Framework</td>
</tr>
<tr>
<td>KJA</td>
<td>Karnataka Jnana Aayoga (Karnataka Knowledge Commission)</td>
</tr>
<tr>
<td>KSCST</td>
<td>Karnataka State Council for Science &amp; Technology</td>
</tr>
<tr>
<td>MeitY</td>
<td>Ministry of Electronics and Information Technology, GoI</td>
</tr>
<tr>
<td>ML</td>
<td>Machine Language</td>
</tr>
<tr>
<td>MSMEs</td>
<td>Medium, Small and Micro Enterprises</td>
</tr>
<tr>
<td>NIC</td>
<td>National Informatics Centre</td>
</tr>
<tr>
<td>NIELIT</td>
<td>National Institute of Electronics and Information Technology</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology, U.S.A.</td>
</tr>
<tr>
<td>NASSCOM</td>
<td>National Association for Software and Services Companies</td>
</tr>
<tr>
<td>PMA</td>
<td>Preferential Market Access</td>
</tr>
<tr>
<td>SDG</td>
<td>Sustainable Development Goals</td>
</tr>
<tr>
<td>SSC</td>
<td>Sector Skill Council</td>
</tr>
<tr>
<td>STQC</td>
<td>Standardization Testing and Quality Certification</td>
</tr>
</tbody>
</table>
EXECUTIVE SUMMARY

KARNATAKA CYBER SECURITY VISION STATEMENT

State of Karnataka to be a model state in the country in providing secure cyber infrastructure for the safe conduct of day-to-day public life, businesses and government services. State to be a technology and innovation hub for cyber security products and services. State to train and equip legislatures, government officials, law enforcement officials, businesses, students and citizens in creating a cyber secure culture for handling successfully any cyber-attacks and intrusions.

KEY CYBER SECURITY GOALS FOR THE STATE OF KARNATAKA

1. Making cyber security an essential part of citizen’s life and promoting cyber secure culture amongst all strata of the society. Educate and promote cyber security awareness at all sections of the society including legislatures, government officials, educators, private industry, society and public at large in partnership with academia and industry. (in tune with Sustainable Development Goal (SDG) 4 on “Quality Education” and SDG-17 “Partnerships to achieve the goal” ¹);

2. Detect, prevent, mitigate, and deter cyber security attacks and crimes by building an enabling infrastructure of incidence response centres, investigation labs, and certification processes through active Government/ Industry/ Academia collaborations (in tune with SDG-17 “Partnerships to achieve the goal” and SDG-16 “Peace and Justice string Institutions”);

3. Making the State as an innovation hub for all emerging cyber security technologies by creating Centers of Excellence and industry/ academia/ government partnerships (in tune with SDG-9 on “Industry, Innovation and Infrastructure” and SDG-17 “Partnerships to achieve the goal”);

4. To evolve the start-up entrepreneurial eco-system in the State to be the best in the country and a leading destination globally in the area of cyber security products and services. Create investor friendly State for nurturing businesses in the area of cyber security to create over one million jobs in the State (in tune with SDG-9 on “Industry, Innovation and Infrastructure” and SDG-8 on “Decent Work and Economic Growth”);

5. Cyber security to be realized as the key component across areas such as agriculture, Industrial, healthcare, rural and urban development, law and justice, transportation, financial and across other sectors of the economy with reasonable data protection and privacy adherence (in tune with SDG-11 on “Sustainable cities and communities”).

¹ United Nations Sustainable Development Goals (SDG). Available at: https://sustainabledevelopment.un.org/sdgs
KEY RECOMMENDATIONS

1. **Enforcement & Protection**: Create a cadre of police corps and forensic officers in the State and train them on intensive skills and practical knowledge in cyber security to be deployed at all the 30 cyber police stations in the State to protect and enforce cyber security in the State.

2. **Skill Development**: Leverage existing expertise and content available with premier Academic Institutions, CDAC centres, and DSCI to train and impart required cyber security skills to all strata of society and thus create a cyber security aware culture in the State.

3. **Product Testing & Certification**: To develop state of the art cyber security testing labs to conduct and certify cyber security products as per International Common Criteria Certification Scheme for global promotion and acceptance.

4. **Business Promotion**: Evolve the start-up entrepreneurial eco-system in the State to be the best in the country in the area of cyber security and promote business environment in the State to be a leading global destination for cyber security products and services.

5. **Research & Development**: Develop the State as an innovation hub for all emerging cyber security technologies by creating Centers of Excellence and strong academia-industry-government partnerships.

6. **State Policies & Regulation**: Constitute Cyber Security Council of Karnataka (CSC-K) to provide strategic advice on cyber security to the government and business communities. Enact cyber laws and regulation as per State’s specific requirements to complement existing national cyber laws for the welfare of the residents of the State.

7. **Outreach Programmes**: Engage with all stakeholders, in particular, the public and students, on a continuing basis through well-orchestrated cyber security outreach programmes and technical events.
1. INTRODUCTION

Presently India has the second largest Internet users, second largest mobile subscribers and second largest broadband subscribers in the world, next only to China. The Government of India initiated a number of digital technology enabled programmes such as Aadhaar, MyGov, Government e-Market, DigiLocker, Bharat Net, Start-up India, Skill India and Smart Cities. India is the third largest hub for technology driven start-ups in the world. Thus, there is a huge domestic demand for digitized services in the country.

Increased digitization has also led to more sophisticated cyber threats. The cyber threat landscape is dynamic and evolving with innovative technologies and attackers. Cyberspace is also increasingly subject to criminal and terrorist activities. The Computer Emergency Response Team India (CERT-In) has reported an increasing trend of cyber incidents. As per the information reported to and tracked by CERT-In a total of 185,100 cyber security incidents were observed during the year 2018 till November. India is ranked 23 out of 165 nations in the Second Global Cyber Security Index, released by the International Telecommunications Union in July 2017.

Over a period, the nature and pattern of incidents are becoming more sophisticated and complex. The attacks and intrusions targeted previously at only enterprises have started affecting common citizens and society at large. Humans are the vulnerable targets for today’s cyber-attacks. It is in this context, that this Vision document takes a systemic approach to protecting the State, the business and its citizens from cyber-attacks, intrusions and cybercrime.

As per the recent IBM study, India ranks higher on average number of breached records (34,110 compared to 31,465 in the U.S.)\(^2\). Though the per capita cost of data breach in India is much lower at $68 compared to that of the U.S. at $233, data shows the vulnerability of the country’s information assets.

Cyber risks pose a serious threat to governments, economies, businesses and individuals. Irrespective of investments made by businesses and government to improve cybersecurity of digital systems, the frequency of attacks and risks are increasing. With the rise in global cybercrime, there is need for effective preventive measures. There is still an evident gap between countries in term of awareness, understanding, knowledge and finally capacity to deploy appropriate cyber strategies, capabilities and programmes to ensure a safe and appropriate use of ICTs as enablers for economic development. As we move towards digitization, the number and type of devices requiring enhanced security measures increase too. Mobiles, tablets, wearables and Internet of Things enabled devices require varied and innovative approaches to cyber secure compared to the traditional approach of network security. Additionally, new technologies such as AI and ML are providing attackers with enhanced tools for more complex cyberattacks.

In this report, we provide a comprehensive policy framework for addressing all aspects of cyber security that have importance for individual States of the country, except *cyber warfare* which is a national subject.

### 1.1 Cyber Security Initiatives by the Government of India


The initiatives taken by the Government have focused on the issues such as cyber security threat perceptions, threats to critical information infrastructure and national Security, protection of critical information infrastructure, adoption of relevant security technologies, enabling legal processes, mechanisms for security compliance and enforcement, Information Security awareness, training and research. These actions are being continued, refined and strengthened to address the dynamic nature of cyber threat scenario.

With the different kinds of Cyber Attacks and Threats experienced by the Industry and Government alike, in last five years, there has been a significant focus on this segment. The domestic consumption and adoption of Cyber Security in different industry sectors is steadily increasing, the early adopters are – Banking and Finance, Manufacturing, Health Care & Insurance segment. However, the Govt. policy is seen as the major enablers for the Indian industry in this segment, such as the soon to be enacted Data Protection Bill 2018. Following Figure gives the existing cyber security initiatives in India.
The National Cyber Security Policy for India was released by Ministry of Communication and Information Technology in the year 2013 with a vision to build a secure and resilient cyberspace for citizens, businesses and Government. The mission of the Policy is to protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology and cooperation.

### 1.2 Cyber Security Framework for the State of Karnataka

Karnataka has been the pioneer in many areas of information technology such as the first one in the country to draft the innovation policy. Continuing on this tradition, it sets itself for a Cyber Security Vision that provides a systemic framework that covers all aspects. Towards this effort, the Karnataka Cyber Security Framework (KCSF) has been developed as indicated in the following Figure across Seven pillars namely:

1. Protection and Enforcement
2. Competency and Skill Development
3. Product Testing and Certification

---

4) Business Promotion  
5) Research and Development  
6) State Policy and Regulation  
7) Outreach Programmes

Rest of the document is organized across these seven pillars of the framework.

The above framework provides a systemic framework to detect, prevent and mitigate cyber security risks at all levels of government, private enterprises, and public. The framework is more comprehensive compared to even the National Cyber Strategy 2018 of the United States.⁴

---

2. PILLAR – 1: Protection and Enforcement

OBJECTIVE:

Detect, prevent, mitigate, and deter cyber security attacks and crimes by building an enabling infrastructure of incidence response centres, investigation labs, and certification processes through active Government/Industry/Academia collaborations

Government and business entities across the country have faced cybersecurity challenges in effectively identifying, protecting, and ensuring resilience of their networks, systems, functions, and data as well as detecting, responding to, and recovering from incidents. Hence protecting the information assets of individuals, society, businesses and government and responding to incidents in a timely manner to mitigate risks forms Pillar-1 of the KCSF. Further, there shall be enabling infrastructure to detect and analyze cyber security incidence through cyber forensics and to deter and if required punish cyber criminals from indulging further in malicious activities through appropriate enforcement of cyber laws and regulation is also considered as part of this pillar.

The different aspects of this pillar on protection and enforcement are given in the following Figure.

2.1. Incidence Resilience and Crisis Management

The Indian Computer Emergency Response Team (CERT-In), Ministry of Electronics and Information Technology, Government of India, has been designated under Section 70B of the Information Technology (Amendment) Act, 2008 to serve as the national agency to perform the following functions in the area of cyber security:

- Collection, analysis and dissemination of information on cyber incidents
- Forecast and alerts of cyber security incidents
- Emergency measures for handling cyber security incidents
• Coordination of cyber incident response activities
• Issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents
• Such other functions relating to cyber security as may be prescribed.

CERT-In creates awareness on security issues through dissemination of information on its website (http://www.cert-in.org.in) and operates 24x7 incidence response Help Desk. CERT-In provides Incident Prevention and Response services as well as Security Quality Management Services.

As part of Cyber Security Assurance, under Security Assurance Framework, CERT-In has empaneled 69 auditors to carry out information security audit, including the vulnerability assessment and penetration test of the networked infrastructure of government and critical sector organizations. Government and critical sector organizations are implementing the security best practices in accordance with ISO 27001 standard and as per the advice issued by CERT-In. Services of CERT-In empaneled IT security auditors are being used to verify compliance.

Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre http://www.cyberswachhtakendra.gov.in) has been launched by CERT-In on February 21, 2017 for detection of compromised systems in India and to notify, enable cleaning and securing systems of end users to prevent further malware infections. The centre is working in close coordination and collaboration with Internet Service Providers, Academia and Industry. The centre is providing detection of malicious programs and free tools to remove the same for common users.

CERT-In has set up phase 1 of National Cyber Coordination Centre (NCCC) to generate necessary situational scenario of existing and potential cyber security threats and enable timely information sharing for proactive, preventive and protective actions by individual entities. A Cyber Crisis Management Plan (CCMP) for countering cyber-attacks and cyber terrorism for implementation by all Ministries/Departments of Central Government, State Governments/UTs and their organizational units in critical sectors has been formulated. In addition, several guideline documents and templates have been published to assist development and implementation of sectoral Cyber Crisis Management Plans. CCMP for countering Cyber-Attacks and Cyber Terrorism is updated periodically to take into account changing scenario of cyber threat landscape. Cyber Security Mock Drills are being conducted by CERT-In to help the organisations to assess their preparedness to withstand cyber-attacks. These drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors.
RECOMMENDATION

It is proposed to set up Karnataka’s Computer Emergency Response Team (K-CERT) along similar lines that of CERT-In as part of the Centre of Excellence – Cyber Security (CoE-CS) that has been set by the GoK. If and when set up K-CERT shall coordinate with CERT-In to provide forecasts and alerts on cyber security incidence, release timely vulnerability disclosures, and assist in emergency measure for handling cyber incidents. K-CERT shall also partner with government, industry, law enforcement, and academia to improve the security and resilience of computer systems and networks in the State.

2.2. State Cyber Crime Cells and Forensic Labs

The State on its part has created Cyber Crime Police Station Corps of Detective Headquarters in Bengaluru, one of its kind in the country, for addressing cybercrimes in the State that falls under the “IT Act 2000”. This police station under the leadership of Director General of Police, Criminal Investigation Department Economic Offenses and Special Units has been functioning since 2001. This is well ahead of time and before the circular on cyber-crime prevention was sent by the Ministry of Home Affairs, GoI (GOI, 2018), requesting all the state administrations to set up cybercrime cells.

Currently, there is one Cyber Crime Police Station at each of the 30-district headquarters in the State. It is noted that at least four cases of cybercrime are reported every day in Karnataka — and three of them are from Bengaluru alone. However, there are crimes reported from different districts as well. Hence, need of the hour is to build capabilities to handle cybercrime investigations across all the Cyber Crime Police Stations in the State.

Further, the Investigating Officers and associated police corps of the cyber police stations often are transferred to other non-cybersecurity related activities thus leading to shortage of expertise in cybersecurity IOs.

2.2.1. Cyber Forensic Section at Bengaluru

In March 2015, Cyber Forensic Section (CFS) has been commissioned as part of the Forensic Science Laboratory (FSL) in Bengaluru. The City police who used services of FSL-Hyderabad and Delhi, are now able to get the samples tested on cybercrimes such as identity theft, software piracy and network intrusion at CFS. Experts in CFS have been trained at CDAC-Trivandrum. Salient features of the CFS are given below:

---

5 [https://timesofindia.indiatimes.com/city/bengaluru/4-cybercrimes-reported-every-day-in-karnataka-3-of-them-in-bengaluru/articleshow/59133563.cms](https://timesofindia.indiatimes.com/city/bengaluru/4-cybercrimes-reported-every-day-in-karnataka-3-of-them-in-bengaluru/articleshow/59133563.cms)
The lab handles cyber forensic cases reported by the Investigation Officers (IOs) of the State Police with about 60% of the cases filed under IT Act 2000 and rest under IPC;

The Lab has been certified by MeitY as the "Examiner of electronic evidence" under section 79A of IT Act whose cyber forensic analysis shall be accepted in the court of law in the country;

The lab is also ISO 17025 certified enabling the test reports and certificates of the lab to be accepted across countries without the need for further testing, thus enabling cross border cybercrime investigations;

The lab has state of the art "dead" article analysis tools (both hardware and software) including disk, mobile, audio and video; the lab does not have adequate infrastructure to provide live analysis of articles and events including network forensics;

The lab also has been using some of the indigenous tools created by the cyber forensics division of CDAC-Trivandrum; however, they are limited due to lack of support and upgrades.

