THE CENTRE FOR internet & society

Cybersecurity Compendium

INDIAN CONTEXT

AUTHOR **Leilah Elmokadem**
EDITOR **Elonnai Hickok**

The Centre for Internet and Society, India

Designed by **Anisha Baid** and **Saumyaa Naidu**

1.0 Introduction

This document intends to serve as a comprehensive source compiling all the cyber-security related regulations, policies, guidelines, notifications, executive orders, court rulings, etc. Ultimately, it attempts to collect all the cyber security initiatives that have been put out by Indian regulatory bodies and organizations. To approach this end, we identified they actors and institutions in cyber security and record their published guidelines, frameworks, ongoing projects and any policies released to strengthen cyber security. We have mostly followed a general framework in which, for each document found, we indicate the definition of cyber security (if stated), the objectives, recommendations/guidelines and scope. This format was sometimes difficult to follow for some types of initiatives in the documents. For example, a document of questions and answers to parliament could not be recorded in this fashion. As a result, the document is not entirely uniform in structure. This research compendium is in continuous progress, expanding along with the base of our knowledge and ongoing research.

POLICY

PUBLICATION

PRESS RELEASE

QUESTION FROM PARLIAMENT

INITIATIVE

TECHNOLOGICAL SOLUTION

DIVISION

LEGISLATION

R & D DIVISION

This document uses the following icons from the **Noun Project**
Gavel created by **www.yugudesign.com**
Book created by Thomas Helbig
Newspaper, Presentation, created by **Gregor Cresnar**
Government created by **Rflor**

	Types of Documents								
Government Regulatory Bodies and Organizations	Policy	Publication	Press Release	Question from Parliament	Initiative	Technological Solution	Division	Legislation	R & D Division
2.0 Ministry of Communication and Information Technology & Department of Electronics and Information Technology	2	1	1	9	1	-	-	-	-
3.0 Data Security Council of India (DSCI)	1	4	1	-	9	1	1	-	-
4.0 Ministry of Law, Justice and Company Affairs (Legislative Department)								1	
5.0 C-DAC (Centre for Development of Advanced Computing)		2			2	7	1		
6.0 DoT (Department of Telecommunications)						1			
7.0 CERT-In (Indian Computer Emergency Response Team)	1	1					1		
8.0 RBI (Reserve Bank of India)	5	1	1				1		1
9.0 SEBI (Security and Exchange Board of India)		1							
10.0 National Critical Information Infrastructure Protection Centre National Technical Research Organization Government of India (NCIIPC)	1	3							
11.0 Information Technology, Electronics & Communications Department of Telangana Government	1								
12.0 Ministry of Electronic and Information Technology (Meity)	1			6	4	1	2		
13.0 National Institute of Electronics and Information Technology (NIELIT)					4				
14.0 Ministry of Defence, Government of India		2		7					
15.0 Ministry of Home Affairs, Government of India		2		3	2				
16.0 Ministry of External Affairs		1		1					
17.0 Central Electricity Authority (CEA)	1								
18.0 Central Bureau of Investigation (CBI)		1			2		2		
19.0 Association of Unified Telecom Service Providers of India (AUSPI)					1				

	Types of Documents								
Government Regulatory Bodies and Organizations	Policy	Publication	Press Release	Question from Parliament	Initiative	Technological Solution	Division	Legislation	R & D Division
20.0 Ministry of Petroleum and Natural Gas	1								
21.0 Central Electricity Regulatory Commission		1							
22.0 Controller of Certifying Authorities (CCA)	2	1						1	
23.0 Centre for Development of Telematics (CDoT)		1				1			
24.0 Ministry of Finance	1			4					
25.0 National Payments Corporation India	3	1					1		
26.0 Electronics and Information Technology Department Government of Odisha	1			-				-	-
27.0 National Technical Research Organization (NTRO)							1		

2.0 Ministry of Communication and Information Technology & Department of Electronics and Information Technology

2.1 Cyber Security Policy (2013)

2.2 Security measures to be adopted in ADSL Modems to safeguard against misuse

2.3 Cyber Crime, Cyber Security and Right to Privacy: 52nd Report

2.4 Press Release: Cyber Security Threat (March 6th 2013)

2.5 Lok Sabha Starred Question no 153; 04.05.16: Cyber Security

2.6 Lok Sabha Unstarred Question no. 2856; 16.12.15: Cyber Security Command

2.7 Lok Sabha Unstarred Question no. 6630; 06.05.15: Collaboration on Cyber Security

2.8 Lok Sabha Unstarred Question no. 6471; 06.05.15: Cyber Security Under Digital India

2.9 Lok Sabha Starred Question 135; 04.03.15: Cyber Security Cooperation

2.10 Lok Sabha Unstarred Question no. 1795; 03.12.14: Cyber Security

2.11 Lok Sabha Unstarred Question no. 74; 24.11.14: National Cyber Security Centre

2.12 Lok Sabha Unstarred Question no. 2647; 28.07.14: Upgradation of Cyber Security

2.13 Lok Sabha Unstarred Question no. 14; 07.07.14: Upgradation of Cyber Security

2.14 STQC Initiative: Common Criteria

2.1 Cyber Security Policy (2013)

2.1.1 Objectives

- To build a secure and resilient cyberspace for citizens, businesses and government
- To protect information and information infrastructure in cyberspace
- To build capabilities to prevent and respond to cyberthreats
- To reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, process, technology and cooperation
- To create a secure cyber ecosystem in the country, generate adequate trust and confidence in IT systems and transactions in cyberspace and thereby enhance adoption of IT in all sectors of the economy
- To create an assurance framework for design of security policies and for promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment
- To strengthen the regulatory framework for ensuring secure cyberspace ecosystem
- To enhance and create national and sectoral level 24x7 mechanisms for obtaining strategic information regarding threats to ICT infrastructure, creating scenarios for response, resolution and crisis management through effective predictive, preventive, protective, response and recovery actions
- To enhance the protection and resilience of national critical information infrastructure by operating a 24/7 National Critical Information Infrastructure Protection Centre (NCIIPC) and mandating security practices related to the design, acquisition, development, use and operation of information resources
- To develop suitable indigenous security technologies through frontier technology research, solution oriented research, proof of concept, pilot development, transition, diffusion and commercialisation leading to widespread deployment of secure ICT products/ processes in general and specifically for addressing national security requirements
- Improve visibility of the integrity of ICT products and services by establishing infrastructure for testing and validation of security of such products
- To create a workforce of 500,000 professionals skilled in cybersecurity in the next 5 years through capacity building, skill development and training
- To provide fiscal benefits to businesses for adoption of standard security practices and processes
- To enable protection of information while in process, handling, storage, and transit so as to safeguard privacy of citizens' data and for reducing economic losses due to data theft or cyber crime
- To enable effective prevention, investigation and prosecution of cybercrime and enhancement of law enforcement capabilities through appropriate legislative intervention
- To create a culture of cybersecurity and privacy enabling responsible user behaviour and actions through an effective communication and promotion strategy
- To develop effective public private partnerships and collaborative engagements through technical and operational cooperation and contribution for enhancing the security of cyberspace
- To enhance global cooperation by promoting shared understanding and leveraging relationships for furthering the cause of security of cyberspace

2.1.2 Recommendations/Regulations/Guidelines

- Creating a secure cyber ecosystem
- Creating an assurance framework
- Encouraging open standards
- Strengthening the regulatory framework
- Creating mechanisms for security threat early warning, vulnerability management and response to security threats
- Securing e-governance services
- Protection and resilience of critical information infrastructure
- Promotion of research and development in cyber security
- Reducing supply chain risks
- Human resource development
- Creating cyber security awareness
- Developing effective public private partnerships
- Information sharing and cooperation

- Adopting a prioritized approach for implementation
- Operationalization of the policy

2.1.3 Scope

- Industries in which organizations rely heavily on IT and cloud-based information storing
- Organizations with large cyber spaces used to store data

2.2 Security measures to be adopted in ADSL Modems to safeguard against misuse

2.2.1 Objectives

- To address vulnerability in ADSL Modems by all ISPs
- These vulnerabilities can be exploited by attackers to implant malwares in modems, change configuration or manipulate data etc.