The lab has well qualified forensic experts; however, there are not enough number of scientists given the workload; the time duration for analysis and reporting of an incident takes 3-7 days;

There is almost 100% success rate of the lab's forensic analysis being accepted in the court of law;

The lab has also been training IOs, and police corps on article collections using standard operating procedures at the crime scene; despite these efforts, the quality of articles remain poor for conducting a good analysis;

The lab has also been training judiciary through Karnataka Judicial Academy; however, more capability and skill development is required;

The lab also is the only nodal forensic analysis lab for all cyber police stations in the State;

---


7 Cyber forensics research at CDAC Trivandrum. Available at: http://www.cyberforensics.in/AboutCdacMore.aspx accessed on 30 Oct 2018
RECOMMENDATION

Due to increase in cybercrime and incidences, it is imperative for the State Police to develop deep expertise in cybercrime investigation and forensics. Hence it is recommended that the State Police develop a cadre for cybercrime so that all cyber police stations in the State be equipped with qualified IOs.

Further, the CFS at Bengaluru provides forensic analysis and support to all cybercrime incidences across the State. It is recommended that a unit comprising of the requisite scientists, administrators and associated infrastructure be set up at each of the 30 cyber police stations with Bengaluru CFS providing expert guidance and support. The cadre of administrators and scientists at CFS be re-examined to provide growth opportunities for this very important section of the State Police.

It is also recommended that the State forensic labs are equipped with network forensic tools apart from disk and mobile forensic tools to enable timely detection and prevention of live cyber-attacks.

2.3. Cyber Secure Critical Information Infrastructure

National Informatics Centre (NIC) is providing network backbone and e-Governance support to Central Government, State Governments, UT Administrations, Districts and other Government bodies. It offers a wide range of ICT services including Nationwide Communication Network for de-centralised planning, improvement in Government services and wider transparency of national and local Governments. NIC has set up a country wide network NICNET which brings about connectivity and thus satisfying information carrying requirements of the Government offices geographically dispersed right down to the grass root levels. NICNET has about 1400 nodes spanning the state centres, district centres and the national capital. Cyber Security Group of NIC is dedicated to formulate security policies and procedures for protecting the information assets on NICNET. The NIC is operating a security monitoring centre for detecting and responding to security incidents.

National Critical Information Infrastructure Protection Centre (“NCIIPC”) is an organisation under the administrative control of National Technical Research Organisation (“NTRO”) and is designated as the National Nodal Agency in respect of Critical Information Infrastructure Protection (“CIIP”). NCIIPC was
constituted vide a Gazette Notification on 16th January 2014 issued under the Section 70A of the Information Technology Act, 2008.

Key responsibilities of NCIIPC are summarized as follows:

- Deliver advice to reduce vulnerabilities.
- Identify all Critical Information Infrastructure (CII) elements for notification.
- Provide strategic leadership and coherent Government response.
- Coordinate, share, monitor, collect, analyse and forecast threats.
- Develop plans, adopt standards, share best practices and refine procurement processes.
- Evolve protection strategies, policies, vulnerability assessment and auditing methodologies and plans for CII.
- Undertake R&D to create, collaborate and develop technologies for growth of CII protection.
- Develop training programs for CII protection.
- Develop cooperation strategies.
- Issue guidelines, advisories etc. in coordination with CERT-In and other organisations.
- Exchange knowledge and experiences with CERT-In and other organisations.

State’s economic prosperity and well-being of its citizens depend on critical information infrastructure across sectors such as Transportation, Telecommunications and the Internet, Banking and Finance, Law and Justice; and that of public sector organizations in the areas of space, energy and utility; and e-government services. The State is developing 6 Smart Cities: Belagavi, Davanagere, Hubli-Dharwad, Mangaluru, Shivamogga and Tumakuru. These cities when fully developed under this initiative will have “smartness” introduced in all aspects of urban life through ICT. The protection of ICT infrastructure is very much required for the proper functioning of the urban life in these cities.

RECOMMENDATION

The setting up Security Operations Compliance (SOC) infrastructure comes under the purview of the e-Governance department of the State. It is recommended that, as part of its responsibility, the e-Governance department shall conduct security auditing of its Critical Information Infrastructure periodically to ensure all vulnerabilities in software and systems used are effectively patched and exposures to cyber-attacks are minimized. The department shall coordinate with NCIIPC to protect the State’s information assets and infrastructure accordingly.

---

2.4. Cyber Security Administration

Cyber security protection, enforcement and governance requires workforce skilled in cyber security. Cyber Security is not just related to a particular sector such as the IT sector. Since digitization spans across industries, it is very important to adopt best of the security practices in all sectors that use ICT intensely. An example of different sectors and the areas in which Cyber Security needs to be implemented and enforced are given in the following Figure. Apart from government services in each sector, private enterprise that provide services also need to be compliant with Cyber Security standards and processes.

Ministry of Electronics and Information Technology (MeitY) has issued direction to all State/UT Governments and all Central Government Ministries/Departments & Critical Sector Organizations to appoint Chief Information Security Officer (CISO). MeitY 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\textsuperscript{10}.

\textsuperscript{10} Key Roles and Responsibilities of Chief Information Security Officers (CISOs) in Ministries/Departments and Organisations managing ICT operations. Available at: \url{http://meity.gov.in/writereaddata/files/CISO_Roles_Responsibilities.pdf} accessed on 14 Sep 2018.
The National Institute of Standards and Technology (NIST) in the United States has created a very comprehensive Cybersecurity workforce framework as given below\textsuperscript{11}. The descriptions of the workforce category is given in Appendix-1 for reference.

![Figure 5. The workforce categorization for “cybersecurity oversee and govern”](image)

**RECOMMENDATION**

The CISO alone is not sufficient for a comprehensive cyber security administration. It is recommended that the State Government creates a separate cadre of technical and administrative officers in the area of “Oversee and Govern” category of workforce as indicated in the NIST framework for appropriate implementation, maintenance and control of cyber security infrastructure and services as per the framework given below. Similarly, it is recommended that in the State police corps, a separate cadre for cybercrime is created to equip the 30 cyber police stations with experts in cyber forensics and investigation.

---

3. **PILLAR-2: COMPETENCY AND SKILL DEVELOPMENT**

The need for a framework for Cyber Security competency development has been proposed in many reports (NASSCOM-DSCI, 2012). Appropriate competencies are required at all levels (viz. State, Industry, Society and Individuals) to handle cyber security threats and intrusions. Hence Pillar-2 in our model addresses competency and skill development in the area of cyber security.

Creating a security consciousness and cybersecurity aware culture demands individuals and organisations to treat security from a different perspective taking cognizance of the nuances involved. Organizations, both public and private, need to change their cultures to truly make security awareness part of their daily activities. Understanding the human element of cybersecurity and the way ICT users adopt the Dos and Don'ts are important for promoting a cyber security culture.

**OBJECTIVE:**

*Making cyber security an essential part of citizen’s life and promoting cyber secure culture amongst all strata of the society. Educate and promote cyber security awareness at all sections of the society including legislatures, government officials, educators, private industry, society and public at large in partnership with academia and industry.*

We propose the following framework for cyber security competence development across six areas to cover the entire gamut of stakeholders.
3.1. Cyber Security Competency Development Initiatives of the Government of India

Ministry of Electronics and Information Technology (MeitY) is implementing the Information Security Education and Awareness (ISEA) Project which aims to generate 1.14 lakhs qualified professionals at various levels in period of 5 years. A total of 51 institutions in various categories across the country are participating in the project. CDAC Hyderabad is the nodal agency for creating the awareness and training material and conducting different types of training programmes. The pioneering work done by CDAC Hyderabad is available at: [https://infosecawareness.in/home/index.php](https://infosecawareness.in/home/index.php). Besides, National Institute of...
Electronics and Information Technology (NIELIT) is conducting certification courses for creation of cyber security professionals.

As part of awareness creation, MeitY has engaged with DSCI for creating Cyber Crime Awareness for Law Enforcement agencies and workshops are being organized in different cities to train police corps. National Law School of India University, Bangalore and National Academy of Legal Studies and Research (NALSAR), University of Law, Hyderabad are also engaged in conducting awareness and training programmes on Cyber Laws and cybercrime investigation for judicial officers.

As part of security awareness, skill development and training, CERT-In regularly conducts trainings / workshops to train officials of Government, critical sector, public/industry sectors, financial & banking sector and ISPs on various contemporary and focused topics of Cyber Security. CERT-In conducts regular training programme to make the network and system administrators aware about securing the IT infrastructure and mitigating cyber-attacks. CERT-In has published guidelines for securing IT infrastructure, which are available on its website (www.certin.org.in).

Mass cyber security awareness project has been implemented in North-Eastern states of Manipur, Nagaland, Tripura, Mizoram and Sikkim targeting creating awareness among youth and public including School / College students.

Strategic cyber security cooperation by CERT-In with the other countries enables creation of a security ring of like-minded and ICT dependent nations around the world that can help safety and security of cyber space. Accordingly, CERT-In enters into international cyber security cooperation arrangements with organizations engaged in similar activities, in the form of Memorandum of Understanding (MoU), to enhance its operational readiness.

The Ministry of Electronics and Information Technology (MeitY), has launched the Cyber Surakshit Bharat initiative in association with National e-Governance Division (NeGD) and industry partners. The purpose of the program is to spread awareness, build capacity as well as enable government departments on steps that need to be taken to create a Cyber Resilient IT setup. This program helps educate and enable the Chief Information Security Officers (CISO) and broader IT community to address the challenges of cyber security. The programme was launched on 19 Jan 2018. The training will be conducted in 5 to 6 cities over a period of one year so as to train and enable around 1200 officials working in Central/State Governments, Banks and PSU.
3.2. Promote “Security Aware Culture” for the Citizens and Society

Today, Karnataka boasts of high mobile density (110.38% total and 58.30% rural) and Internet penetration (44.32% total and 17.27% rural) and broadband penetration as percentage of Internet subscriptions (80% total and 63% rural). These penetration levels, on one hand improve economic well-being of the society as many researchers have pointed out, but also increase vulnerability of the State population at large against cybercrimes and attacks.

Hence, a “cyber security aware” society needs to be developed which is capable of cyber security incidence handling and recover from cybercrimes and attacks in a timely manner.

3.2.1. Cyber security awareness programme of CDAC Hyderabad

Every citizen is vulnerable to cyberattacks. In the U.S., Lock Down your Login programme (https://www.lockdownyourlogin.org/) has been created by Google for promoting public awareness of dos and don'ts in the context of cyber security. Along similar lines, CDAC Hyderabad (CDAC-H) has done extensive work on developing content in various formats including posters, videos, images, newsletters (available at: https://infosecawareness.in/) in English and Hindi and select regional languages for educating public at large including school children. Being a nodal agency for ISEA, CDAC-H has also trained the teachers at various schools and colleges on Cyber Security with material created under the ISEA program. The content available in various multimedia formats are available in ready-to-use formats. One of the major challenges is in translating the training material so developed in English in regional languages. Though some have been translated, lack of translators with technical knowledge is a problem.

**RECOMMENDATION**

It is recommended that resources available at CDAC-H be leveraged by the State to prepare cyber security awareness campaign in various formats (e.g. posters, videos, newsletters, and other artefacts) in Kannada. Further, it is recommended that the State shall review the cyber security syllabus and the associated books to be published by NCERT to assess whether these shall be included in the State board curriculum as well at appropriate classes both in Kannada and English.

3.3. “Train the Trainer” approach for teaching cybersecurity in Educational Institutes

Though most of the technical institutes in the state have some courses in cyber security, the competency of teachers in the evolving field is not commensurate with the rapid developments in the field. Hence there is a need to train both the faculty and students of various technical institutes in the State so that
the required manpower need in the industry and government can be met. We recommend “train the trainer” approach for competency development so that the training programmes can be scaled up and meet the growing needs huge needs of the educational Institutes in the State. The initial sets of faculty at various engineering colleges in the State can be trained by reputed Institutes such as IISc, IITs and IIITs in the State. These faculty then in turn can conduct training programmes with part financial assistance from the State for teaching other faculty members so that it can have a cascading effect.

Initiatives of this type are already in place as given below and the resources and content shall be leveraged in a collaborative mode to scale up cybersecurity competency at the Institutes across the State.

3.3.1. Information security courses for students in colleges and universities

The IIT-Madras has developed and has been offering introductory and advanced courses through NPTEL MOOC platform, details of which are available at: https://nptel.ac.in/courses/. These are a set of 4 courses in Information Security. These are specifically intended for students who want to explore the field of information security, and students who currently are undergoing a course in information security. Some courses can also be taken by IT professionals who wish to explore the nuances of information security, security professionals who want to revisit the fundamentals, top management and senior management of corporate companies who wish to learn the concept of information security and implement them in their companies, professionals from BFSI segment who wish to understand the depth and average of information security and of course anyone with an aptitude to learn\(^{12}\). These courses apart from covering fundamentals on information security also have hands-on components where the candidates can use various open source tools to understand the concepts using a “hands-on” approach. The Indian Institute of Science has been offering a number of courses offered by the Security Research Group\(^{13}\).

3.3.2. Initiatives of CDAC-H on cyber security awareness programmes for school students

In an innovative effort, CDAC-H has created a text book on Cyber Security, the syllabus of which has been accepted by NCERT and will be printed soon. The book can then be included in CBSE curriculum in the appropriate primary and secondary classes. CDAC-H also has been conducting training programmes for school teachers as well. These programmes can be used to spread cybersecurity awareness at schools.

---

\(^{12}\) Introduction to Information Security course available at: https://nptel.ac.in/courses/106106129/1 accessed on 29 Oct 2018.

\(^{13}\) Cybersecurity courses offered at IISc are available at: https://securityresearch.iisc.ac.in/courses.html accessed on 30 Oct 2018.
3.3.3. Cyber security Qualification Packages developed by DSCI

DSCI, in collaboration with IT/ITeS Sector Skills Council of NASSCOM, has been working towards building a robust Cyber Security skills ecosystem in the country. A joint endeavour is being executed under the aegis of National Skills Development Corporation (NSDC), Ministry of Skills & Entrepreneurship Development, and GoI. Under this program, DSCI has developed cybersecurity training Qualification Packages (QPs) covering the following aspects:

- Analyst: Application Security
- Analyst: Compliance Audit
- Analyst: End Point Security
- Analyst: Identity and Access Management
- Analyst: Security Operations Centre
- Architect: Identity and Access Management
- Consultant: Network Security
- Forensic Specialist
- Penetration Tester
- Security Infrastructure specialist
- Security Analyst

These courses are available online. NASSCOM SSC has also been offering in-class training programs through its industry partners and academic institution partners. The content and assessments are as per National Skills Qualification Framework (NSQF) of the Ministry of Skill Development Entrepreneurship of GoI covering skills levels 6-10. Post the assessment of the skills and knowledge learned through the above packages, the candidates participating in these programmes receive certificates from NASSCOM SSC. Though some of the Tier-1 institutes have been offering these courses to their students and teachers, it is a challenge to induct tier-2 and 3 type institutes in to this programme. Some of these packages are also being used in the Pradhan Mantri Kaushal Vikas Yojana (PMKVY) as part of the skill development program of GoI, administered through NASSCOM SSC.

---

RECOMMENDATION

It is recommended that cyber security course resources available NPTEL offered by Institutes such as IISc and IIT-M shall be leveraged to educate the students and faculty at Institutes and colleges. Hub-and-spoke - “Train the trainer” model is recommended for scaling up the cybersecurity training programmes, with premier institutes in the State including IISc, IITs and IIITs being at the hubs in the cog, to reach out to the faculty in tier-2 and 3 institutes in the State. It is recommended that the State shall actively review the cybersecurity text books available at CDAC-H/ NCERT developed under the ISEA programme of MeitY for incorporating in the State Board curriculum both in English and Kannada mediums to improve information and cyber security awareness amongst secondary school children in the State.