2.2.2 Recommendations/Regulations/Guidelines

- The customer must changed to a strong password at time of installation of modem at customer site, to avoid unauthorized access to modem. The ISP executive visiting the customer for installation should ensure the completion of this step.
- The protocol ports in ADSL modem on WAN side (e.g. FTP, TELNET, SSH, HTTP, SNMP, CWMP, UPnP) be disabled
- There should be a mechanism to upgrade firmware of the ADSL modems remotely by ISPs. So ISPs must have a separate login password, which is not possible in the present system of ADSL modem design. ISP should advise the customer to upgrade/download the latest firmware and software for their modem by visiting the site of the manufacturer's website or from their website in case of ISP supplied ADSL modems
- ISPs should explore the possibility of having separate user ID and password for Lan and WAN with vendors for future supplies along with other necessary security features in ADSL modems
- When a reset button of a modem is operated, all configuration settings in ADSL modem should be reset to factory default settings, resulting in the resetting of modem login and password to default admin and admin respectively. Customer should change the default password again to earlier password or another password.
- The customer should switch off their ADSL modem when not in use
- The customer should check online his/her daily usage. If any unexpected high usage of data is noticed, he may bring in the notice of ISP concerned

2.2.3 Scope

- These recommendations would apply to the ISPs of internet service providers
- Somewhat apply to internet consumers as well since they must cooperate with some of these recommendations to achieve the purpose of modem security

2.3 Cyber Crime, Cyber Security and Right to Privacy: 52nd Report

2.3.1 Objectives

- The report makes observations and direct recommendations at the Department of Electronics and Information Technology
- Since cyber security is a complex issue that cuts across domains and national boundaries and makes it difficult to attribute the origin of cyber attacks, this report intends to take a strategic and holistic approach requiring multi-dimensional and multi-layered initiatives and responses
- The report discusses a wide array of risks associated with lack of user end discipline and inadequate protection of computer systems
- The report also discusses types of cybercrime/attacks, their methodology and impacts as well as growing incidents of cyber crime and financial loss
- The report covers the roles of different government departments in the field of strengthening cyber security
- The report addresses the lack of adequate human resource to tackle the challenge (auditors, experts, skill development in IT) and explores infrastructure and research development's role in securing cyberspace
- The report makes budgetary allocations to tackle the cyber threats

- It also brings attention to threats emerging from servers hosted outside india and the challenges posed by imported electronics/IT products
- The report discusses the role of upcoming technology viz. Cloud computing etc
- It also discusses the role of CERTiN and other organizations/ departments and the importance of MoUs and international treaties to secure cyber space
- Provides an assessment of the preparedness of the government and policy initiatives for securing cyber spaces
- The report overviews the Cyber Crisis Management Plan (CCMP), the National Cyber Security Policy (NCSP 2013), and the Information Technology Act, 2000
- The report looks at cyber security with respect to the right to privacy
- It also emphasizes the importance of a Monitoring and Grievance Redressal Mechanism and a Cyber Appellate tribunal
- The report highlights the importance of education and awareness

2.3.2 Recommendations/Regulations

- The department should put the proposed agenda of 24x7 National Critical Information Critical Infrastructure protection centre, which aims to protect the critical information infrastructure in the country, on top priority and implement its cyber security programmes expeditiously so that any kind of cyber attack have no impact on functioning of critical sectors
- There should be one single, centralised cell/agency to deal with all cases of cyber crime/threat in the country. This will help the department in knowing patterns of crime but also prevent the recurrence of the same crimes with newer strategies
- The department should take necessary steps in identifying the reasons for all government departments/organizations for not following the information security best practices and urge upon them to expeditiously obtain ISO 27001 certification to enable them to adhere to information security practices
- The department should make concerted efforts to increase the number of cyber security experts/auditors/IT skill in the country on top priority basis so as to ensure that shortage of manpower does not come in the way of securing indian cyber space
- The department should immediately take necessary steps for optimum utilisation of funds under R&D in cyber security and also facilitate research in strategic technology. The department should also facilitate in design for programmes for development/ enhancement/promotion of skills/expertise for R&D in cyber security
- The department should take concrete initiatives in setting up the cyber-crime cells and labs in states where these do not exist and also upgrade and strengthen the existing cyber crime cells with adequate fund and infrastructure so as to cope up with the rapid cyber threat and privacy infringement
- The department should have a stringent measures to safeguard the indigenous servers as most of the cyber attacks are ".in" domain.
- The department should lay down provisions for mandatory certification for all imported electronics/it/telecom products and have certification centres in each state/UT specifically at all airports/ naval docks/international borders
- The department should conduct a study/survey to find out the instances of cyber security breaches in NeGP projects
- The department should redouble their efforts in making india a pioneering country for the cause of cyber jurisprudence
- CCMP should be frequently reviewed and revised so as to keep pace with the rapid changing nature of cyber threats the department should take
- The department should be prepared to amend the IT act to suit emerging cyber threats
- The Department in coordination with the Department of Personnel and Training, multi-disciplinary professionals/experts should come out with a comprehensive and people friendly policy which may protect the privacy of citizen and is also foolproof from security point of view
- The department to take remedial measures and come out with a policy which should be implemented stringently so as to obviate recurrence of cyber instances
- The department should have a mandatory cyber-crime cell not only in each state but also in each district and block.
- Should also have a centralized system/cell for monitoring cyber-crime

which would have real-time details of registration and disposal status of cyber-crime throughout the country

- The department to deploy adequate manpower ASAP so that appeals that are pending for hearing in the tribunal are disposed of expeditiously
- The department should implement their initiated project “National eSecurity Index” ASAP
- The department should take necessary action in coordination with concerned authorities to make the curriculum of cyber security mandatory in school syllabi