3.4. Cyber Security Competency Development for Government, Enterprises and Small Businesses

The cyber security competency requirements within the enterprises can be largely grouped at three levels, namely cyber security operations, management and governance. Across industries, the IT and ITES industry have been relatively well prepared in developing cyber security operations and management competency in their organizations. The requisite competency for operations and management are being addressed through organic development within the enterprise. However, organizations still struggle to keep pace with increasing complexity and nature of cyber-attacks. As much as they would like to keep it within their internal teams and captives, the complexity and speed element will force them to have trusted partners in their efforts to counter cyber threats.

IT/ITES companies are also governed by local obligations that stem from the IT Act 2000 (amended 2008) and also by virtue of contractual obligations to laws in the jurisdictions of their customers. Such obligations place increased responsibilities on IT/ITES companies for securing their IT infrastructure. Some of the practices followed by IT/ITES companies would include:

- Well defined CISO organizations
- ISO 27001 Certification
- SSAE 18 reporting
- Data Privacy Compliance
- Transparent External / Customer audits
- Clearly defined Incident Response and breach notification processes
- Awareness Training (For Data Privacy, Infosec etc.) for the internal users
Though IT departments in firms in other industries are also relatively well equipped with minor security threats and intrusions, their technical and managerial employees need to be continuously educated and given practical exposure to emerging new areas in cyber security. Though private sector has been adept in training its officials in cyber security due to their business imperatives, public sector and government department lags behind. Hence, there is a need to educate and train the IT staff and managers of Public Sector Enterprises, Public Sector Banks and government officials on cyber security fundamentals, cyber security preparedness, incidence response and management. The need for appropriate training of IT departments in SMEs on cyber security is also the need of the hour.

As most of the government services are digitized the vulnerability of such digital systems are ever increasing. It is important for all state officials in-charge of various e-government services to be aware about security precautions and proactive measures. Critical infrastructure that provide public utilities such as electricity, water and sanitation are also being exposed to cybercrimes. Hence it is of utmost important to train officials in utility providing organizations on the impact of cyber security as appropriate to their services.

3.4.1. Yuva Yuga Scheme

This scheme was instituted by the Government of Karnataka in 2017 as a skill upgradation programme targeted at the youth of Karnataka. The scheme also allocates 30% of the seats to women candidates. Out of the five programmes listed under this scheme, NASSCOM IT-ITES SSC has been providing the training for IT and ITES. Some aspects of cyber security are covered under by NASSCOM through accredited partners. Examples of cybersecurity modules in this program include the following:

- Analyst: Application Security
- Analyst: Security operations Centre
- Forensic Specialist
- Ethical Hacker Foundation & Security Analysts Course

The above courses are part of the NASSCOM SSC Cyber Security Skills QPs as given in section 3.4.3. The State has selected thousands of candidates to be trained by NASSCOM SSC using its accredited partner network, funding for which is provided by the State under the skill development programme.

3.4.2. Cybersecurity upskilling scheme for Women

It is observed that there is lack of activities to continue the IT employment for women, who have returned to duty after completion of maternity leave or study leave. This Prerarna scheme is to assist women to upgrade their skills, especially in the area of Cyber Security. So the mandate is not just to re-skill them but to ensure that they get back to work. So, the workforce is the only measure of success. Along the same lines, NASSCOM also has initiated Women Wizard Rule Tech (W2RT) program to specifically train women
professionals in the IT ITES sector on core technologies, including cyber security. Underlining the need to bolster the cybersecurity ecosystem in the country, Microsoft India and the Data Security Council of India (DSCI) have launched the *Cyber Shikshaa*, a 3-year program to create a robust pool of skilled women professionals in the country\(^\text{16}\). Supported by the Ministry of Information Technology (MeitY)’s Information Security Education & Awareness (ISEA), Cyber Shikshaa recognizes the growing potential of cybersecurity as a sunrise segment and the need for a large base of diverse industry ready talent.

### 3.4.3. Future of Skills programme of NASSCOM

NASSCOM has created a platform referred to as “Future Skills” (http://futureskills.nasscom.in/) for upskilling the IT ITES workforce in the industry. The Futureskills portal is a marketplace and content library, wherein training packages in emerging and deep technologies including cybersecurity are made available by a consortium of expert content providers targeted at professionals in the IT ITES industry to upgrade their skills and knowledge in these emerging areas. This also provides a continuous education programme for working professionals to constantly upgrade their capabilities. This platform is along the lines of the training platform on Cyber Security, made available by the Software Engineering Institute at the Carnegie Mellon University, U.S., referred to as “CERT STEPfwd (Simulation, Training, and Exercise Platform)” (available at: https://stepfwd.cert.org/lms). The Futureskills platform is available currently for NASSCOM members, it is also envisioned to be available for academic institutes as well.

DSCI in association with MeitY and Google India have crafted an awareness campaign to promote 'Digital Payment Suraksha' to address the need to educate end users and merchants on security and safety best practices while making digital transactions. 'Digital Payment Suraksha' Campaign has the following mutually complementary two-pronged approach\(^\text{17}\):

- *'Digital Payment Security Awareness Campaign'* will engage communities including individuals (users), micro, and small and medium businesses, traders by making them aware of best practices and do's and don'ts on different payment channels including Debit and Credit Card, Online and Mobile Banking, Mobile Wallets, Unified Payment Interface (UPI) & BHIM, Aadhaar Enabled Payment Systems (AEPS), USSD Payments.
- *'Digital Payment Security Alliance'* facilitating the ecosystem to deliberate on a common agenda focusing on policy, deriving best practices from global success stories.


IIIT Bangalore has been offering certificate courses in information security courses through its industry partners for working executives\textsuperscript{18}.

### 3.4.4. Certificate Programmes

I. One of the objectives of the ISEA project is to implement a robust certification mechanism in Information Security with technical experience and guidance from premier institutes such as IITs and IISc, with National Institute of Electronics & Information Technology (NIELIT), Gorakhpur as the implementing organization. NIELIT has launched a National Level Certification Scheme in Information Security with the support of MeitY under which certification at the following three levels are offered:

1) Level 1: Certified System Security Analyst (CSSA)
2) Level 2: Certified System Security Professional (CSSP)

II. In the past, security was often left to managers and administrators at the technical and operational levels. However, as both technology and the nature of threats have increased in scale and complexity, the ultimate responsibility for protecting an organization’s mission and assets is now being been laid at the doorstep of senior management. An organisation’s board is responsible (and accountable to shareholders, regulators and customers) for the framework of standards, processes and activities that, together, secure the organisation against cyber risk. Corporate boards can create a culture of security to mitigate risk and better protect their company’s critical infrastructure, data systems and reputation.

The Centre For Corporate Governance and Citizenship, IIM Bangalore has been offering certification courses for Directors on Corporate Boards with a module on cyber security. A standalone certification course on Cyber Security and Risk Mitigation in Corporate Governance can be offered by The Centre For Corporate Governance and Citizenship, IIM-Bangalore.

### 3.4.5. Training in Cybersecurity Governance

In the past, security was often left to managers and administrators at the technical and operational levels. However, as both technology and the nature of threats have increased in scale and complexity, the ultimate responsibility for protecting an organization’s mission and assets is now being laid at the doorstep of senior management. An organisation’s board is responsible (and accountable to shareholders, regulators and customers) for the framework of standards, processes and activities that, together, secure the organisation against cyber risk. Corporate boards can create a culture of security to mitigate risk and better protect their company’s critical infrastructure, data systems and reputation. Appendix-2 provides

\textsuperscript{18} Details of the Certified Cyber Warrior programme offered by IIIT-B is available at: https://www.iiitb.ac.in/programs.php?pid=certified-cyber-warrior accessed on 30 Oct 2018.
the governance principles that are applicable for Cyber Security Risk management for enterprises, both for CXOs and Board of Directors. Based on these principles, curricula shall be developed for educating cyber security governance to enterprise management and directors. Workshops shall be conducted to sensitize the business leaders on the impact of cyber security to business governance and disclosure controls to build competency at the level of top management and directors of organizations. There are not many training programmes available in this area currently.

**RECOMMENDATION**

It is recommended that the State shall promote the Futureskills platform of NASSCOM, the cyber security QPs developed by DSCI, information security courses offered through NPTEL, Certification course offered by NIELIT, and Cyber Security certificate programmes for Directors of corporate boards offered by IIMB for enhancing the skill and knowledge levels of government officials associated with IT and IT services implementation, and State-owned Public-Sector Enterprises and financial institutes.

### 3.5. Vocational Education in Cyber Security

Cyber security is a technology intensive area and practical training is required to detect and resolve cyber security incidents. Hence the theory and classroom-based sessions will have to be augmented with technical hands-on training. Further the trained manpower needs to be certified by an accredited agency for employment purposes.

#### 3.5.1. Vocational Education and Training

Vocational Education and Training (VET), also called Career and Technical Education (CTE), prepares learners for jobs that are based in manual or practical activities, traditionally non-academic and closely related to a specific trade, occupation or vocation. It is sometimes referred to as Technical Education, as the learner directly develops expertise in a particular group of techniques or technology. As the labor market becomes more specialized and economies demand higher levels of skill such as in cyber security, governments and businesses are increasingly investing in the future of vocational education through publicly funded training organizations and subsidized apprenticeship or traineeship initiatives for businesses. Today VET as a model is well established internationally in Australia, Commonwealth of Independent States, European Union, Finland, Germany, Hong Kong, Hungary, India, Japan, South Korea, Mexico, The Netherlands, New Zealand, Norway, Paraguay, Russia, Sweden, Switzerland, Turkey, United Kingdom, and United States.

India is a pioneer in vocational training in Film & Television, and Information Technology. Today VET in India is provided through Government and Private Industrial Training Institutes (ITI) throughout the country. The total Number of ITIs in the country are 10,750, [Government - 2,275 & Private - 8,475] and
the mode of instruction is English, Hindi and all regional languages. There are 1,227 ITIs in India are under the Public Private Partnership model. Core Group Members which includes 20 members from Directorate General of Training (DGT) in Ministry of Skill Development and Entrepreneurship, and Champion ITIs are the Master Trainers and they in turn teach other instructors / teaching staff of all Government ITIs and private ITIs. This ensures a standardized delivery mechanism as well as standardized content which is further imparted to the students.

The possible current and future roles that may be required in jobs of craftsmen have been shortlisted as follows:

- a. Network security and IT infrastructure technician
- b. Desktop / Laptop / Tablet security technician (OS, network, firewall, Anti Malware)
- c. Modem security technician
- d. Mobile and internet technician
- e. Computer operator and / or Secretarial with appreciation of security and privacy
- f. Proficiency as Guard to monitor CCTV and access control with respect to security and privacy
- g. Car network security technician
- h. TV network security technician
- i. ATM network security technician
- j. Refrigerator and A/C network security technician

The ISEA project described in section 3.3 provides security awareness to individuals. However, it is envisioned that phase II of ISEA shall include capability building in the area of cyber security to cater to the demands of cyber security professionals in the country. In this context, a sub group on capacity building on cyber security proposed vocational training to be offered in cyber security through ITIs. The report suggests incorporating cyber security courses in the existing Modular Employee Skills (MES) and Craftsmen Training Scheme (CTS) schemes offered by the ITIs 19. The number of it is and their reach across the length and breadth of the country will offer scalability of the programmes.

Assessment of the candidates who take the above programmes will be done in designated Testing Centres by assessing bodies. The State /UT Governments shall provide necessary support to the assessing bodies in selecting the Testing Centres and conducting assessments. Successful candidates from these proposed programmes will be awarded certificates issued by National Council for Vocational Training (NCVT).

The State has more than 175 government ITIs and close to 1,500 private ones and has the largest number of seats in the southern region. The State shall leverage the scale and reach of the ITIs in providing vocational education in the area of cyber security, thus leading to gainful employment.

19 Details on vocational training programmes are available at http://dget.nic.in/content/innerpage/schemes-for-training.php accessed on 20 Nov 2018.
3.6. Cyber Security Training for Law Enforcement Agencies (LEAs)

Recognizing the specialized knowledge required for handling cybercrimes, it is the need of the hour for imparting appropriate training for police officers, public prosecutors as well as judiciary officers. Increasingly, devices are being discovered on crime scenes which must be dealt with quickly by frontline police Investigating Officers (IOs). When police arrive at a crime scene, speed is essential. Every second a computer, mobile or device is left unattended, data stored in its memory cache is irretrievably lost. IT systems must remain running to enable a first responder to collect the necessary volatile data and make initial assessments of running processes. Police also need the technical skills to respond to other forms of cybercrime, including hacking and possession or distribution of malicious software. Recognizing the needs of police officials in the field of cyber security, a Cyber and Hitech Crime Investigation and Training (CHCIT) Centre (http://www.cbiacademy.gov.in/chcit.php) was setup in and is functioning at CBI Academy, Ghaziabad since June, 2010. CHCIT offers introductory and advanced courses for IPS officials and other law enforcement officers of CBI on varied topics.

- Recognizing the importance of cyber forensics, training labs have been set up by the Government of India in association with DSCI and CDAC with support from MeitY at the training academy of CBI, Ghaziabad, in States of Kerala, Assam, Mizoram, Nagaland, Arunachal Pradesh, Tripura, Meghalaya, Manipur and Jammu & Kashmir and in Mumbai, Pune, Bangalore and Kolkata cities to train the officials from Police and Judiciary.

So far, these labs have trained more than 28,000 Police officials and 1000 judiciary officials:

3.6.1. Cyber Forensics Training Lab at Bengaluru

NASSCOM and DSCI established the Cyber Lab in the premise of CID Headquarters in Bengaluru and has been offering cyber-crime investigation and forensic training to LEAs of the State. The Cyber Lab has so far trained over 13,000 LEAs including police and military corps, and judiciaries through Karnataka Judicial Academy in the past 10 years. The Cyber Lab has all the infrastructure including hardware software and tools for digital forensic analysis. The Lab is continuously updating the library of open as well as proprietary digital forensic tools for training the police corps on analysis and investigation of cybercrimes. The Lab has made available cybercrime investigation manuals, SOPs in cybercrime investigation and cyber investigation pocket book for LEAs through their training initiatives. This has to be strengthened and augmented to provide training for cyber labs across the State. The activities of the lab are summarized as follows:\n
• Provide Short-term programs (1-day and 2-day programs) for personnel from government, public sector, defense and paramilitary forces on the basics of Cyber Security;
• Provide technical guidance and support to LEAs during investigations;
• Organize Cyber Safety weeks to spread public awareness on Cyber Security;
• Serve as the single point of contact for the industry to provide guidance on Cyber Security breach response;
• Conduct programmes for other government agencies and departments including Income Tax Department and Banks;

Further, in October 2018, Centre for Cybercrime Investigation Training & Research (CCITR) has been created in Bengaluru in a tri-lateral collaboration consisting of Karnataka State CID; DSCI and Infosys Foundation. The CCITR aims to train police, prosecution, judiciary and other departments in handling technology investigations and create Standard Operating Procedures (SOPs) in cybercrime investigations. The center will also be used to perform research in digital forensics and cybercrime investigation that will improve the prosecution of cybercrime cases investigated by the Karnataka Police. CCITR will also act as a resource centre for digital forensics in the State and provide forensics investigation support to the LEAs of the State. A malware research centre is also proposed to be hosted in CCITR to provide incidence reporting, handling and protection on malware.

3.6.2. Cyber Forensics Training for LEAs by Academic Institutions

Apart from the DSCI Cyber Labs, the premier academic institutes in the State, such as IISc, IITs and IIITs have also been offering training programmes to LEAs, government officials and working executives. National Law School of India University (NLSIU) is offering a post graduate diploma course in “Cyber Law & Cyber Forensics” as a distance education programme.

Appendix-3 provides a model of types of cybersecurity courses that can be offered by Institutes.

---

RECOMMENDATION

It is recommended that the State shall use its existing industry and academic resources and establish a special entity for public-private partnership in cybersecurity. Such an entity could aspire to bring various stakeholders such as police, forensics, academia, research groups, analysts, government departments and private organizations to develop interdisciplinary capability in combating cybercrime and promote a cyber secure state along the lines of the Cyberdome initiative of the Kerala State Police.

3.7. Competency Development for State Legislatures and Policy Makers

Legislatures and policy makers are more at risk due to cybercrime due to their public standing. Simple attacks such as hijacking of social media accounts can spread mis-information amongst public. There are not enough training programmes to address this need.

RECOMMENDATION

The State shall leverage its premier institutes such as IIM and NLSIU in preparing short-term training programmes for legislators and policy makers in the area of cybersecurity. Resources at the CFS at the FSL and Cyber Forensics Training labs in Bengaluru shall also be used to prepare a case based approach to training officials.

The following depicts the skill development programs available and being offered currently by various entities in the State and the country.

---

3.8. Estimation of skill requirement in Cyber Security in Karnataka

As on June 2018, there are 30,000 unfilled cyber jobs in the country, due to an absence of skilled individuals as per KPMG-NASSCOM report. Majority of the cyber security professionals today, have demonstrated their already gained expertise via recognized certifications such as CISSP, CISM & CISA. The following Table gives the percentage of these certified professional across different regions.

India has around 2055 CISSP certified professionals as of June 2018, which accounts for only 2% of the global CISSP talent pool.

---

24 CISSP, Certified Information Systems Security Professionals; CISA, Certified Information Systems Auditor; CISM, Certified Information Security Manager
One reason, for the low number of certified professionals from India, could be the high cost of these certifications. The CISM and CISA certifications cost more than $500 while a CISSP certification could cost an individual $699 to achieve. Companies focusing on cyber security should have certain provisions in place, to pay a part of the cost for their employee. The Government of Karnataka can take this one step further and offer individuals that have established their skill and shown their keen interest in cyber security, certain subsidies or scholarships. This will help bolster the cyber security talent in the country.

The skill problem is also intensified due to the new technology requirements. There is a lot of behavioral modelling and risk modelling that requires good statistical and mathematical background. The potential of using AI requires skills in machine learning and neural networks. Blockchain and quantum computing also bring in their nuances. Understanding of the new network capabilities like 5G is also key for designing the right cyber strategy. Essentially the increasing requirement is for multi skills or single stack engineers in the cyber security space. These skills are required to encourage global organizations to direct higher value-oriented work in the cyber security space to India.

Based on the above, following table gives an estimate of the manpower requirement in the State:

Table 2. Estimate of Cyber Security Professionals required in the State

<table>
<thead>
<tr>
<th>Employment (in Millions)</th>
<th>2018</th>
<th>2022</th>
<th>2025</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>India</strong> 25</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT/ITES Sector</td>
<td>4 Million</td>
<td>6.5 Million</td>
<td></td>
</tr>
<tr>
<td>Cyber Security</td>
<td>150,000 (as per NASSCOM Estimates)</td>
<td>1.0 Million</td>
<td></td>
</tr>
<tr>
<td><strong>Karnataka</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT/ITES Sector 26</td>
<td>1.2 Million</td>
<td>2 Million</td>
<td>3 Million</td>
</tr>
<tr>
<td>Cyber Security (Estimated)</td>
<td>40,000</td>
<td>80,000</td>
<td>300,000</td>
</tr>
</tbody>
</table>


26 Vision 2025 Karnataka (2018). Available at: https://navakarnataka2025.in/site/en/about#
4. PILLAR-3: PRODUCT TESTING AND CERTIFICATION

Testing and certification of ICT products to be compliant with national and international standards with respect to cyber security is essential for cyber security proof services. This is of utmost importance especially for ICT products used in government for providing its services.

OBJECTIVE:

To develop state of the art cyber security testing and assurance centres and processes to test and certify cyber security products as per International Common Criteria Certification Scheme for global promotion and acceptance.

Standardization Testing and Quality Certification (STQC) Directorate is an attached office of MeitY, GoI, that provides quality assurance services in the area of Electronics and IT through countrywide network of laboratories and centres. The services include testing, calibration, IT & e-Governance, training and certification to public and private organizations. STQC on behalf of India is the signatory to Common Criteria Recognition Arrangement (CCRA) with Indian Common Criteria Certification Scheme (IC3S) for evaluation and certification of IT products for security as per Common Criteria standards, Ver. 3.1/ISO/IEC 15408, up to EAL4 assurance level.

Further, the Department of Telecommunications has established the National Security Assurance Standards Facility of the National Centre for Communication Security in Bangalore on the 15th November 2018. These two initiatives go a long way in testing and certification of telecom products that would be deployed throughout the country and give an assurance of security for such products and the nation’s telecom infrastructure.

4.1. India Common Criteria Certification Scheme (IC3S)

The IC3S scheme has been set up by MeitY as part of Cyber Security Assurance initiatives of the Government of India to evaluate and certify IT security products and protection profiles against the requirements of Common Criteria Standards Ver 3.1 R2 at Evaluation Assurance Levels (EAL) 1 through 4. Presently the scheme provides national certification. The main players in this programme are developer of IT Security Products or Protection Profiles, Sponsors, Common Criteria Test Laboratory (CCTL) and Certification Body. The scheme would also provide a framework for international certification through the National Mutual Recognition Arrangement with the other member countries of CCRA. Along with 24 other

---

27 Standardization Testing and Quality Certification (STQC) Directorate. Available at: [http://meity.gov.in/content/stqc](http://meity.gov.in/content/stqc) accessed on 11 Dec 2018.
28 Indian Common Criteria Certification Scheme (IC3S) . Available at: [http://www.commoncriterion-india.gov.in/Pages/CCSOverview.aspx](http://www.commoncriterion-india.gov.in/Pages/CCSOverview.aspx) accessed on 11 Dec 2018.
countries, India has already become a member of CCRA as a certificate consuming nation and soon will be recognized as a certificate producing nation. As per the article 1 of the CCRA, certificates issued by one-member countries are accepted in other countries without re-certification.

STQC Directorate has the following objectives in developing, operating & maintaining Common Criteria based IT Security Evaluation & Certification Scheme:

i. To meet the needs of government and industry for cost-effective evaluation of IT products;
ii. To encourage the formation of commercial security testing laboratories
iii. To ensure that security evaluations of IT Security products are performed to consistent standards;
iv. To improve the availability of evaluated IT Security products.

The scheme is intended to serve following many communities of interest with very diverse roles and responsibilities:

i. IT product developers,
ii. IT security Product vendors,
iii. Value-added resellers of IT security product,
iv. Systems integrators for IT security infrastructure,
v. IT security researchers,
vi. Acquisition/procurement authorities of IT Security product,

4.1.1. Common Criteria Evaluation and Certification

Common Criteria evaluation is an impartial assessment of an IT product by an independent body. This provides users of such products with confidence in the security functionality provided. It also provides users with a metric to compare the security capabilities of products that they are intending to buy. The IT products to be evaluated are referred to as the Target of Evaluation (TOE). Certification provides independent confirmation of the validity of evaluation results, and thereby ensures comparability of these results across all evaluations under the scheme and facilitates mutual recognition of results between national schemes. Certification confirms that the TOE needs its security target to the claimed assurance level and that the evaluation has been conducted in accordance with the Standard of the scheme i.e. Common Criteria (eq.: ISO 15408).

The participation in the scheme and its associated evaluation & certification activities is strictly voluntary (unless mandated by government policy or regulations). In addition, organizations may undertake alternative activities to use Common Criteria and to demonstrate product conformance to IT security requirements.
The Certification Body (CB) is the STQC Directorate, Department of Electronics and Information Technology, Govt. of India. The Certification Body has been established under the official administration procedures of Govt. of India to meet the requirements of ISO Guide 65. Individual CCTL can register for empanelment with the STQC directorate as per the associated processes and guidelines. The CB shall enlist the details of the empanelled CCTL indicating the evaluation assurance levels for which they have been empanelled to carry out evaluation as per the requirements of Common Criteria standards. This is similar to the National Information Assurance Partnership (NIAP) that oversees a national program to evaluate Commercial Off-The-Shelf (COTS) Information Technology (IT) products for conformance to the international Common Criteria in the United States 29.

RECOMMENDATION

It is recommended that the State Government shall ensure the systems it owns and operates meet the benchmark cyber security standards and cybersecurity best practices. Projects that receive State funding must meet these standards as well. The State shall also take a lead in developing cyber security certification of products and services that are used for the provisioning of e-government services, including outsourced IT projects. The State e-Governance department shall set up Common Criteria Testing Lab (CCTL) for cyber security and get it empanelled by the STQC Directorate. Further, the State shall provide partial financial assistance for setting up and empanelment of IC3S CCTL by private firms.

4.2. State Advisory Committee for Cyber Security Assurance (SAC-CSA)

Addressing both security functionality and security assurance ensures that information technology products and the information systems built from those products using sound systems and security engineering principles are sufficiently trustworthy. Security controls shall be set so that they address security from both a functionality perspective (the strength of security functions and mechanisms provided) and an assurance perspective (the measures of confidence in the implemented security capability) 30. Much like the NIAP in the U.S., a State level advisory committee shall be set up to oversee cyber security controls and assurance across all stakeholders. The advisory committee shall manage a State level program for developing Protection Profiles, evaluation methodologies, specification of security and privacy controls especially for government organizations, that will ensure achievable, repeatable, and

---

testable cyber security requirements. In partnership with STQC, DSCI, and select premier Institutes in the State, the committee approves Common Criteria Testing Laboratories to conduct these security evaluations in private sector operations across the State. It is recommended that the IT procurements for the government are standardized and centralized and that SAC-CSA shall specify cyber security assurance framework and levels for the same.

The committee shall take a collaborative approach to technology-specific protection profile development by supporting the creation of international technical communities of representatives from industry, government, end users, and academia. The committee shall also specify consistent evaluation methodologies across the State testing labs associated with IC3S.

**RECOMMENDATION**

_The State shall constitute a State Advisory Committee on Cyber Security Assurance (SAC-CSA) for guiding testing and certifications of products and services across the state and also empanel CCTLs in the State to be compliant with IC3S._
5. PILLAR-4: BUSINESS PROMOTION

OBJECTIVE:

To evolve the start-up entrepreneurial eco-system in the State to be the best in the country and a leading destination globally in the area of cyber security products and services. Create investor friendly State for nurturing businesses in the area of cyber security to create over one million jobs in the State.

India continues to be the major provider of global IT services. According to NASSCOM, the Indian IT industry is set to reach a size of USD 350-USD 400 billion by 2025. There are about 1,140 Global Capability Centres (GCCs) of major multinationals in India. Many of the Global Capability Centres (GCCs) have their Cyber Security programmes situated in India. The average budget allocated to Global Cyber Security delivered by India based GCCs have been increasing rapidly (KPMG, 2018). Hence there is a potential for developing and providing Cyber Security products and services out of India. Globally, major markets for the export of Cyber Security Services include the U.S., U.K., Singapore, Switzerland and EU member countries.

The IT industry in the country, due to projects with multinational clients has always been ahead of the curve in implementing IT security policies and deployment architecture. We find that from 2015 to 2016, according to the Gartner report there has been a 10.6 percent increase in India’s enterprise security spending (hardware, software and services). In the current scenario, enterprises in India, understanding the magnitude of the problem, are now prioritizing cyber security, which now occupies 30-40% of most overall IT budgets. The ecommerce landscape has changed in the past four to five years. Though businesses like banks, telecom companies and insurance firms have always been mandated to have cyber protection in place, now new-age companies (like ecommerce companies or online food portals), with their increasing online presence, have joined the band wagon.

Most of the IT and IT Enabled Services firms are ISO 27001 compliant, indicating thereby that these firms have deployed enterprise security architecture and controls in place. Further, due to the enforcement of European Union General Data Protection Regulation (EU GDPR) from 25 May 2018, most of the IT and ITES firms that serve EU clients have put in place data protection framework that complements enterprise security. Legislation has become stronger with about 50% of the 18 countries analyzed in 2017 have clearly defined laws which mandate notifying concerned data subjects upon detection of a data breach 31. As a consequence, share of overall enterprise IT budget allocated for security is about 4% - 8%. The Indian Industry has been offering security related services traditionally for many years. Most of the large IT/ITES companies have dedicated units focused on offering Cyber Security services that typically include:

---

• Consulting around Strategy, governance, technology & architecture
• Security implementation
• Threat intelligence collection, feeds and analysis
• Threat & vulnerability assessment and management
• Cyber security certification and training
• Risk & compliance consulting
• Incident management services
• Managed services for IT infrastructure
• Identity & access management
• Incident investigation and forensics

5.1. Business Growth drivers for Cyber Security in the State of Karnataka

The State of Karnataka has played a prominent role in contributing to the growth of IT sector in the country.

Following table gives the status of the IT sector in the State.

<table>
<thead>
<tr>
<th>Table 3. Highlights of the IT Sector in Karnataka ³²</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Number of IT companies</strong></td>
</tr>
<tr>
<td><strong>Number of high-tech start-ups</strong></td>
</tr>
<tr>
<td><strong>Direct Employment in the IT Sector and Percentage of national IT workforce</strong></td>
</tr>
<tr>
<td><strong>Percentage of contribution to the national software export revenue</strong></td>
</tr>
<tr>
<td><strong>Percentage of Global Capability Centres of multinational companies in the State (out of about 1,140)</strong></td>
</tr>
</tbody>
</table>

Though reliable estimates do not exist, about 40,000 are employed in cyber security and related technical areas in the State as given in Section 3.8. The country can build a cyber security product and services industry of USD 35 billion by 2025 and generate a skilled workforce of one million in the security sector.

³² Source: Economic Survey of Karnataka 2016-17
http://des.kar.nic.in/docs/Final%20English%20Economic%20Survey%202016-17_Full.pdf
³³ The employment includes those in IT sector and about 30,000 in the ESDM sector.
Karnataka enjoys major share of the country’s IT activities, therefore, it can be safely assumed that about 35 to 40% of this business activities may be conducted in Karnataka.

Following are the areas identified under this Pillar that are described in the next sections.

**Figure 8. KCSF Pillar 3: Business Promotion**

5.2. Promotion of Local Security Industry

Nurturing the start-up environment is therefore a critical component in the larger national strategy. Karnataka is home to 35% of the total number of start-ups in the country. However, there is no noticeable start-ups in the Cyber Security space. Though Bengaluru is ranked very high globally in the start-up ecosystem, there are only about 30-40 start-ups in the area of cyber and information security. To promote domestic Cyber Security industry, MeitY is working on a proposal of Grand Challenge for Start-ups to develop a Cyber security product on a given problem statement. The DSCI has incubated 80 cyber security startups in the past two years.

5.2.1. Venture Capital activity in cyber security startups

The US is home to close to 63 percent of the world’s privately-owned cybersecurity companies. Of these, only six California based cybersecurity companies raised over $200 million in funding in a year. The following Table gives the funding details of Cyber Security start-ups. According to research firm CB
Insights, most of the $3 billion invested globally in the cybersecurity space in 2015 went to startups in the US and Israel.