2.3.3 Scope

- The report targets the Department of Electronics and Information Technology

2.4 Press Release: Cyber Security Threat (March 6th 2013)

- A sophisticated virus called “Stuxnet”, targeting Industrial Control Systems, was reported to be spreading worldwide since july 2010
- The steps taken by the government immediately after the threat was reported:
    - Alerts and advisories about Stuxnet threat were issued on website of the indian computer emergency response team (CERT-in).
    - Measures to be taken to detect infected systems, disinfect the same and prevent further propagation were advised to all critical sector organizations in india.
    - Government in association with Internet Service Providers (ISPs) and security vendors tracked the infected systems and advised the owners of the systems to disinfect the same. Workshops conducted by CERT-In and other government agencies jointly for critical sector organizations to create awareness and suggest steps to be taken to counter the threat
- The government has also taken the following steps to protect cyber networks:
    - Department of information Technology and Electronics has circulated computer security guidelines and cyber security policy to all the ministries/departments on taking steps to prevent, detect and mitigate cyber attacks
- All Central Government Ministries/ Departments and State/Union Territory Governments have been advised to conduct security audit of entire Information Technology Infrastructure, including websites, periodically to discover gaps with respect to security practices and take appropriate corrective actions.
- Government called for setting up Early Warning and Response to cyber security incidents through the Indian Computer Emergency Response Team (CERT-In) and to have collaboration at national and international level for information sharing and mitigation of cyber attacks. CERT-In regularly publishes Security Guidelines and advisories for safeguarding computer systems and these are widely circulated. CERT-In also conducts security workshops and training programs on regular basis to enhance user awareness.
- The ‘Crisis Management Plan for countering cyber attacks and cyber terrorism’ was prepared and circulated for implementation by all Ministries/ Departments of Central Government, State Government and their organizations and critical sectors.
- CERT-In is conducting mock cyber security drills to enable assessment of preparation of organizations to withstand cyber attacks.
- The Information Technology Act, 2000 as amended by the Information Technology (Amendment) Act, 2008 has been enforced on 27.10.2009. The Act provides legal framework to address the issues connected with security breaches of information technology infrastructure.
- National Informatics Centre (NIC) managing Govt. websites and providing e-mail service is implementing measures to secure the Govt. IT infrastructure from cyber attacks.

2.5 Lok Sabha Starred Question no 153; 04.05.16: Cyber Security

Questions

- Whether there is a lack of expertise in handling the cyber security cases in the country and if so, the details thereof and the steps taken by the Government for enhancing the same;

- Whether the Government has collaborated with other institutions for strengthening the cyber security and if so, the details thereof;
- Whether cyber security mock drills were conducted at National and international level by various agencies and if so, the details and outcome thereof; and
- The steps taken/being taken by the Government to create cyber security awareness in the country?

Answers

- See detailed answers *here*

2.6 Lok Sabha Unstarred Question no. 2856; 16.12.15: Cyber Security Command

Questions

- Whether the Government is planning a cyber security command to facilitate manufacture of electronic products in the country;
- If so, the details thereof;
- Whether the Government is planning a policy of manufacturing all electronics in the country; and
- If so, the details thereof and the time by which the said policy is likely to be implemented?

Answers

- See detailed answers *here*

2.7 Lok Sabha Unstarred Question no. 6630; 06.05.15: Collaboration on Cyber Security

Questions

- Whether a strategic collaboration on cybersecurity is being worked out between India and Japan
- If so, the details thereof and
- Whether National Security Council proposes public-private partnership for cybersecurity by setting up a permanent joint working group, multi-disciplinary centers of excellence etc and if so, the details thereof
- Whether a japanese company has initiated dialogue with the Government and public sector to set up an academy to build capabilities for cybersecurity in the country and;
- If so, the details thereof?

Answers

- See detailed answers *here*

2.8 Lok Sabha Unstarred Question no. 6471; 06.05.15: Cyber Security Under Digital India

Questions

- Whether the existing cybersecurity framework commensurate with the latest technology that will be developed and implemented under the Digital India project
- If not, whether the government has considered any measures to strengthen cyber security vis-a-vis the Digital India project; and
- The details of the recent updates made to the Indian cyber security framework from the policy and legislative perspective?

Answers

- See detailed answers *here*

2.9 Lok Sabha Starred Question 135; 04.03.15: Cyber Security Cooperation

Questions

- Whether the government proposes to create sub-working groups to assess opportunities, institutions and mechanisms of cooperation with the European Union (EU) on cyber and telecom security and if so, the details thereof
- Whether the the government proposes joint R&D apart from partnership in 5G development programme and if so, the details thereof

- Whether the government is seeking investment in telecom test labs from foreign agencies and EU since they have better technical know-how, if so, the details thereof and the progress made in this regard so far?

Answers

- See detailed answers *here*

2.10 Lok Sabha Unstarred Question no. 1795; 03.12.14: Cyber Security

Questions

- Whether the Indian cyberspace, particularly the sensitive establishments are prone to cyber attacks by cyber criminals of hostile nations;
- If so, the details thereof and whether Government proposes to set up Cyber intelligence body or Cyber Regulatory Advisory committee
- If so, the terms of reference of the said body along with the financial outlay made for the purpose;
- The time by which the said committee is likely to be functional
- The strategy/cyber security policy of the government on cyber attacks?

Answers

- Please see detailed answers *here*

2.11 Lok Sabha Unstarred Question no. 74 ; 24.11.14: National Cyber Security Centre

Questions

- Whether the government has been actively considering to set up National Cyber Security and Coordination Centre to check cyber threats in the country
- If so, the details thereof
- Whether the government has sought the views of the various intelligence and security agencies to set up National Cyber Security and Coordination Centre;
- If so, the details thereof; and
- The extent to which it would be benefited in the event of cyber attack?

Answers

- See detailed answers *here*

2.12 Lok Sabha Unstarred Question no. 2647 ; 28.07.14: Upgradation of Cyber Security

Questions

- Whether the government has prepared an elaborate plan to upgrade cyber security capabilities in the Country;
- If so, the details thereof
- Whether the Government has any proposal to have qualified IT Experts to deal with cyber attacks in the country;
- If so, whether the government is also considering to setup dedicated Computer Emergency Response Team for critical sectors such as power, aviation etc. where no such national monitoring mechanism exists in the country and if so, the measures taken in this regard and
- The steps taken by government to monitor and scan critical networks and stepup up security levels for networks?

Answers

- See detailed answers *here*

2.13 Lok Sabha Unstarred Question no. 14 ; 07.07.14: Upgradation of Cyber Security

Questions

- Whether the government has recently announced a policy to address the increasing cyber security threat in the country;
- If so, the details thereof including the proposed structure of the agencies; and

- The manner in which it would coordinate with the existing multiple agencies that are required to counter this threat including local law enforcement agencies in the country?

Answers

- See detailed answers *here*

2.14 STQC Initiative: Common Criteria

- STQC as part of Cyber Security Assurance Program, established a Certification Body and Test Lab for evaluation & certification of IT products
- This initiative is under National Security Architecture of National Security Council Secretariat
- Cabinet Committee on Security on 8th May, 2013 approved the setting up of National Certification Body as an integral part of the " Framework for Enhancing Cyber Security of Indian space"
- Products tested and certified under Indian Common Criteria Certification Scheme (I3CS) up to EAL 4 would be acceptable in other member countries of CCRA without the need for further testing.
- Participating in CCRA allows India to be a part of the global process of deciding the security standards incorporating the national requirements and protecting the interest of the local developer and user organizations.
- This also enables Indian assessors to participate in CCRA Assessment of different member countries. This would ensure exposure of Indian assessor in benchmarking their process w.r.t internal best practices for continued effectiveness.