<table>
<thead>
<tr>
<th>Year</th>
<th>Number of Companies Founded</th>
<th>Number of Companies Funded</th>
<th>Number of Funding Rounds</th>
<th>Total Funding ($M)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2010</td>
<td>13</td>
<td>3</td>
<td>3</td>
<td>$14.42</td>
</tr>
<tr>
<td>2011</td>
<td>10</td>
<td>3</td>
<td>3</td>
<td>$2.60</td>
</tr>
<tr>
<td>2012</td>
<td>15</td>
<td>3</td>
<td>3</td>
<td>$0.58</td>
</tr>
<tr>
<td>2013</td>
<td>16</td>
<td>9</td>
<td>9</td>
<td>$12.86</td>
</tr>
<tr>
<td>2014</td>
<td>13</td>
<td>7</td>
<td>7</td>
<td>$15.38</td>
</tr>
<tr>
<td>2015</td>
<td>26</td>
<td>4</td>
<td>4</td>
<td>$2.50</td>
</tr>
<tr>
<td>2016</td>
<td>12</td>
<td>7</td>
<td>8</td>
<td>$13.74</td>
</tr>
<tr>
<td>2017</td>
<td>0</td>
<td>3</td>
<td>3</td>
<td>$0.52</td>
</tr>
</tbody>
</table>

Since cyber security (both in consumer and enterprise space) in India is at a nascent stage, VCs are yet to invest in big numbers in this new business. Data shows that the number of companies funded every year has failed to cross the single digit mark as given in Appendix-4. Nevertheless, there are a few VC firms that recognize the potential of this industry.

We find from the above analytics that out of the 29 funded startups in the cybersecurity space, 12 have raised funding in 2015 and 2016. Also 27 new companies came up in this space in the same period. Almost all the funded companies in India were bootstrapped for quite a significant amount of time, due to lack of early-stage funds. All of the investments made since 2015 were raised by companies that were formed on or before 2013.

5.2.2. Role of Start-up Accelerators

Many companies are not aware of potential cyber security breaches as most of these information is not publicized. Hence the start-ups see less business potential for their Cyber Security products. Another challenge for cyber security start-ups is that gaining large firms as clients can be difficult. Funding and managerial talent together are required to support startups.

Start-up accelerator could help by delivering business development programmes, engineering resource, professional services, and access to corporate customers and investors. The accelerator’s mission must
be to bring the whole industry together to accelerate innovation, entrepreneurship and business growth for Karnataka.

Startups moving through the accelerator programme should receive support from leading security authorities as they work with larger tech firms to identify critical cyber security challenges and threats, in the process create possibilities of securing commercial contracts and investment, and creating the type of services companies can benefit from. There is a need to develop "innovative solutions" to combat the increased scale and sophistication of cybersecurity threats. The accelerator must support both local and foreign cybersecurity startups, helping them fine tune their products for global markets. The accelerator must work with other cybersecurity accelerators around the world to offer learning platforms and other resources to help startups through initial support programmes to test cybersecurity business concepts, to provide early stage start-ups with financial and business structures, and go-to-market strategies.

**Recommendation**

*It is recommended that a cyber security start-up accelerator shall be set up jointly between the GoK and institutes of higher education. The accelerator shall consist of a cybersecurity research lab that would establish data analytics techniques to better detect and respond to cybersecurity attacks in real-time as well as new approaches to deploy IT system. The government must actively disseminate this information so that at least 100 companies will take advantage of the state-of-the-art accelerator during a three-year period, and should also get access international support through the Global Ecosystem of Partnership in Innovation and Cyber security (Global EPIC).*

5.3. Public Procurement and Make in India

The Government has issued Public Procurement (Preference to Make in India) Order 2017 vide the Department of Industrial Policy and Promotion (DIPP) Notification No. P45021/2/2017-B.E.-II dated 15.06.2017 and partially modified order no No.P-45021/2/2017-PP (BE-II) was issued on 28.05.2018, to encourage ‘Make in India’ and to promote manufacturing and production of goods and services in India with a view to enhancing income and employment. In furtherance of the Public Procurement (Preference to Make in India) Order 2017 notified vide reference cited above, the Ministry of Electronics and Information Technology (MeitY) has notified on 2nd July 2018 that Cyber Security being a strategic sector, preference shall be provided by all procuring entities to domestically manufactured/produced Cyber Security Products as per the aforesaid Order. Further, guidelines for Secure Application development have

---

34 Details of Global EPIC is available at: [https://globalepic.org/HomePage](https://globalepic.org/HomePage) accessed on 31 Oct 2018.
been issued by MeitY in June 2017. Karnataka Start-up policy also indicates Preferential Market Access (PMA) on public and government procurement for start-ups.

**Recommendation**

*It is recommended that the GoK shall engage with the industry and start-ups in the public procurement of cyber secure products to develop indigenous technologies and tools for use in the delivery of e-government and other electronic delivery systems. The PMA for indigenously developed cyber security products and services as laid down in other State/ Central policies on public and government procurement shall be followed.*

5.4. Developing indigenous Cyber Security Products

India became the 42nd signatory of the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies on 08th Dec 2017. This arrangement had included “intrusion software” and “intrusion software technology” under the controlled list in 2013, which essentially covered most of the active research in vulnerabilities and prevention technologies. This means certain high-end technology can be refused for use in India based on the global conditions at a specific time. For example, such a regime was in place post Pokhran blasts in 1998.

- The ability to scan and detect vulnerabilities in applications, infrastructure and networks is one of the fundamental stepping-stones to implement cyber security. Towards this, following capabilities need to be immediately established indigenously, to offset India’s current reliance on global providers for these technologies:
  - Active research for detection of vulnerabilities in widely used application, operating systems and infrastructure devices. This research would enable a more real time updation of ‘signatures’ in the detection technologies.
  - Development of cyber security products to support India’s Critical Infrastructure based on contemporary technologies.

Protecting intellectual property in the area of Cyber Security is also important given the various internationalization of cybercrimes. Hence efforts are needed both by the State and private firms to engage in building Intellectual Property (IP) in the cyber security area and obtaining associated patents. In this regard, world class institutions such as IISc, IIIT-B and other NITs in the State can contribute to IP

---

37 United Nations Security Council resolution 1172
and patent generation in the State. Hence a collaborative Academia-Industry-Government partnership is essential in building indigenous technologies and products in the area Cyber Security.

5.4.1. Use Case Clearing House

A “Use Case Clearing House” is proposed to be set up as part of CS-CoE for identification of problem statement and converting to PoC by start-ups. The creation of a marketplace for match making of the problem statement and industry solution is also being considered to take the cyber security solutions so developed to the market.

**Recommendation**

*The State through CS-CoE, industry and academic partners encourage development of IP and patents in the area of cyber security. As per the State Start-up policy [38], patent filing cost shall be reimbursed for start-ups filing cyber security patents. Further the cyber security accelerators as mentioned in 5.2.2. Shall provide start-ups with mentors, IP lawyer assistance, and funding assistance in the area of cyber security.*

5.5. Effective Public-Private Partnerships

Cyber Security is a shared responsibility across both public and private sectors. Recognizing the need for engagement with the private sector, a Joint Working Group has been set up at the National Security Council Secretariat. The National Cyber Strategy of the U.S. also indicates such partnerships for effective implementation of cyber secure State. Similarly, in the State of Karnataka, the Karnataka Information Technology Services (KITS) in partnership with private firms has been creating conferences, workshops, security awareness programmes under the auspicious of CS-CoE.

The city of Bengaluru is home to the development centres of the top multinational cybersecurity firms such as McAfee, Symantec, Cisco, Microsoft, Sophos, Trend Micro, British Telecom, and Check Point. Moreover, cybersecurity operations and support of large Global Capability Centres of multinationals are located in Bengaluru. With active public private partnerships, the State can become a leader in the cybersecurity industry and provide state of the art solutions to firms, and government in the State.

---

Recommendation

It is recommended that the GoK through KITS shall continue the public private partnership with industry specialists to promote cyber security infrastructure and skill development in the State.
6. PILLAR-5: CYBER SECURITY: RESEARCH & DEVELOPMENT

OBJECTIVE:

Making the State as an innovation hub for all emerging cyber security technologies by creating Centers of Excellence and industry/ academia/ government partner

Cyber Security R&D is one of the major initiatives identified by MeitY for securing the cyber space and it is aimed at promotion of development & technology, demonstration, proof of concept and R&D test bed projects for enhancing indigenous skills and capabilities in the area of cyber security. Research and development is carried out in the thrust areas of cyber security including (a) Cryptography and cryptanalysis, (b) Network & System Security, (c) Monitoring & Forensics and (d) Vulnerability Remediation & Assurance through sponsored projects at recognized R&D organizations. Various R&D projects have been initiated at institutions (including institutions in the North East). These institutions include CDAC centres, NIELIT centres, IISc, IITs, NITs, and other central universities.

The major outcomes include:

- R&D Capacity building in the areas of: cryptanalysis, steganalysis, cyber forensics, network traffic, malware, image, speech, audio/video, text mining etc.
- Setting up of R&D Infrastructure (including test beds)
- Creating indigenous solutions
- Creation of cyber forensic training infrastructure
- Training and awareness initiatives
- Development of skilled manpower for support to industry/user organisations
- Providing support to LEAs
- Enabling launch of Auditing services

The solutions developed under these projects have been provided to user agencies for testing, evaluation and operational deployment as indicated in previous section through different modes.
The framework for R&D in cybersecurity in the State can be as described in the following Figure:

**Figure 9. KCSF Pillar 4: Framework for R&D in cybersecurity**

6.1. Karnataka Cyber Security – Centre of Excellence

In accordance with and in continuing to nurture innovations in the area of cyber security, the State of Karnataka has created Cyber Security - Centre of Excellence (CS-CoE). The IISc has been chosen as the anchor institution for the CS-CoE. The basic framework of CS-CoE are given in the following Figure.

**Figure 10. Cyber Security – Centre of Excellence Framework of the Government of Karnataka**

CS-CoE Framework – Areas of Operation – 4 Pillars

- **Enabling Cybersecurity Industry in Karnataka**
  - Objectives:
    - Supporting high-potential early stage companies
    - Establishing Karnataka as hub for cybersecurity industry
  - Outcomes:
    - Boost cybersecurity industry - Start-ups, Solution providers, Managed services, Services Industry, OEM's

- **Enabling cybersecurity capacity building**
  - Objectives:
    - Develop reference architectures and leading practice guides
    - Assist state in tackling cyber threats
  - Outcomes:
    - Develop thought leadership
    - Encourage organizations to increase investment in cybersecurity

- **Collaboration and standardization**
  - Objectives:
    - To address skill gap
    - To design and develop cybersecurity courses
  - Outcomes:
    - Skilled workforce & increased employability
    - Skilling of Govt. officials

- **Cybersecurity awareness**
  - Objectives:
    - To help acquaint citizens with cybersecurity
    - To build campaigns focusing on citizen awareness
  - Outcomes:
    - Increased level of awareness among citizens
    - Pooled corpus of CSR initiatives focused on cultural shift in adoption of cyber safe practices
Following are the CS-CoE Framework Activities related to industry development:

- Contribute in cybersecurity start-up/ incubation programs
- Selection of participants for incubation program
- Scrutiny of ideas based on the potential and feasibility
- Provide business plan assistance in terms of business modelling, feasibility study and future scope
- Provide opportunity to security services and security solution providers to leverage cybersecurity opportunities in the state
- Carry out campaigns to educate cybersecurity user industry

CS CoE Framework Activities related with Research; Collaboration & standardization are given below:

- Creation of thought leadership and research in emerging areas of cyber security such as block chain and its application in information security, security applications of Artificial Intelligence (AI), adversarial AI, emerging techniques in authentication
- Creation of reference architecture for different areas of cybersecurity
- Identification, development and documentation of leading practices and standards
- Advisory to state on cyber threats, sharing threat intelligence with the government and industry amongst others
- Drive agenda for Industry development and on increasing uptake of cybersecurity solutions and services

CS-CoE Framework Activities related with capacity building are as follows:

- Design and develop roadmap for cybersecurity capacity building
- Assessment of skill gaps on regular basis
- Conduct training/workshops for different capacity building programs
- Develop cybersecurity course and curricula in partnership with academia/ universities
- Train government officials in cybersecurity

CS-CoE Framework Activities related with Cybersecurity Awareness are given below:

- Creation of citizen centric cybersecurity awareness campaigns
- Creation of awareness programs for universities and colleges
- Identification of delivery methods for awareness programs
- Assessment of different awareness programs for its impact and outreach
- Development of content on different awareness programs for publishing in the form of booklets, web content and social media
- Creation of customized awareness programs for government officials to make them abreast with current and upcoming cybersecurity threats

The current status and outcome achieved by CS-CoE and the targets for the year are provided in Appendix-5.
6.2. Institutional Collaborations

The State is also home to some of the best academic institutes in technology (e.g. IISc, IIT Dharwad, IIT Raichur, IIIT Bangalore, IIIT Dharwad), management (IIM Bangalore), and law (NLSIU) institutions in the country. The Cryptology and Information Security lab and the Security Research Group at IISc \(^{39}\), is one of the few centres of excellence in cybersecurity research. These institutes along with CDAC centres in Cybersecurity and Forensics could lead cybersecurity research in the State, spill overs of which could result in effective implementation of a cyber secure State.

Government entities such as ISRO, DRDO, and DAE have embedded security governance, administration and preparedness in their programmes and have expertise in handling various security issues of national importance. The State which is home to some of the research labs of these entities should forge a collaboration with them to harness their knowledge and experience in furthering cyber security programmes.

---

**Recommendation**

*The State shall leverage the R&D capabilities of its strong institutions though it’s CoE to address leading research problems in cybersecurity. It is recommended that active collaborations between the Cyber Forensic Division, Cyber Labs, and CS-CoE is facilitated for reaping the benefits of leading research in cybersecurity.*

---

\(^{39}\) Security Research Group at IISc. Available at: [https://securityresearch.iisc.ac.in/](https://securityresearch.iisc.ac.in/) accessed on 4 Nov 2018.
7. PILLAR-6: STATE POLICIES AND REGULATION

OBJECTIVE:

Providing strategic advice on cyber security to the State and business communities. Developing cyber laws and regulation as per State’s specific requirements to complement already existing national cyber laws.

To achieve the above objectives, it is recommended that the State shall constitute a Cyber Security Council and a legal/policy think tank as illustrated in the following Figure.

Figure 11. KCSF Pillar 6: State Cyber laws and regulation

7.1. Cyber Security Council of Karnataka (CSC-K)

The Government shall constitute the Cyber Security Council of Karnataka (CSC-K), an independent advisory body of the State consisting of high-ranking representative from (i) academic and scientific communities and institutions; and (ii) public and private sector organisations. The Council must undertake efforts at strategic level to bolster cyber security in the State. The Council must aim at providing solicited and suo moto strategic advice on cyber security to the State government and the business community. It shall also monitor trends and new technologies developments and where necessary, translate these into
potential measures to reduce the cyber security risks. The Council shall initiate and accelerate relevant initiatives in the State to noticeably improve the level of cyber security in the State.

### 7.2. Cyber Security Legal and Policy Think Tank (CS-LPTT)

The GoI has enacted cyber and associated laws such as IT Act 2000, and Indian Telegraph Act, and will soon be tabling Data Protection Bill in the parliament. The focus of these acts have been protecting national, enterprise and individual security. However, certain cyber offenses and incidents may be location specific and might be attributed to the linguistic, religious, and political issues of the State, especially in the areas of digital social media. There are states such as Telangana have proposed State specific cyber laws and related legislation. It is recommended that the State sets up a legal and policy think tank with members from Government, CERT-In, Industry and Academia to provide recommendations and advice on state specific policies and regulations relating to cyber security.

---

**RECOMMENDATION**

The State shall constitute the Cyber Security Council of Karnataka (CSC-K) to provide strategic advice on cyber security to the State government and business communities. Further, in accordance with preserving State’s interest in regulating cyber content and at the same time enabling free speech, it is recommended that the State creates legal and policy think tank, anchored in NLSIU to provide inputs on State specific laws and regulations in the area of cybersecurity.

---

8. PILLAR-7: OUTREACH PROGRAMMES

OBJECTIVE:

*Engage with all stakeholders, in particular, the public and students, on a continuing basis through well-orchestrated cyber security outreach programmes and technical events.*

Cyber security is ever evolving and hence the need to spread awareness, and knowledge about dos and dont’s to general public regularly. Students and youngsters are particularly vulnerable to cyber threats and incidents due to their constant digital interactions. Hence there is a need for the State to reach out to the youngsters in colleges and schools on a regular basis through well organized and schedule outreach events and activities. There shall also be regular hackathons at engineering and technical institutes to nurture students in developing security products, services and programmes to counter the increasing cyber security threats. The State has been conducting the Annual Bangalore IT Summit that draws many industry leaders, businesses and start-ups to the city. Along these lines, the State shall organize an Annual Industry Cyber Security Summit in Bengaluru that show cases the industry and business leadership of the State in the area of cyber security. Apart from the summit, the State shall engage with academic institutions to conduct an annual research conference on cyber security to demonstrate cutting edge research in the area. Karnataka State Council for Science & Technology (KSCST) at the IISc shall promote these programmes through its outreach wing.

Following figure provides a view of various outreach programmes that shall be conducted to keep public at large informed about cyber security.
**RECOMMENDATION**

*Recognizing the ever-evolving cyber security technology landscape, the State shall promote annual events, hackathons and conferences on the subject to promote awareness, education, knowledge and skills for combating cyber security threats and incidents. These events shall be coordinated by the KSCST.*
9. INTERNATIONAL PRACTICES OF CYBER SECURITY GOVERNANCE

As indicated in the previous sections, cyber security cuts across many sectors and hence the policy makers have struggled to adapt the existing bureaucratic structures to cyber security management and governance. In many countries, a government ministry or a central organization has evolved by accident or design to coordinate and lead cyber security initiatives. The following Table illustrates the various models of cyber security governance adopted by different countries including India at the national level 41. Based on these various models and to synchronize with the national governance structure, it is recommended that the Department of IT-BT-ST be made as the coordinating department in the State for all cyber security related activities.

---

Table 5. Karnataka State Cyber Security 2025 Key Goals

<table>
<thead>
<tr>
<th>Country</th>
<th>Ministry Responsible</th>
<th>Model of Governance</th>
<th>CERTs</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Netherlands</td>
<td>Ministry of Security and Justice</td>
<td>National Cyber Security Centrum (NCSC) acts as a central node, facilitating cooperation between other government ministries and private firms for crisis management in a distributed manner.</td>
<td>Government and Defense CERTs for civilian and defense needs respectively</td>
</tr>
<tr>
<td>Denmark</td>
<td>Ministry of Defence</td>
<td>Danish Emergency Management Agency under the Ministry of Defence is responsible for crisis management.</td>
<td>Military and government CERTs were combined to form Centre for Cyber Security.</td>
</tr>
<tr>
<td>Estonia</td>
<td>Economic Affairs and Communication</td>
<td>Estonian Information Systems Authority (Riigi Infosusteemi Amet (RIS) is responsible for cyber security governance using effective public private partnerships.</td>
<td>CERT-EE combines both the national and government CERT functions.</td>
</tr>
<tr>
<td>United States</td>
<td>Department of Homeland Security (DHS) – cabinet department of the U.S. government</td>
<td>DHS National Cyber Security Division (NCSD) is responsible for response system, risk management program, and requirements for cyber-security in the U.S.</td>
<td>National Cybersecurity and Communications Integration Center (NCCIC) is the Nation’s flagship cyber defense, incident response, and operational integration center. NCCIC integrated United States Computer Emergency Readiness Team (US-CERT) and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT).</td>
</tr>
<tr>
<td>India</td>
<td>Ministry of Electronics and Information Technology (MeitY)</td>
<td>Cyber laws and e-security division of MeitY is responsible for coordinating cyber security functions.</td>
<td>CERT-In housed within MeitY is the nodal agency for responding to cyber security incidents.</td>
</tr>
</tbody>
</table>
10. METHODOLOGY

The methodology we used in this study is represented in the following Figure.

![Figure 13. Methodology used in the study](image)

10.1 Secondary Data Sources

Industry reports, government reports and web sites as indicated in the References section and footnotes were analyzed and distilled. The key findings from these reports have been used in drawing our recommendations.

10.2 Inputs from Experts and Members of the Task Group

Members of the KSCV Task Group had five meetings in which various aspects of the report were discussed. The comments and feedback from the members have been taken in to account in the final preparation of the report.

10.3 Inputs from Other Key Stakeholders

Inputs from various industry bodies such as NASSCOM and DSCI, central government institutions such as CDAC and CERT-In, academic institutions such as IIT-M have been taken in to account in the preparation of the report. Inputs from department of IT-BT-ST is included in the report.
The final report with recommendations have been arrived at by synthesizing all the above inputs and deliberations of the Task Group members.

**RECOMMENDATION**

*Since this report is based on thought leadership, secondary data, inputs from experts and information available from relevant bodies, it is recommended to commission a primary survey and market research that shall reflect the practical ground realities and major issues impacting across the six pillars of this Vision Study. The finding of such survey research may also serve a reference to build the design and prepare a blue-print for the program implementation.*
### 11. KARNATAKA CYBER SECURITY VISION 2025: SUMMARY OF RECOMMENDATIONS AND KEY GOALS

#### 11.1. KEY CYBER SECURITY GOALS

Summary of recommendations for achieving Karnataka Cyber Security Vision are given below

<table>
<thead>
<tr>
<th>Pillars</th>
<th>Key Objective</th>
<th>Recommendations</th>
</tr>
</thead>
</table>
| 1: Enforcement and Protection | Detect, prevent, mitigate, and deter cyber security attacks and crimes by building an enabling infrastructure of incidence response centres, investigation labs, and certification processes through active Government/Industry/Academia collaborations | 1) Due to increase in cybercrime and incidences, it is imperative for the State Police to develop deep expertise in cybercrime investigation and forensics. Hence it is recommended that the State Police develop a cadre for cybercrime so that all cyber police stations in the State be equipped with qualified IOs.  
2) Further, the CFS at Bengaluru provides forensic analysis and support to all cybercrime incidences across the State. It is recommended that a unit comprising of the requisite scientists, administrators and associated infrastructure be set up at each of the 30 cyber police stations with Bengaluru CFS providing expert guidance and support. The cadre of administrators and scientists at CFS be re-examined to provide growth opportunities for this very important section of the State Police.  
3) It is recommended that all the CFS of Cyber Police Stations be equipped with disk, mobile and network forensic tools for effective evidence analysis.  
4) It is proposed to set up Karnataka's Computer Emergency Response Team (K-CERT) along similar lines that of CERT-In as part of the Centre of Excellence – Cyber Security (CoE-CS) that has been set by the GoK. K-CERT shall coordinate with CERT-In to provide forecasts and alerts on cyber security incidence, release timely vulnerability disclosures, and assist in emergency measure for handling cyber incidents. |
| 2: Skill Development     | Making cyber security an essential part of citizen's life and promoting cyber secure culture amongst all | 1) It is recommended that resources available at CDAC-H be leveraged by the State to prepare cyber security awareness campaign in various formats (e.g. posters, videos, newsletters, and other artefacts) in Kannada. Further, it is recommended that the State shall review the cyber security awareness campaign in the State and update the program as necessary. |
strata of the society. Educate and promote cyber security awareness at all sections of the society including legislatures, government officials, educators, private industry, society and public at large in partnership with academia and industry.

**security syllabus and the associated books to be published by NCERT to assess whether these shall be included in the State board curriculum as well at appropriate classes both in Kannada and English.**

2) It is recommended that cyber security course resources available NPTEL offered by Institutes such as IISc and IIT-M shall be leveraged to educate the students and faculty at Institutes and colleges. Hub-and-spoke - “Train the trainer” model is recommended for scaling up the cybersecurity training programmes, with premier institutes in the State including IISc, IITs and IIITs being at the hubs in the cog, to reach out to the faculty in tier-2 and 3 institutes in the State. It is recommended that the State shall actively review the cybersecurity text books being developed by CDAC-H/ NCERT for incorporating in the State Board curriculum both in English and Kannada mediums to improve information and cyber security awareness amongst secondary school children in the State.

3) It is recommended that the State shall promote the Futureskills platform of NASSCOM, the cyber security QPs developed by DSCI, and information security courses offered through NPTEL for enhancing the skill and knowledge levels of government officials associated with IT and IT services implementation, and State-owned Public-Sector Enterprises and financial institutes.

4) It is recommended that State shall create a consortium of premier Institutes with support from NIELIT, Gorakhpur to develop Cyber Security Certification Courses

5) It is recommended that the State shall use its existing industry and academic resources and establish a special entity for public-private partnership in cybersecurity. Such an entity could aspire to bring various stakeholders such as police, forensics, academia, research groups, analysts, government departments and private organizations to develop interdisciplinary capability in combating cybercrime and promote a cyber secure state along the lines of the Cyberdome initiative of the Kerala State Police.

6) The State shall leverage its premier institutes such as IIM and NLSIU in preparing short-term training programmes for legislatures and policy makers in the area of cybersecurity. Resources at the CFS at the FSL and Cyber Forensics Training labs in Bengaluru shall also be used to prepare a case based approach to training officials.

7) The State shall also use the hundreds of ITIs – both Government and Private to impart vocational training as part of the existing certification programmes to scale up human resources in the area cyber security skill development.

<p>| 3. Product Testing and Certification | To develop state of the art cyber security testing labs to conduct and certify cyber security products | 1) It is recommended that the State Government shall ensure the systems it owns and operates meet the benchmark cyber security standards and cybersecurity best practices. Projects that receive State funding must meet these standards as well. |</p>
<table>
<thead>
<tr>
<th>4: Business Promotion</th>
<th>To evolve the start-up entrepreneurial eco-system in the State to be the best in the country and a leading destination globally in the area of cyber security products and services</th>
</tr>
</thead>
<tbody>
<tr>
<td>1)</td>
<td>It is recommended that a cyber security start-up accelerator shall be set up jointly between the GoK and institutes of higher education. The accelerator shall consist of a cybersecurity research lab that would establish data analytics techniques to better detect and respond to cybersecurity attacks in real-time as well as new approaches to deploy IT systems. The government must actively disseminate this information so that at least 100 companies will take advantage of the state-of-the-art accelerator during a three-year period, and should also get access international support through the Global Ecosystem of Partnership in Innovation and Cyber security (Global EPIC).</td>
</tr>
<tr>
<td>2)</td>
<td>It is recommended that the GoK shall engage with the industry and start-ups in the public procurement of cyber secure products to develop indigenous technologies and tools for use in the delivery of e-government and other electronic delivery systems as per the PMA policies of State/ Central governments.</td>
</tr>
<tr>
<td>3)</td>
<td>The State through CS-CoE, industry and academic partners encourage development of IP and patents in the area of cyber security. As per the State Start-up policy(^{42}), patent filing cost shall be reimbursed for start-ups filing cyber security patents. Further, the cybersecurity accelerators as mentioned in 5.2.2. Shall provide start-ups with mentors, IP lawyer assistance, and funding assistance in the area of cyber security.</td>
</tr>
<tr>
<td>4)</td>
<td>It is recommended that the GoK through KITS shall continue the public private partnership with industry specialists to promote cyber security infrastructure and skill development in the State</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>5: Research &amp; Development</th>
<th>Making the State as an innovation hub for all emerging cyber security technologies by creating Centers of</th>
</tr>
</thead>
<tbody>
<tr>
<td>1)</td>
<td>The State shall leverage the R&amp;D capabilities of its strong institutions though its CoE to address leading research problems in cybersecurity. It is recommended that active</td>
</tr>
</tbody>
</table>

---

| 6: State Policies and Regulation | Developing cyber laws and regulation as per State’s specific requirements to complement already existing national cyber laws | 1) The Government shall constitute the Cyber Security Council of Karnataka (CSC-K) to provide strategic advice on cyber security to the State government and business communities.  
2) In accordance with preserving State’s interest in regulating cyber content and at the same time enabling free speech, it is recommended that the State creates legal and policy think tanks, anchored in NLSIU to provide inputs on State specific laws and regulations in the area of cybersecurity. |
| 7. Outreach Programmes | Engage with all stakeholders, in particular, the public and students, on a continuing basis through well-orchestrated cyber security outreach programmes and technical events through the outreach wing of KSCST. | 1) Organize an annual Industry Summit on Cyber Security along the lines of BangaloreIT.com to show case the business and industry leadership of the State in cyber security.  
2) Organize an annual flagship conference on “Information Security Engineering” to showcase talent, innovation, technology, products, services, and business in the area;  
3) Organize regular hackathons at engineering and technical institutes in the State to nurture students in developing security products, services and programmes to counter the increasing cyber security threats;  
4) Conduct public events and workshops to educate general public about cyber security incidents and protection at each district of the State. |
### 11.2. KEY PERFORMANCE INDICATORS AND TARGETS

#### KARNATAKA CYBER SECURITY VISION 2025

**Table 7. Key Performance Indicators and Targets**

<table>
<thead>
<tr>
<th>S.No.</th>
<th>Key Performance Indicators</th>
<th>Current</th>
<th>Implementing Agency(^{43})</th>
<th>Target for 2022</th>
<th>Target for 2025</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>1. Protection &amp; Enforcement</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1.</td>
<td>Number of Cyber Police Stations equipped with Cyber Forensic Section with disk, mobile and dynamic network analysis tools</td>
<td>One in Bengaluru</td>
<td>CID, EOSU</td>
<td>One in each of the major district headquarters of Belagavi, Hubballi-Dharwad, Mangaluru, Mysuru, and Tumakuru</td>
<td>One in each of the other major urban agglomerations of Hassan, Davanagere, Ballari, Gulbarga, Chitradurga and Hosakote</td>
</tr>
<tr>
<td>1.2.</td>
<td>Karnataka Computer Emergency Response Team (K-CERT)(^{44})</td>
<td>None</td>
<td>IT-BT(^{45})</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1.3.</td>
<td>State Cyber Security Oversee and Governance Cell</td>
<td>None</td>
<td>IT-BT</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1.4.</td>
<td>State’s rank in the order of lowest number of users affected by ransomware/ malware attacks</td>
<td>-</td>
<td>IT-BT</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1.5.</td>
<td>State’s rank in the order of fastest cyber security incident response</td>
<td>-</td>
<td>IT-BT</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td><strong>2. Competency &amp; Skill development</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.1.</td>
<td>Number of Cyber Security Professionals in the State</td>
<td>40,000</td>
<td>DTE-DE</td>
<td>80,000</td>
<td>300,000</td>
</tr>
<tr>
<td>2.2.</td>
<td>Number of Certified Cyber Security Professionals in the State through employment linked skilling programme</td>
<td>1,000 (Est) (through Yuva Yuga programme)</td>
<td>CoE-CS with industry partnership</td>
<td>2500 (through Yuva Yuga programme)</td>
<td>5000</td>
</tr>
<tr>
<td>2.3.</td>
<td>No. of government ITIs equipped to provide cyber security courses</td>
<td></td>
<td>DSDEL</td>
<td>50 (of the about 175 Govt. ITIs)</td>
<td>100</td>
</tr>
</tbody>
</table>

---

\(^{43}\) Notes:
CID-EOSU – Criminal Investigation Department, Economic Offences and Special Units; CeG-DPAR – Centre for e-Governance, Department of Personnel and Administrative Reforms; CoE-CS – Centre of Excellence in Cyber Security, Karnataka Information Technology Services; DME – Department of Mass Education; DSKEL – Department of Skill Development, Entrepreneurship and Livelihood; DTE-DE – Directorate of Technical Education – Department of Education; IT-BT-ST – Department of Information Technology, Bio Technology, Science & Technology

\(^{44}\) IT Act 2000 does not have provision to set up state level CERT as per Sections 70A and 70B. Hence the Government of Karnataka shall enable creation of CERT-K though an executive order.