3.0 Data Security Council of India (DSCI)

3.1 Security Strategy Policy (SSP)

- Proactive initiative to devise a defense plan of organizations against the evolving security threats, addressing multiple dimensions for structured, effective and efficient defense
- Organization’s responsibility to ensure cyber safety

3.1.1 Defining Cyber Security

- Not explicitly defined
- Used interchangeably with: information security and data security

3.1.2 Objectives

- Objectives of information security: confidentiality, availability, integrity, with demonstrated accountability and assurance
- a mechanism that monitors compliance to the policy and assesses the

3.1.3 Recommendations/Regulations/Guidelines

- Plan and develop security countermeasures across all layers of infrastructure, including network, server, systems, endpoints, application infrastructure, messaging, databases, etc
- Cyber security for electronic banking
- Organizations must have complete and dynamic visibility over all their cyber activities that require security attention
- Must have a mechanism to evaluate sensitivity and criticality of business functions, services and processes
- Organizations must have a complete visibility and understanding of its security posture and has a program for assessing the security posture and has a program for assessing the security posture regularly
- Security preparedness of the organization is regularly evaluated to provide inputs for the strategic initiative for security
- Security solutions are derived from well-devised security architecture of the organization
- Developing security intelligence that collaborates with the external and internal information sources
- Frequently communicate management’s commitment towards the policy to employees, partners and service providers
- Non-compliances to the policy are identified and addressed in a timely manner, and everyone clearly understands the consequences for non compliance

3.1.4 Scope

- Organizations that rely on information technology for operation
- Organizations that store data in cloud/cyber spaces

3.2 MoU with CBI to Fight Cyber Crime

- MoU reaffirms DSCI’s objective of strengthening abilities of law enforcement officials in combating cyber crimes
- Establishes collaboration between law enforcement agencies through CBI, Cyber and Hi-Tech crime investigation and Training Centre (CHCIT) and the IT industry through DSCI
- Aimed at spreading awareness on the security standards, sharing best practices amongst various enforcement agencies globally, collaborating with global think tanks, finding solutions to emerging challenges in cyber crime prevention, detection, investigation and prosecution and enabling the stakeholders in their ability to educate and update themselves on cybercrime investigations leading to data protection
- CHCIT Centre to serve as a networking platform and DSCI to act as a knowledge partner for the CBI in the cyber security areas
- Through the MoU, DSCI will facilitate, guide and ensure the active involvement in bringing out latest compendium of best practices from across the world and help CBI in fighting cybercrimes in the country
- DSCI to help in capacity building and create a pool of instructors who can train the officers to investigate cases involving cybercrimes that have national and global ramifications

3.3 Proposal for “Cyber crime Awareness Workshop for Law Enforcement Agencies” (LEA) -- phase -- II

- The workshop seeks to provide awareness to public prosecutors, judiciary, adjudicating officers and fraud/vigilant officers of user companies of banks, telecom, etc
- It was implemented by Data Security Council of India (DSCI) New Delhi

3.4 Cyber-crime Awareness Workshop for Law Enforcement Agencies (LEA) - Phase III

- The workshop aims to create awareness among Law Enforcement Officers of the states on investigating cyber crimes, towards which 12 cybercrime awareness workshops would be carried out in states where such awareness is lacking
- It was implemented by DSCI New Delhi

3.5 Development of Robust and Generic Model of e-Security Index

- The initiative is to develop robust and generic model of e-security index with carefully selected parameters and with adjustable weights assigned at every level where consolidation of scores takes place such as sub-index, area and parameter and sub-parameter level
- It was implemented by DSCI New Delhi

3.6 Annual Information Security Summit 2010 (5th summit)

3.6.1 Objective

- The summit's objective is to raise public, corporate and industrial involvement in raising awareness and developing best practices for data privacy and security

3.6.2 Key Areas of Discussion

- Data protection as a level for economic development through global integration of practices and standards conforming to various legal regimes
- Challenges faced by industries and government in securing operations to protect data and personal info of consumers and citizens
- The need to focus on cyber security and data protection separately
- Hosted an encryption session
- Discussed the DSCI's 5 year e-security strategy
- Discussed the principle of "security by design"

3.7 The Cybersecurity Agenda

3.7.1 Objective:

- To bring recommendations to build the legal, technical and administrative foundations for an international system to secure cyberspace

3.7.2 Key Focus Areas

- The importance of private-public partnerships for Cybersecurity
- The dangers of cyber crimes and cyber attacks to social and national security
- Cyber security challenges and policy considerations

3.8 NASSCOM Cyber Security Task Force (CSTF)

***Briefing Paper**: https://www.dsci.in/sites/default/files/NASSCOM%20CSTF_Briefing%20Paper_0.pdf*

3.8.1 Objective:

- To develop an action plan to build India as a global hub for providing CS solutions, developing CS R&D plan and develop skilled workforce of CS experts

3.8.2 Key Focus Areas:

- The Task Force has proposed setting up 4 working groups. For each group, these questions guide the general agenda:

Industry Development

- How can a conducive environment for cyber security products and services be created in the country?
- How can India be branded and positioned as a global hub for cyber security?
- What roles should different stakeholders play in this direction?
- How can the education and skill development initiatives be aligned with the industry requirements to build a competent and adequate workforce for the global market in the services sector?

Technology Development

- What are the key technology capabilities which India must have to adequately address cybersecurity risks?

- How can such capabilities be developed?
- How can Research & Development in cyber security be promoted in the country?
- How can government-industry-academia linkage be strengthened?
- What market development initiatives need to be undertaken in Government and Enterprise sectors for the emerging product ecosystem in India?

Skills Development

- How can India create the requisite workforce in cybersecurity to serve national as well as global requirements?
- How can capacity building of LEAs and judiciary be actualized?
- Given the demand for security expertise within the government, what mechanism can be created, to help government source expertise from the private sector?

Policy Development

- What policy initiatives are required in the country to establish India as a global hub for cyber security products & services, develop strategic capabilities and develop skills?
- How can policy help enhance trust between the government and private sector to enable better flow of ideas, manpower and funds?
- How can the implementation of existing cyber security policies and regulations be expedited?
- How can India enhance international cooperation in cyber security?
- How can internal consultation process to formulate national positions be strengthened?

3.9 Cybersecurity Delegation

- 39 representatives from the Central and State government, industry, user organizations and academia to attend tour to Hague Security Delta (Netherlands) and Malvern Cyber Security Cluster (UK) with the objective of opening opportunities for initiating long-lasting collaborations between the regions, helping in understanding the cluster ecosystem and implementing it in Indian cities, exploring avant-garde research, technologies and solutions in Cyber Security and establishing the Indian brand in global CS ecosystem.