\(^{45}\) For KPIs 1.2-1.5, commensurate with the national nodal agency (CERT-In) under MeitY as mentioned in Section 9, we recommend that these are owned and managed by Department of IT-BT in Karnataka. Since K-CERT will mainly deal with cyber security incidents affecting government, businesses and citizens of the State and not focus on cyber warfare and International cyber terrorism, other departments such as Home Ministry may not be technically as competent as IT-BT to manage these KPIs.
2.4. Percentage of State Government Departments provided with Cyber Security Training Programmes | CeG-DPAR | 50% of the departments | 100% of the departments
2.5. Percentage of District and Taluk officials provided with Cyber Security training | CeG-DPAR | 15 districts | All districts
2.6. Cyber Security awareness programmes conducted for legislatures and policy makers | CeG-DPAR | 5 | 10
2.7. Cyber Security awareness programmes conducted for Law Enforcement Officials | EOSU | 10 | 20
2.8. Cyber Security awareness programmes conducted for Citizens of the State | DME | 15 districts | All

### 3. Product Testing and Certification

| 3.1. Empaneled Common Criteria Testing Labs for IC3S cyber security certification | - | CeG-DPAR | 5 | 10
| 3.2. State Advisory Committee – Cyber Security Assurance | - | CeG-DPAR | One | One

### 4. Business Development

| 4.1. Direct employment of Cyber Security professionals in the State skilled through the Yuva Yuga programmes | 40,000 | IT-BT | 80,000 | 300,000
| 4.2. Number of Cyber Security Start-ups in the State (through subsidizing seats for Cyber Security startups in state supported Incubators/CS-CoE) | 30 | IT-BT | 50 | 100
| 4.3. Number of Unicorns (valuation more than $1 billion) in Cyber Security | - | IT-BT | 2 | 5
| 4.4. Number of Cyber Security Accelerators in the State (by supporting existing and new accelerators with dedicated subsidized seats for Cyber Security startups) | - | IT-BT | 2 | 5

### 5. Research & Development

| 5.1. National Cyber Security Centre of Excellence (CS-CoE) | One in Bengaluru (at IISc) | IT-BT | 1 | 2 (Additional one in Dharwad at IIT/IIIT)
| 5.2. Number of Granted Cyber Security patents for which financial support/incentives provided through CoE-CS | None | CoE-CE | 25 | 100

### 6. State Policies & Regulation

| 6.1. Cyber Security Council of Karnataka (CSC-K) | - | IT-BT | 1 | 1
| 6.2. Cyber Security Legal and Policy Think Tank | - | IT-BT | 1 | 1

### 7. Outreach Programmes

| 7.1. Annual research conference | - | CoE-CS | 1/year: 4 for the period | 1/year: additional 3 events
| 7.2. Hackathons at various Institutes | - | CoE-CS | 12/year, one at each institute per month at 12 Institutes; about 50 for the period | Additional 50
| 7.3. Public events and workshops | - | CoE-CS | About 2 per quarter at various districts; cover all 30 districts once | Provide a second time offering at each of the 30 districts
<table>
<thead>
<tr>
<th></th>
<th>7.4 Annual Industry Summit on Cyber Security</th>
<th>-</th>
<th>CoE-CS</th>
<th>1/year; 4 for the period</th>
<th>1/year; additional 3 years</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1</td>
<td>Conduct primary survey and market research study to assess the ground realities and prepare an implementation plan</td>
<td>CoE-CS</td>
<td>One at the beginning of implementation</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>State Budget</td>
<td>90.03 Cr</td>
<td>Additional 49.63 Cr</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**8. Methodology**

**9.1. State budget for Cyber Security Programme**
## 11.3. PROPOSED GOVERNMENT BUDGET

### Table 8. Proposed Government Budget for the Cyber Security Programme

<table>
<thead>
<tr>
<th>S.No.</th>
<th>Key Performance Indicators</th>
<th>Cost Details</th>
<th>Implementing Agency</th>
<th>Target for 2022</th>
<th>Target for 2025</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>In Rs.</td>
<td>Activity Budget (in Lacs of Rs.)</td>
<td>Activity Budget (in Lacs of Rs.)</td>
<td></td>
</tr>
<tr>
<td>1.1.</td>
<td>Number of Cyber Police Stations equipped with Cyber Forensic Section</td>
<td>Equipment and software cost: 30,00,000 for each station along with disk, mobile and network analysis tools</td>
<td>CID, EOSU</td>
<td>One in each of the major district headquarters of Belagavi, Hubballi-Dharwad, Mangaluru, Mysuru, and Tumakuru</td>
<td>150</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Initial employee salary cost for one Administrator, one Sr. Scientist and one Jr. Scientist at a total salary cost of 3,00,000 per month until target years</td>
<td>CID, EOSU</td>
<td>720</td>
<td>540</td>
</tr>
<tr>
<td>1.2.</td>
<td>Karnataka Computer Emergency Response Team (K-CERT)</td>
<td>Hardware, software for analysis, testing and reporting at 25,00,00,000</td>
<td>IT-BT-ST</td>
<td>1</td>
<td>2,500</td>
</tr>
</tbody>
</table>

### 2. Competency & Skill development

| 2.1   | No. of government ITIs equipped to provide cyber security courses | Content, hardware and software cost at 5,00,000 per ITI | DSDEL | 50 (of the about 175 Govt. ITIs) | 250 | Additional 50 | 100 |
| 2.2   | Percentage of State Government Departments provided with Cyber Security Training Programmes | One programme at a cost of 5,00,000; two such programmes per department | CeG-DPAR | 20 of the 40 departments | 200 | Additional 20 departments | 200 |
| 2.3   | Percentage of District and Taluk officials provided with Cyber Security training | Three programmes in each district with | CeG-DPAR | 15 districts | 113 | Remaining 15 districts | 113 |
| 2.4 | Cyber Security awareness programmes conducted for legislatures and policy makers | One programme at a cost of 2,50,000 | CeG-DPAR | 5 programmes | 50 | Additional 5 programmes | 50 |
| 2.5 | Cyber Security awareness programmes conducted for Law Enforcement Officials | One programme at a cost of 10,00,000 | EOSU | 10 programmes | 50 | Additional 10 | 50 |
| 2.6 | Cyber Security awareness programmes conducted for Citizens of the State | Content development and distribution at Rs. 2,00,000 for each district | DME | 15 districts | 30 | Remaining 15 districts | 30 |

### 3. Product Testing and Certification

| 3.1 | Empaneled Common Criteria Testing Labs for IC3S cyber security certification | Auditing and empanellement at 10,00,000 for each lab | CeG-DPAR | 5 | 50 | Additional 5 | 50 |
| 3.2 | State Advisory Committee – Cyber Security Assurance | Running expenses of 10,00,000 per year | CeG-DPAR | One | 40 | | 30 |

### 4. Business Development

| 4.1 | Number of GoK supported Cyber Security Accelerators/ augmenting seats for cyber security start-ups in existing accelerators | Set up cost of one accelerator at 10,00,00,000 | IT-BT-ST | One in Bengaluru | 1,000 | Additional one in Mangaluru | 1,000 |

### 5. Research & Development

| 5.1 | National Centres of excellence in Cyber Security | Set up cost of one CoE at 15,00,00,000 | IT-BT-ST | 1 | 1,500 | Additional one | 1,500 |
| 5.2 | Number of Granted Cyber Security patents for which financial support is provided by the GoK | Patent filing and grant cost at 2,00,000 per patent | CoE-CS | 25 | 50 | Additional 75 patents | 150 |

### 6. State Policies & Regulation

| 6.1 | Cyber Security Council of Karnataka (CSC-K) | Operational cost of 50,00,00,000 per year | IT-BT-ST | Constitution and one meeting per quarter | 200 | Additional one meeting per quarter | 150 |
| 6.2 | Cyber Security Legal and Policy Think Tank | Set up cost of 10,00,00,000 | IT-BT-ST | 1 | 1,000 | | |

### 7. Outreach Programmes
### KARNATAKA CYBER SECURITY VISION 2025

<table>
<thead>
<tr>
<th>7.1.</th>
<th>Annual research conference on Information Security Engineering</th>
<th>At Rs. 50,00,000 per annual conference</th>
<th>CoE-CS</th>
<th>1/ year: 4 for the period</th>
<th>200</th>
<th>1/ year: additional 3 events</th>
<th>150</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.2</td>
<td>Annual Industry Summit on Cyber Security</td>
<td>At Rs. 1,00,00,000 per year</td>
<td>CoE-CS</td>
<td>One per year</td>
<td>400</td>
<td>One per year</td>
<td>300</td>
</tr>
<tr>
<td>7.3</td>
<td>Hackathons at various Institutes</td>
<td>At Rs. 5,00,000 per hackathon including prizes for the winners, venue and coordination</td>
<td>CoE-CS</td>
<td>12/ year, one at each Institute per month at 12 Institutes; about 50 for the period</td>
<td>250</td>
<td>Additional 50</td>
<td>250</td>
</tr>
<tr>
<td>7.4</td>
<td>Public events and workshops</td>
<td>At Rs. 5,00,000 per event</td>
<td>CoE-CS</td>
<td>About 2 per quarter at various districts; covering all 30 districts once</td>
<td>150</td>
<td>Provide a second time offering at each of the 30 districts</td>
<td>150</td>
</tr>
</tbody>
</table>

### Methodology

<table>
<thead>
<tr>
<th>6.2.</th>
<th>Primary Research to prepare a comprehensive implementation plan</th>
<th>Appointing a consulting body to conduct primary research for implementation of the Task Group recommendation at 1,00,00,000</th>
<th>CoE-CS</th>
<th>100</th>
</tr>
</thead>
</table>

### Total

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>9,003</strong></td>
<td><strong>4,963</strong></td>
</tr>
</tbody>
</table>
References

### Appendix-1. The Oversee and Governance Job Categories

(adapted)

<table>
<thead>
<tr>
<th>Job Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legal Advice and Advocacy (LGA)</td>
<td>Provides legally sound advice and recommendations to leadership and staff on a variety of relevant topics within the pertinent subject domain. Advocates legal and policy changes, and makes a case on behalf of client via a wide range of written and oral work products, including legal briefs and proceedings.</td>
</tr>
<tr>
<td>Training, Education, and Awareness (TEA)</td>
<td>Conducts training of personnel within pertinent subject domain. Develops, plans, coordinates, delivers and/or evaluates training courses, methods, and techniques as appropriate.</td>
</tr>
<tr>
<td>Cybersecurity Management (MGT)</td>
<td>Oversees the cybersecurity program of an information system or network, including managing information security implications within the organization, specific program, or other area of responsibility, to include strategic, personnel, infrastructure, requirements, policy enforcement, emergency planning, security awareness, and other resources. Enforcing compliance to standard cyber security operations procedures; auditing and reporting of deviations including levying penalties.</td>
</tr>
<tr>
<td>Strategic Planning and Policy (SPP)</td>
<td>Develops policies and plans and/or advocates for changes in policy that support organizational cyberspace initiatives or required changes/enhancements.</td>
</tr>
<tr>
<td>Executive Cyber Leadership (EXL)</td>
<td>Supervises, manages, and/or leads work and workers performing cyber and cyber-related and/or cyber operations work.</td>
</tr>
<tr>
<td>Program/Project Management (PMA) and Acquisition</td>
<td>Applies knowledge of data, information, processes, organizational interactions, skills, and analytical expertise, as well as systems, networks, and information exchange capabilities to manage acquisition programs. Executes duties governing hardware, software, and information system acquisition programs and other program management policies. Provides direct support for acquisitions that use information technology (IT) (including National Security Systems), applying IT-related laws and policies, and provides IT-related guidance throughout the total acquisition life cycle.</td>
</tr>
</tbody>
</table>
Appendix-2. Cyber Security Governance Principles for Corporate Directors

The National Association of Corporate Directors has distilled the responsibilities of CXOs and corporate directors as the following five principles:

1. **PRINCIPLE 1**: Directors need to understand and approach cyber security as an enterprise-wide risk-management issue, not just an IT issue.
2. **PRINCIPLE 2**: Directors should understand the legal implications of cyber risks as they relate to their company’s specific circumstances.
3. **PRINCIPLE 3**: Boards should have adequate access to cyber security expertise, and discussions about cyber-risk management should be given regular and adequate time on the board meeting agenda.
4. **PRINCIPLE 4**: Directors should set the expectation that management will establish an enterprise-wide, cyber-risk management framework with adequate staffing and budget.
5. **PRINCIPLE 5**: Board discussion of cyber risk management should include identification of which risks to avoid, accept, mitigate, or transfer through insurance, as well as specific plans associated with each approach.

---

46 National Association of Corporate Directors (NACD) Director’s Handbook on Cyber-Risk Oversight. Available at: https://www.nacdonline.org/insights/publications.cfm?ItemNumber=10687
Appendix-3. Model Cybersecurity training curriculum

- **Short Term (3 days) Certificate Courses (online/off-line)**
  - Application Level Security
  - OS Security
  - Network Security
  - Penetration Testing
  - Cyber Forensics

- **Mid Term (2-6 months) (mainly on-line)**
  - Theories as in Short Term Courses
  - Hands-on practical sessions on each topic

- **Long Term (1-2 Semesters) Courses (face to face)**
  - Logic & Reasoning
  - Combinatorics
  - Basics of Cryptography
  - Data Analysis
  - Architectural aid to Information Security
  - Hands-on Projects
Appendix-4. India based Cyber Security Start-ups and associated Funding
# Appendix-5. Current and Expected outcomes of CS-CoE

## Current Status – Outcome Achieved @CS-CoE

<table>
<thead>
<tr>
<th>Area</th>
<th>Major Parameters</th>
<th>Measure / Detailed Activities of Performace @ CoE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Internship pool created</td>
<td>30 CS Certified Work-Force Identified to be trained by End of October. Ready to be adopted / employed by the Partners</td>
</tr>
<tr>
<td>2</td>
<td>Enablement to Start-up's</td>
<td>~15 CS Startups Identified for Mentoring &amp; Acceleration Program</td>
</tr>
<tr>
<td>3</td>
<td>Capacity building</td>
<td>Started Implementation &amp; planning for Training through CoE; Physical Setup and Infra under Procurement. Current Team Strength of CoE - TWO : CEO + Center Manger</td>
</tr>
<tr>
<td>4</td>
<td>Thought leadership/ Whitepapers</td>
<td>Info-Sec-Best Practices Concept Note for Govt Dept. For implementation. 6 Thought Leaders &amp; Influences in CS Visited CoE, of which 2 are Global Leaders. 4 Thought Leadership program events attended, presented Key Notes 7 Core Team members identified for Panel of Deep Tech Expert / Ethical Hacker</td>
</tr>
<tr>
<td>5</td>
<td>Cybersecurity awareness workshops</td>
<td>621+ Industry Professionals Contacts / Connected through CoE Outreach. 80+ CS Aware Workforce through 2 Industry Town-hall Workshops Conducted CS-CoE Portal and KX (Knowledge eXchange) Portal launched under “Innovate Karnataka Online Portal Framework” CS-Authentication Standards Awareness – Launched</td>
</tr>
<tr>
<td>6</td>
<td>Global Collaboration</td>
<td>3 Global Collaboration Partners Identified (Netherland, Israel, France)</td>
</tr>
</tbody>
</table>

## Expected Outcome – By End of DEC 2018 (next 4 Months)

<table>
<thead>
<tr>
<th>Area</th>
<th>Major Parameters</th>
<th>Measure / Detailed Activities of Performace @ CoE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Internship pool created</td>
<td>Tech Aware Workforce @30 Per Month, once CoE is operational 30 District of KA – Hub &amp; Spoke Model Framework &amp; Plan for Internship for College / University</td>
</tr>
<tr>
<td>2</td>
<td>Enablement to Start-up's</td>
<td>100+ Corporate Members : From Corporate, MSME, Public Sector, Govt. 100+ Tech Trained Workforce from CoE [ Basic / Intermediate/ Advanced] Build a 7 Member Core CoE Team: CTO, Center Manager, Training Manager, Community Manger, Tech Expert, Tech Lab Assistant, General Admin.</td>
</tr>
<tr>
<td>3</td>
<td>Capacity building</td>
<td>CoE Physical Infra and Setup to be ready. 100+ Tech Trained Workforce from CoE [ Basic / Intermediate/ Advanced] Build a 7 Member Core CoE Team: CTO, Center Manager, Training Manager, Community Manger, Tech Expert, Tech Lab Assistant, General Admin.</td>
</tr>
<tr>
<td>4</td>
<td>Thought leadership/ Whitepapers</td>
<td>10 Thought Leaders / Influencers Visits to CoE – from National / Global CS Community 2 Participation / Key Note Address in National Collaboration CS Technology Events ( @Mumbai in Sept &amp; One More) Project Implementation by CoE on Information Security at KITS</td>
</tr>
<tr>
<td>5</td>
<td>Cybersecurity awareness workshops</td>
<td>8 Industry Town-hall Workshop (one external &amp; one internal venue every month)</td>
</tr>
<tr>
<td>6</td>
<td>Global Collaboration</td>
<td>2 International Events Participation (HSD in Oct &amp; BTS in Nov) To conduct Initial meetings with France &amp; Israel for building alliance. Global Exchange Program in CS: Adopt the existing one from Govt of KA</td>
</tr>
</tbody>
</table>
Appendix-6. GO on Karnataka Jnana Aayoga

PROCEEDINGS OF THE GOVERNMENT OF KARNATAKA

Subject: Reconstitution of Karnataka Knowledge Commission.