3.10 MoU between DSCI, SSC NASSCOM and ISACA

3.10.1 Objective

- To address the Cyber Security Skills Shortage in India

3.10.2 Strategy

- Developing a long-term road map for CS skills development and borrowing capacity-building expertise from ISACA.
- Accelerate building a pipeline of qualified CS candidates who can skillfully protect their enterprise systems and data to inspire organization-wide confidence to innovate and improve overall business performance

3.11 Best Practices Meet on “Security Data Science”

3.11.1 Objective

- The event was held to facilitate discussion around the contemporary evolution of varied aspects of security: identifying the unique needs of information security professionals from diverse industry sectors and provide opportunity to undertake review of policy development, deliberations on global issues relating to security and privacy, and check the progress of CS industry development efforts

3.11.2 Key Focus Areas

- Security Innovation
- Privacy Workshop for Start-ups
- Industry consultation on “National Encryption Policy”
- “Cybercrime Incident Response Management”

3.12 IT Security Standards Working Group Meeting (Jaipur)

3.12.1 Objective

- The meeting comprised of 300+ experts deliberating on forging international standards on Privacy, Security and Risk management in IoT and Cloud Computing
- Participants gathered to discuss and collaborate on the development of standards, encompassing generic methods, techniques and guidelines to address both security and privacy issues
- This was held by DSCI in collaboration with the Bureau of Indian Standards (BIS)

3.12.2 Key Focus Areas

- Privacy
- Security
- Technology
- Security standards
- Collaboration

3.13 Cybersafe Pune 2009

3.13.1 Objective:

- To host a 3-day awareness campaign on cyber security for all stakeholders
- To advocate for public-private-partnership
- The event was an effort to educate users and make them aware of best practices
- The campaign focused on high impact areas like financial services, BPO sector, user community, child safety issues and rising Cyber Crime

3.13.2 Key Focus Areas

- Cyber safety
- Security issues
- Customers- industry
- Academia
- Stakeholders
- Best practices
- Preventative measures
- Information security

3.14 Building an Ecosystem for Cyber Security and Data Protection in India

3.14.1 Objective

- Setting up an ecosystem capable of understanding new age complexities and offering swift response mechanism, which requires a strong legal framework, contribution by industry and effective law enforcement mechanism

3.14.2 Key Focus Areas

- Cyber security ecosystem
- Legal framework
- Government initiatives
- Law enforcement
- Special projects
- Industry initiatives
- Government and industry partnership
- Protecting personal information

3.15 Cyber Security Research Developments: Global and Indian Context

3.15.1 Objective

- To provide an overview of existing initiatives in research and development in the field of Cyber Security

3.15.2 Key Focus Areas

- Cyber security
- Research developments
- User protection and education (CUPE)
- Technology evaluation and transition (CTET)

3.16 Cyber Labs

3.16.1 Objective

- To equip the Police or Prosecution or Judiciary with necessary capacities to deal with Cybersecurity and Cyber Crime Issues and Investigations.
- To create awareness among other stakeholders of the society about the threats of cyber crimes.
- To advise the IT industry in case of any cyber security breach or incident.
- To provide technical assistance in the investigation of cyber crimes.
- To promote establishment of e-Security Clubs in schools & colleges, to raise interest in information security among students

3.16.2 Strategy

- Promoting collaboration between the IT industry, academia and concerned citizens to address cybercrime and related issues.
- Creating Information Security infrastructure in collaboration with stakeholders, based on the 'Hub and Spokes' model.
- Developing pro-active strategies for predicting trends in cyber crime and formulating technical and legal responses on various fronts.
- Strengthening cyber crime investigation training among police officers.
- Developing cyber crime technology tools for criminal investigation.
- Enhancing awareness about cyber crime among citizens of India to enhance Information Security.
- Acting as a Resource Centre for other police organizations in the country

3.17 Recommendations of (the) Joint Working Group on Engagement with Private Sector on Cyber Security

3.17.1 Objective:

- To lay out the Roadmap for cybersecurity cooperation between private and public sector

3.17.2 Recommendations/guidelines/principles

- The guiding principles in public private partnership with respect to cybersecurity are:
- Institutional mechanisms to be set up to promote convergence of efforts both in public and private domains
- Use existing institutions and organizations to the extent possible in both private sector and government and create new institutions
- Establishing a permanent mechanism for private public partnership
- Identify bodies that can play a wider role in funding and implementation in the public and private sector;
- Identifying areas where both private and public sector can build capacities for cyber security;
- Putting in place appropriate policy and legal frameworks to ensure compliance with cybersecurity efforts;

3.17.3 Strategy

- Institutional framework
- Capacity building
- Security standards and audits
- Testing and certification
- Pilot projects

4.0 Ministry of Law, Justice and Company Affairs (Legislative Department)

4.1 The information Technology ACT (2008)

4.1 The information Technology ACT (2008)

4.1.1 Defining Cyber Security

“Protecting information, equipment, devices, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction”

4.1.2 Objectives

To provide legal recognition for the transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as “Electronic Commerce”, which involves the use of alternatives to paper based methods of communication and storage of information, to facilitate electronic filings of documents with the government agencies, to facilitate electronic filings of documents with government agencies and to amend past relevant policies

4.1.3 Recommendations/Regulations/Guidelines

- Authentication of electronic records using electronic signatures
- Legal recognition of electronic records
- Legal recognition of electronic signature
- Use of electronic records and signatures in government agencies
- Retention of electronic records
- Audit of documents in electronic form
- Publication of rules, regulations, etc. in electronic gazette
- Secure electronic records and signatures
- Every certifying authority shall:
    - Make use of hardware, software and procedures that are secure from intrusion and misuse
    - Adhere to security procedures that the secrecy and privacy of electronic signature as assured
- Penalty and compensations for damaged computers and computer systems
- Compensation for failure to protect data
- Composition of Cyber Appellate Tribunal

4.1.4 Scope

Organizations involved in electronic commerce

5.0 C-DAC (Centre for Development of Advanced Computing)

5.1 R&D: Cyber Security and Cyber Forensics

5.2 Annual Report 2014/2015

5.3 Cyber Security Brochure

5.4 Browser JS Guard

5.5 Malware Resist - (Heuristic based Anti-malware solution)

5.6 Development of face recognition system for handling large database and development of advanced techniques for video enhancement

5.7 Design Development and Enhancement of Cyber Forensics Tools

5.8 Design and Development of Honeynet System for Broadband Networks

5.9 Setting up of National Digital Crime Resource and Training Centre (NDCRTC) by SVP

5.10 Development of security solution for defence against attacks in virtualization and hypervisor technologies for cloud computing

5.11 Setting up of Cyber Forensic Training Centre (Cyber Centre) for Uttarakhand Police

5.12 Development of Cyber Security Test Bed Specifications and Test Methodologies for Industrial Control Systems

5.1 R&D: Cyber Security and Cyber Forensics

- Research and development leading to various technologies and solutions in network and gateway security, end-point security, mobile security, security analysis, authentication and identity management, and cyber forensics.
- Focus areas:
  - Biometrics
  - Cyber forensics
  - Endpoint security
  - Network security
  - Mobile and web security
  - SCADA security
  - Cloud Security
  - Honeynet technologies

5.1.1 Objective

- To use technology to develop solutions for cyber security threats and attacks
- To offer cyber security auditing services such as consultancy, analysis, training, laboratory development, malware analysis, vulnerability assessment and penetration testing of web applications and networks

5.1.2 Regulations/Recommendations/Guidelines

n/a

5.2 Annual Report 2014/2015

- The report mentions on cyber security and cyber forensics
- In the area of cybersecurity and cyber forensics, C-DAC carried out research and development leading to various technologies and solutions in network and gateway security, endpoint security, mobile security, security analysis, authentication and identity management, and cyber forensics.
- CDAC provided vulnerability assessment and penetration testing services and conducted skill-based training and nation-wide awareness programmes in this area. The activities carried out during the year are described below.
- CDAC developed the RTU Vulnerability Testing Tool
- This state-of-the-art cyber security test bench ensures the security and wellness of controllers in a process plant operating with complex logic and controlling sensitive machines. It is an open source cyber security analysis tool integrated with an inhouse developed RTU penetration testing tool. This tool can be used for testing automation controllers and developed by C-DAC and third party products.
- See report *here*

5.3 Cyber Security Brochure

- The brochure summarizes several biometric solutions, cyber forensic solutions, endpoint and network security solutions, mobile and web security solutions

5.4 Browser JS Guard

- Browser JS Guard detects and defends from malicious html & Javascript based attacks made through the web browser. It blocks access to the harmful, inappropriate and dangerous websites that may contain malicious content through Heuristics.
- It alerts the user on visiting any malicious web pages and provides the detailed analysis threat report of the web page
- This is a C-DAC site that provides a slot to enter your email address to receive the download link for the Browser JS Guard

5.5 Malware Resist - (Heuristic based Anti-malware solution)

- Malware Resist protects an end system from damage caused by malware or any other rogue software by continuously scrutinizing the active programs or processes for malicious behaviour
- The processes are monitored for a set of critical behaviours that could affect the normal functioning of the system.
- Malware Resist notifies user through an alert in case of any suspicious programs running on the end system

- The solution helps user to protect from the Malware by quarantining the processes
- These quarantined processes are terminated and will not be allowed to create again.
- In spite of alert from Malware Resist, in case if the user trusts the program, Malware Resist provides facility to enable it as a trusted program
- The detection process is based on runtime behaviour
- It has a small memory footprint and high detection rate
- It can co-exist with anti-virus solutions
- *https://cdac.in/index.aspx?id=cs_ss_mr*

5.6 Development of face recognition system for handling large database and development of advanced techniques for video enhancement

- CDAC developed advanced techniques for video enhancement
- CDAC also worked on enhancing the capabilities of already development automatic face recognition system to handle large facial database with size of 100,000 faces
- Implemented by CDAC Kolkata

5.7 Design Development and Enhancement of Cyber Forensics Tools

- Enhancement and refining of existing tools (cyber check, mobile check, enterprise forensics system, network session analyzer, cyber investigator, winlift, CDS analyzer, multilingual search tool, image forensics tool, movilextractor) with features incorporating technology advancement and requirements from Law Enforcement Agencies (LEAs)
- Implemented by C-DAC, Thirvannanthapuram

5.8 Design and Development of Honeynet System for Broadband Networks

- Design and development of a honeynet sensor for broadband networks
- Customization of botnet tracking engine (developed in earlier project) for broadband networks
- Development of a dashboard for the visualization of attack data from multiple sensors
- Implemented by C-DAC Mohali

5.9 Setting up of National Digital Crime Resource and Training Centre (NDCRTC) by SVP

- The centre designs and develops the course curriculum and its delivery for various stakeholders like law enforcement agency (LEA) s, prosecution, judiciary, banking industry, etc. in the field of digital crime prevention, detection, mitigation and investigation (digital forensics) etc
- Began “Train the Trainer” program to augment the capacity building of the State Police Digital/Cyber Crime Training Centers
- Best practices for the investigation and prosecution of digital crime of various nature, bringing uniformity and standardization in investigation of such crime(s) and make case studies for training
- The centre is a liaison with various national and international agencies working in the same arena
- The centre engages in the creation of resource portal along with e-learning methodologies over cloud and facilities for courseware dissemination, information exchange, resource persons/organizations sharing of expertise
- Implemented by National Police Academy CDAC Hyderabad

5.10 Development of security solution for defence against attacks in virtualization and hypervisor technologies for cloud computing

- CDAC is designing and developing hypervisor security components to provide defenses against the identifies runtime attacks to ensure confidentiality in the virtualization and hypervisor layers of cloud computing infrastructures
- Implemented by C-DAC Bangalore

5.11 Setting up of Cyber Forensic Training Centre (Cyber Centre) for Uttarakhand Police

- C-DAC Noida is engaged in setting up and establishing a state-of-the-Art cyber Forensics Training Facility in Uttarakhand for the benefit of Uttarakhand police, law enforcement agencies and other stakeholders
- The initiative is intended to help develop human resources in Uttarakhand by creating awareness level, expert and technical manpower from amongst the Uttarakhand police, Law Enforcement Agencies and other Stakeholders
- The Centre will conduct training programs on cyber forensics for Uttarakhand police and other stakeholders
- The plan is to use the developed training facility for Cyber Forensic Analysis in the Uttarakhand (North Region) and to assist the Law Enforcement Agencies in case analysis with a ready setup for analysis
- Implemented by C-DAC Noida

5.12 Development of Cyber Security Test Bed Specifications and Test Methodologies for Industrial Control Systems

- CDAC is conducting a study on the security standards relating to industrial standards relating to industrial control systems and on the security of an industrial control system with detailed system study in one of the automation system implemented in power sector
- The system study is aimed to be conducted covering all the details of an automation system including all automation devices, sensors, actuators, signals and computer systems of a typical industrial control system in power systems SCADA from major vendors
- Implemented by C-DAC Thiruvanthapuram

6.0 DoT (Department of Telecommunications)

⚙ 6.1 Term Cells

6.1 Term Cells

- Telecom Enforcement, Resource and Monitoring Cells (TERM cells)
- The government set up the Telegraph Authority in the field at all the License Service Areas and Large Telecom Districts of the country, with the purpose of ensuring network security.
- Focus area: telecom network security

6.1.1 Objectives

- The Term Cells are intended to ensure that Telecom service providers adhere to the license conditions and to take care of network security issues

6.1.2 Regulations/Recommendations/Guidelines

Vigilance of Telecom and Internet Service Providers

- Inspection of premises
- Curbing illegal activities
- Control over clandestine/illegal operation of telecom networks by vested interests having no license
- File FIT against culprits, pursue cases, issue notices indicating violation of condition of various Acts
- Analysis of call/subscription/traffic data of various licensees
- Technical arrangement for the lawful interception/monitoring of all communications
- Ascertain that licensee is providing the services within permitted area
- Coordination with all service providers

Monitoring

- Coordination with various network operators
- Monitoring of network parameters
- Checking for compliance by licensee in respect to the license conditions and any directions issued by the licensor in public interest
- Ensure optimum call competition ratio of inter operator calls
- Matters related to national security
- Disaster management
- Grievance redresses of subscribers in respect to deficiency by various operators
- Customer Document Verification with the objective to ascertain whether the mobile service operators are following the DoT guidelines for Customer Verification before providing connections
- Performs such other functions as may be