Read:

Preamble:-

Karnataka has emerged as the Knowledge Capital of the country. The State needs to take on the global challenges in terms of innovation, conservation of heritage, generation of new knowledge, application of knowledge in every sphere of life, skill development, enhancement of competencies, creation of better human capital to create new knowledge economy besides creation of a more human society. Keeping that in view, the Karnataka Knowledge Commission was constituted in 2008, vide Government Order No: ED 110 URC 2008, dated 5-9-2008 read at (1) above, under the guidance and Chairmanship of renowned Space Scientist Dr. K. Kasturirangan. After completion of term. The Commission was reconstituted and the term was extended till December 28, 2013 vide G.O. read at (2) above. Further, the term of the Commission was extended for 03 years vide Notification read at (3) above. Subsequently, the Commission was re-constituted under the Chairmanship of Dr. K. Kasturirangan vide Government Order No. ED 354 URC 2016 (Part-1) dated 02-8-2017 read at Sl.No.4 above.

The State Government has duly considered the necessity of Knowledge Commission in addressing the key aspects of development of the State with Knowledge and techno – managerial recommendation and advice. Consequently, after taking the role to be played by the Karnataka Knowledge Commission in making Karnataka a Knowledge State and a knowledge economy, in to account, the Government aptly decides to reconstitute Karnataka Knowledge Commission Hence the following order.


In the circumstances explained above, the Government is pleased to reconstitute the Karnataka Knowledge Commission with the following eminent persons as Chairman and Members.
<table>
<thead>
<tr>
<th>Sl.No</th>
<th>Name and Address</th>
<th>Designation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Dr. K. Kasturirangan, Former Chairman of ISRO, Ex-Member (Science), Planning Commission, Gol, Emeritus Professor, National Institute of Advanced Studies, Bengaluru</td>
<td>Chairman</td>
</tr>
<tr>
<td>2</td>
<td>Dr. Mukund Kadursrinivas Rao, Adjunct Professor, NIAS and Head of NIAS Centre for Spatial Analytics and Advanced GIS, NIAS, IISc Campus, Bengaluru</td>
<td>Member - Secretary</td>
</tr>
<tr>
<td>3</td>
<td>Sri. P.G.R. Sindhia, Former Minister for Home, Transport and Finance, Government of Karnataka</td>
<td>Member</td>
</tr>
<tr>
<td>4</td>
<td>Sri. Mohandas Pai T V, President, MEMG International India Ltd. No. 70, 4th Floor, Grace Towers, Above Navaneeth Motors, Milers Road, Bengaluru – 560052</td>
<td>Member</td>
</tr>
<tr>
<td>5</td>
<td>Prof. Anurag Behar, Vice Chancellor, Azim Premji University, PES Institute of Technology Campus Pixel Park, B’ Block Electronic City Hosur Road, Bengaluru</td>
<td>Member</td>
</tr>
<tr>
<td>6</td>
<td>Prof. M. R. Satyanarayana Rao, Ex - Director, Jawaharlal Centre for Advanced Scientific Research (J.N.C.A.S.R), Jakkur, Bengaluru - 560064</td>
<td>Member</td>
</tr>
<tr>
<td>7</td>
<td>Dr. Nazeer Ahmed, Advisor, World Organization for Research Development and Education, Ex-Scientist, NASA, No. 4, 9th Cross, Jayamahal Main Road, Jayamahal Extension, Bangalore – 560046</td>
<td>Member</td>
</tr>
<tr>
<td>8</td>
<td>Prof. Sunney Tharappan, Director, C.L.H.R.D, Valencia Circle, Mangalore – 575002</td>
<td>Member</td>
</tr>
<tr>
<td>9</td>
<td>Prof. G. Padmanabhan, Former Director of IISc, Bangalore – 560012</td>
<td>Member</td>
</tr>
<tr>
<td>10</td>
<td>Dr. Gayatri Saberwal, Academic Dean, Institute of Bioinformatics and Applied Biotechnology, Biotech Park Electronics City Phase I, Bangalore – 560100</td>
<td>Member</td>
</tr>
<tr>
<td>11</td>
<td>Prof. S. Sadagopan, Director, IIIT-Bangalore, 26/C, Electronics City, Hosur road, Bangalore – 560100</td>
<td>Member</td>
</tr>
<tr>
<td>12</td>
<td>Dr. Devi Prasad Shetty, Heart Specialist, Narayana Hrudayalaya, 258/A, Bommasandra Industrial area, Anekal Taluk, Bangalore – 560099</td>
<td>Member</td>
</tr>
<tr>
<td>No.</td>
<td>Name</td>
<td>Designation</td>
</tr>
<tr>
<td>-----</td>
<td>----------------------------------------------------------------------</td>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td>13</td>
<td>Dr. Rajashekar H. B,</td>
<td>Member</td>
</tr>
<tr>
<td></td>
<td>Director</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Dr. B.M. Hegde,</td>
<td>Member</td>
</tr>
<tr>
<td></td>
<td>Ex-Vice Chancellor</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Dr. P. Balakrishna Shetty,</td>
<td>Member</td>
</tr>
<tr>
<td></td>
<td>Vice Chancellor</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>Dr. Mohan Alva,</td>
<td>Member</td>
</tr>
<tr>
<td></td>
<td>Chairman</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>Dr. B N Suresh,</td>
<td>Member</td>
</tr>
<tr>
<td></td>
<td>Vikram Sarabhai Professor</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>Sri. S V Ranganath,</td>
<td>Member</td>
</tr>
<tr>
<td></td>
<td>Retd.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>Smt. Ashwini Nachappa,</td>
<td>Member</td>
</tr>
<tr>
<td></td>
<td>Retd. IAS &amp; Chief Secretary</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>Dr. Pulak Ghosh,</td>
<td>Member</td>
</tr>
<tr>
<td></td>
<td>Professor</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>Prof. K.E. Radhakrishna,</td>
<td>Member</td>
</tr>
<tr>
<td></td>
<td>Academician</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>Prof. Basavarajappa K. P.,</td>
<td>Member</td>
</tr>
<tr>
<td></td>
<td>Former Research Fellow, IIM-B, No. 120, 2nd Main, KUS Layout</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(Next to National Law School of India University)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>Dr. S.R. Patil,</td>
<td>Member</td>
</tr>
<tr>
<td></td>
<td>Rtd. Professor &amp; Head</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>Dr. Angarai Ganeshan Ramakrishnan</td>
<td>Member</td>
</tr>
<tr>
<td></td>
<td>Professor &amp; Chairman</td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>Prof. O.V. Nandimuth,</td>
<td>Member</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

KJA Recommendation
### Ex-Officio Members

<table>
<thead>
<tr>
<th>Sl. No</th>
<th>Name and Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Additional Chief Secretary to Government, Finance Department, Government of Karnataka, Vidhana Soudha, Bengaluru-560001</td>
</tr>
<tr>
<td>2</td>
<td>Additional Chief Secretary to Government, Primary and Secondary Education Department, Government of Karnataka, 6th Floor, 2nd Stage, M.S. Building, Bengaluru-560001</td>
</tr>
<tr>
<td>3</td>
<td>Additional Chief Secretary to Government, Medical Education Department, Government of Karnataka, 6th Floor, 4th stage, MS Building, Bengaluru-560001</td>
</tr>
<tr>
<td>4</td>
<td>Principal Secretary to Government, Higher Education Department, Government of Karnataka, 6th Floor, 2nd Stage, MS Building, Bengaluru-560001</td>
</tr>
<tr>
<td>5</td>
<td>Principal Secretary to Government, Health and Family Welfare Department, Government of Karnataka, # 105, 1st Floor, Vikasa Soudha, Bengaluru-560001</td>
</tr>
<tr>
<td>6</td>
<td>Principal Secretary to Government, Information Technology, Bio Technology and Science &amp; Technology Department, Government of Karnataka, 5th Floor, 5th stage, M.S Building, Bengaluru-560001</td>
</tr>
</tbody>
</table>
Term of Reference:-

The Commission shall strive to give recommendations in the following areas.

1. To focus on institution building, policy innovation and excellence in the field of education, health, science and technology, industry, entrepreneurship, research and innovation, traditional knowledge, agriculture, e-governance, rural development, etc., and other relevant areas in the context of Karnataka.

2. Build excellence in the educational system to meet the challenges of the 21st century and increase Karnataka’s competitive advantage in the fields of knowledge.

3. Promote creation of knowledge in all formal and non-formal educational, scientific and Knowledge institutions of Karnataka.

4. Improve the leadership and Management of educational and knowledge institutions of Karnataka.

5. Promote knowledge applications in agriculture, rural development, health, industry and other areas.

6. Enhance the use of knowledge capabilities in making government an effective service provider to the citizen and promote widespread sharing of knowledge to maximize public benefit.

7. Promote inter sectoral interaction and interface with the objective of preservation, access, new concepts, creation, application, dissemination, outreach and services relating to knowledge.

8. Develop appropriate institutional frameworks to strengthen the education system, promote domestic research and innovation, facilitate knowledge application in various sectors.

9. Leverage information and communication technologies to enhance governance improve connectivity and reduce digital divide.

10. Device mechanisms for exchange and interaction between knowledge System in the global arena.

11. Conserve indigenous and heritage knowledge in Karnataka for better Utilization of time tested concepts and knowledge by society.
By Order and in the name of the Governor of Karnataka

Sd/-
(M.A. AHAMED JHON)
Under Secretary to Government
Higher Education Department (Universities-2)

To,

The Complier, Karnataka Gazette -for publication in next issue of the Gazette.

Copy to:
1. Dr. K. Kasturirangan, Former Chairman, ISRO and Former Member (Science), Planning Commission, Government of India. Director, National Institute of Advanced Studies, Bengaluru
2. The Vice Chairman, Karnataka State Council for Higher Education, Bengaluru.
3. The Vice Chancellors/Registrars of All Universities.
4. The Executive Director, Karnataka State Council of Higher Education, Bengaluru.
5. Dr. Mukund Kadursrinivas Rao, Adjunct Professor, and Head, NIAS Centre for Spatial Analytics and Advanced GIS, Bengaluru
7. Sri. Mohandas Pai T V, President, MEMG International India Ltd., No. 70, 4th Floor, Grace Towers, Above Navaneeth Motors, Milers Road, Bengaluru - 560052
8. Prof. Anurag Behar, Vice Chancellor, Azim Premji University, PES Institute of Technology Campus Pixel Park, B’ Block Electronic City Hosur Road, Bengaluru
12. Prof. G. Padmanabhan, Former Director of IISc, Emeritus Professor Department of Biochemistry, Indian Institute of Science Bangalore – 560012.
14. Prof. S. Sadagopan, Director, IIT-Bangalore, 26/c, Electronics City, Hosur road, Bangalore – 560100
15. Dr. Devi Prasad Shetty, Heart Specialist, Narayana Hrudayalaya, 258/A, Bommasandra Industrial area, Anekal Taluk, Bangalore – 560099.
16. Dr. Rajashekar H B Director, Jawaharlal Nehru Medical College, JNMC Campus, Nehru Nagar, Belgaum – 590010.
17. Dr. B.M. Hegde, Ex-Vice Chancellor, Manipal University, Ganesh Lower Bendur, 2nd Cross, Mangaluru -575702.
19. Dr. Mohan Alva, Chairman, Alva Education Society, Vidyagiri, Moodbidri, Dakshina Kannada Dist – 574 227.
20. Dr. B N Suresh, Vikram Sarabhai Professor, ISRO Hqs, Antariksh Bhavan, New BEL Road, Bengaluru-560 231
21. Shri. S V Ranganath Retd. IAS & Ex- Chief Secretary, Vice-Chairman, Karnataka State Higher Education Council, GOK
23. Dr. Pulak Ghosh, Professor, IIM-Bengaluru, Bengaluru, Bannerughatta Road, Bengaluru-560076.
24. Prof. K.E. Radhakrishna, Academician, J C Nagar, Mahalakshmpuram, Bengaluru.
25. Prof. Basavarajappa K P, Professor, IIM Bengaluru, Bannerughatta Road, Bengaluru-560076.
26. Dr. S.R. Patil M. A. Ph.D, Professor of Geography, (Retd) Department of Geography, Karnataka University, Dharwad
27. Dr. Ramakrishnan Angarai Ganeshan Ph.D,(Bio-Medical Engineer), Department of Electrical Engineering, IISc, Bengaluru
28. Prof. O.V. Nandimath, Professor of Law & Registrar, NISLU, Bengaluru
29. Dr. Radha Murthy, Director, Nightingales Home Health Services and the Nightingales Medical Trust, Bengaluru
30. Dr. C.N. Manjunath, Professor & Head of Cardiology Director, Sri Jayadeva Institute of Cardiovascular, Science & Research,9th Block Jayanagar, Bannerghatta Road, Bengaluru - 560069
31. Dr. M.K. Shankaralinge Gowda, IAS (Rtd),Ex-Chairman, Karnataka Electricity Regulatory Commission,E-79, 6th A Cross, Manyata Residency Behind Manyata Tech-Park,Hebbal Ring Road, Bengaluru -560045.
32. Prof. S.N. Hegde, Vice- Chancellor (Rtd), Chairman, Vishranti Kulapatigala Vedike.
33. Sri. P.N. Nayak,Rtd., Chief Engineer, No. 202, Yadugiri Next Appartment, 11th Main Road, 14th Cross, Malleshwaram, Bengaluru – 560003.
34. PS to Chief Secretary to Government of Karnataka, Vidhana Soudha, Bengaluru.
35. PS to Additional Chief Secretary to Government of Karnataka, Vidhana Soudha, Bengaluru.
36. PS to Additional Chief Secretary & Development Commissioner to Government of Karnataka, Vidhana Soudha, Bengaluru.
37. PS to Additional Chief Secretary to Hon’ble Chief Minister, Government of Karnataka, Vidhana Soudha, Bengaluru.
38. PS to Hon’ble Higher Education Minister, Government of Karnataka, Vidhana Soudha, Bengaluru.
39. PS to Additional Chief Secretary to Higher Education Department, Government of Karnataka, Multi storied Building, Bengaluru.
40. PS to ALL Additional Chief Secretaries/Principal Secretaries/Secretaries, Government of Karnataka, Bengaluru.
41. SGF/Spare Copies

****

****