Security

- Technical interface between Security Agencies and Telecom Service Providers

6.1.3 Scope

- The term cells are a regulatory measure targeting telecommunications companies

7.0 CERT-In (Indian Computer Emergency Response Team)6.1 Term Cells

7.1 Information Security Policy for Protection of Critical Information Infrastructure (2006)

7.2 CERT-IN Annual Report 2015

7.3 Botnet Cleaning and Malware Analysis Centre

7.1 Information Security Policy for Protection of Critical Information Infrastructure (2006)

www.cert-in.org.in

Cyber security assurance tab → IT security policy → IT Security Policy for For Government and Critical Sector Organizations

7.1.1 Objectives

- To reduce the risk of cyber attacks and improve upon the security posture of critical information infrastructure

7.1.2 Regulations/Recommendations/Guidelines

- Government and critical sector organizations required to:
- Appoint a Chief Information Security Officer (CISO), who is knowledgeable in information security and related issues and designate them as a "Point of contact", responsible for coordinating security policy compliance efforts and to regularly interact with CERT-In, which is the nodal agency for coordinating all actions pertaining to cyber security
- Carry out periodic IT security risk assessments and determine acceptable levels of risks, consistent with criticality of business/functional requirements, likely impact on business/functions and achievement of organizational goals/objectives
- Periodically test and evaluate the adequacy and effectiveness of technical security control measures implemented for IT systems and networks (penetration testing, vulnerability assessment, application security testing, web security testing)
- Carry out Audit of Information infrastructure on an annual basis and when there is a major change in the IT infrastructure, by an independent IT security auditing organization
- Periodically report to CERT-In the cyber security incidents

7.1.3 Scope

- The policy applies to government and critical sector organizations

7.2 CERT-IN Annual Report 2015

- CERT-In organized 25 training programmes on specialized topics in the area of cyber security for constituency
- The Information Technology Act, 2000 designated CERT-In to serve as the national agency to perform the following functions in 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 cyber incidents
    - Such other functions relating to cyber security may be prescribed
- CERT-In provides
    - Proactive services in the nature of Advisories, Security Alerts, Vulnerability Notes, and Security Guidelines to help organizations secure their systems and networks
    - Reactive services when security incidents occur so as to minimize damage
    - Security Quality management services in the form of cyber security audits, promotion of best practices and cyber security exercises/drills
- Conducted workshops
    - "Cyber security threats and mitigation" March 05, 2015
    - "Cyber security threats and countermeasures" July 30 2015
    - "Cyber security Threats and mitigation" November 4th 2015
    - Latest" Cyber Security Threats and Mitigations" December 11, 2015
- CERT-In carries out mock drills with organizations from key sectors to enable participating organizations to assess their preparedness in dealing with cyber crisis situations. These drills have helped improve the cybersecurity posture of the information infrastructure and

training of manpower to handle cyber incidents, besides increasing the cyber security awareness among the key sector organizations

- Established collaborations with international security organizations and CERTs to facilitate exchange of information related to latest cyber security threats and international best practices
- Planned to set up mechanisms to generate necessary situational awareness of existing and potential cyber security threats and enable timely information sharing for proactive, preventive and protective actions by individual entities

7.3 Botnet Cleaning and Malware Analysis Centre

- The “ Cyber Swachhta Kendra “ (Botnet Cleaning and Malware Analysis Centre) is a part of the Government of India’s Digital India initiative under the Ministry of Electronics and Information Technology (MeitY) to create a secure cyber space by detecting botnet infections in India and to notify, enable cleaning and securing systems of end users so as to prevent further infections.
- The “Cyber Swachhta Kendra “ (Botnet Cleaning and Malware Analysis Centre) is set up in accordance with the objectives of the “National Cyber Security Policy”, which envisages creating a secure cyber ecosystem in the country.
- Operates in close coordination and collaboration with Internet Service Providers and Product/Antivirus companies.
- Operated by the Indian Computer Emergency Response Team (CERT-In) under provisions of Section 70B of the Information Technology Act, 2000

8.0 RBI (Reserve Bank of India)

8.1 Information Technology (IT) Subsidiary (2016)

8.2 Information Technology Vision Document (2011-2017)

8.3 The Institute for Development and Research in Banking Technology (IDRBT)

8.4 Cyber Security Framework in Banks (2016)

8.5 The RBI Guidelines (2012)

8.6 Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds

8.7 Report of the Group on Enabling PKI in Payment System Applications. March 2014

8.8 Core Banking Solution Requirements for Urban Cooperative Banks: Functional and Technical. June 2016

8.9 Inte-Disciplinary Standing Committee on Cyber Security (Feb 2017)

8.1 Information Technology (IT) Subsidiary (2016)

Focus areas:

- Cyber security
- Research and innovation
- IT systems audit and assessment of RBI regulated entities
- IT project management including Support and Advisory Services

8.1.1 Objective

The RBI's IT Subsidiary is responsible for IT requirements of the RBI, including cyber security, with the objective of protecting the banking sector and its customers from the threat of systemic vulnerabilities that enable technology and banking related frauds

8.1.2 Regulations/Recommendations/Guidelines

The IT Subsidiary's role is to aid the RBI in effectively monitoring and supervising internet-based activities and services across India.

It must also participate in setting standards to strengthen the RBI's role as regulator

It is also tasked with forming Advisory committees to provide guidance on cyber security, current and futuristic requirements of entities regulated by the Reserve Bank, particularly from the regulatory and supervisory perspectives, and to the RBI on its IT systems and projects

Periodical reporting to apex level committees of the RBI is required from the IT subsidiary

8.2 Information Technology Vision Document (2011-2017)

Focus areas:

- Knowledge based system
- Information security
- IT governance
- Project management

8.2.1 Objectives

To provide a roadmap towards a knowledge-based transformation that uses information as its focal point.

This transformation is intended to conform Data management to internationally accepted standards and to use business intelligence from data warehouse

To set information security frameworks

Information security is only one of a few focus areas in this document. See more details *here*

8.2.2 Regulations/Recommendations/Guidelines

- To enhance enterprise knowledge using relevant data effectively and applying knowledge either in the same context or in a new one (where knowledge is created). We must improve channels and contests as a means of enhancing enterprise knowledge
- To reduce reporting burden, ease validation and improve overall efficiency of data-driven decision making, we need:
  - Uniform data reporting standards
  - Automated data flow from the source systems of Banks to their MIS server
  - Submitting data to the Reserve Bank in an automated manner without manual intervention
- To create a dedicated pool of human resources for a set of purposes including information security management
- Information Security Policy
  - To review and update existing IS policy periodically
  - The reviewed policy should relate to policies such as firewall, email, network security and password. It should also address issues relating to prevention of cyber attacks by deploying appropriate technologies such as two-factor authentication
- Audit of IT processes and infrastructure: constant vigilance for the safety of IT systems

8.2.3 Scope

- The vision document targets organizations that rely on information technology for operation and organizations that store data in cyberspaces as well as banks

8.3 The Institute for Development and Research in Banking Technology (IDRBT)

The Institute for Development and Research in Banking Technology has a Centre for Cyber Security

Its focus areas:

- Financial networks and applications
- Electronic payments and settlement systems
- Security technologies for the financial sector
- Financial information systems and analytics

8.3.1 Objectives

- To carry out research and development in areas of cybersecurity and digital forensics and related areas with a specific focus on the banking and financial sector
- To provide thought leadership in the above areas to the banking and financial sector
- To conduct employee development training programs
- To develop frameworks and standards for the BFSI sector
- To conduct cyber drills for banks and train bank personnel to deal with cyber attacks

8.4 Cyber Security Framework in Banks (2016)

Focus areas:

- Cyber security
- Banking
- Cyber fraud
- IT architecture
- Network and database security
- Customer protection
- Crisis management
- Supervision and reporting

8.4.1 Objectives

- To enhance the resilience of the banking system to cyber threats by improving the current defences in addressing cyber risks. This includes putting in place an adaptive Incident Response, Management and Recovery Framework to deal with adverse incidents/ disruptions should they occur.

8.4.2 Recommendations/Regulations/Guidelines

- Banks should immediately implement a Board approved Cyber-security policy revealing a strategy containing an approach to combat cyber threats
- Banks must work to distinguish cyber security policy from broader IT policy/IS security policy so that it can highlight the risks from cyber threats and measures to address these risks
- Banks must install continuous surveillance and testing for vulnerabilities at frequent intervals by a SOC (Security Operations Centre) which is to be set up immediately
- IT architecture must be designed in a way that is conducive to security; meaning it takes care of facilitating the security measures
- Banks must thoroughly review and comprehensively address network and database security
- Banks must ensure protection of consumer information- preserving confidentiality, integrity and availability of user data irrespective of whether the data is stored/in transit within themselves or with customers or third party vendors.
- Banks must establish a Cyber Crisis Management Plan (CCMP) to address: detection, response, recovery and containment. this should be a board approved strategy.
- Banks must establish cyber security preparedness indicators that would be used for comprehensive testing through independent compliance checks and audits carried out by qualified and competent professionals
- Banks must share information on cyber incidents with the RBI
- Supervisory reporting framework must be followed: banks must collect both summary level information and details on info security incidents including cyber-incidents
- Banks must hold immediate assessment of gaps in preparedness

must be reported to the RBI

- Organizational arrangements should be reviewed to ensure that security concerns are appreciated, receive adequate attention and get escalated into appropriate levels in the hierarchy to enable quick action
- Banks must actively raise cybersecurity awareness among stakeholders/top management/ and boards of banks

8.4.3 Scope

- Banks

8.5 The RBI Guidelines (2012)

Focus areas

- Information technology
- Information security
- IT operations
- IT services outsourcing
- IS audit
- Cyber frauds
- Business continuity planning
- Consumer education
- Legal issues

8.5.1 Objectives

- To incorporate IT risk assessment and management into the risk management framework of banks
- To push for internal audits/information system audits to independently provide assurance that IT-related processes and controls are working as intended
- To improve controls and examine the need for pro-active fraud assessment and management processes in commercial banks
- To examine the legal implications for banks arising out of cyber laws and steps that were required to be taken to suitably mitigate legal risks

8.5.2 Recommendations/Regulations/Guidelines

There is a section for each focus area but this compendium will focus on cyber security related sections (Information Security, Is Audit and Cyber Fraud)

Information Security

- Focus areas: confidentiality, integrity and availability of information
- Bank management must establish and maintain a framework to guide the development and maintenance of a comprehensive information security programme
- IS governance entails:
  - Alignment of information security with business strategy to support organizational objectives
  - Management and mitigation of risks and reduction of potential impacts on information resources to an acceptable level
  - Management of performance of info security by measuring, monitoring and reporting IS governance metrics to ensure that organizational objectives are achieved
  - Optimization of IS investments to support of organizational objectives
  - Critical components:
    - Policies and procedures to be board approved and reviewed annually
    - Risk assessment for each asset
    - Maintaining detailed inventory of info assets and classification of info/data
    - Defining roles and responsibilities
    - Banks need to grant authorization for access to info assets only where valid business need exists
    - IS to be considered at all stages of info asset's life cycle
    - Banks to have a process to verify job application info on all employees
    - Banks to implement suitable physical and environmental controls
    - User training awareness programs on IS for employees and vendor personnel

- Incident management process to maintain capability to manage incidents
- Application control and security -- there should be documented standards/procedures for administering an application system, which are approved by the application owner and kept up-to-date. Access to applications should be based on the principle of least privilege and “need to know” commensurate with the job responsibilities
- Mitigation controls indicating the requirement of roadman/ migration plan/methodology for data migration
- Implementation of new technologies to be done with due diligence as they can introduce risk
- Encryption algorithms approved by authoritative professional bodies to be used
- Data security measured to define and implement international standards and which have been subjected to digital viewing by international community and authoritative bodies
- Vulnerability assessment: banks need to scan frequently for vulnerabilities and address discovered flaws proactively to avoid likelihood of having their systems compromised
- Ongoing security monitoring processes to identify suspicious activity
- Security measures against malware to prevent, detect and correct malware
- Patch management to access technical system and software vulnerabilities quickly and effectively in order to reduce the likelihood of a serious business impact arising
- Change management -- documented and approving testing changes to ensure that they do not compromise security controls
- Audit trails for IT assets satisfying the bank’s business requirements including regulatory and legal requirements, facilitating audit, serving as forensic evidence when required and assisting in dispute resolution
- Information security reporting metrics to measure the performance and continuous improvement for effective implementation of IS practices
- IS and critical service providers/vendors: relationship between enterprise and 3rd party provider should be documented in the form an executed contract
- Network security measures to be incorporated
- Remote access controls need to be initiated
- Distributed denial of service attacks (DDoS/DoS): banks should install and configure network security devices for reasonable preventative/detective capability
- Implementation of ISO 27001 IS management System to be implemented by commercial banks
- Wireless security: enterprise security assurance needs to be obtained through periodic penetration testing exercises, audits and vulnerability assessments
- Business continuity considerations
- Information security assurance: provision of various electronic banking channels like ATM/debit cards/internet banking/phone banking should be issued only at the option of the customers based on specific written or authenticated electronic requisition along with a positive acknowledgement of the terms and conditions from the consumer

IS Audit

- Auditors required to be independent, competent and exercise due professional care
- Outsourcing relating to IS audit: risk evaluation to be done prior to entering into an outsourcing agreement and reviewed periodically in light of known and expected changes, as part of the strategic planning or review process
- Audit charter, audit policy to include IS audit
- Planning an IS audit using the Risk Based Audit approach, which involved aspects like IT risk risk assessment methodology, defining the IS audit universe, scoping and planning the audit, execution and follow up activities
- Executing IS audit: auditors should obtain evidences, perform test procedures, appropriately document findings, and conclude a report

- Reporting and follow up: reporting audit findings to the CAE and Audit Committee. IS Audit must prepare an audit summary memorandum providing overview of the entire audit processing from planning to audit findings
- Quality review: to assess audit quality by reviewing documentation, ensuring appropriate supervision of IS audit members and assessing whether IS audit members have taken due care while performing their duties

Cyber Fraud

- Fraud prevention practices need to be followed by banks
    - Fraud vulnerability assessment
    - Review of new products and processes
    - Fraud loss limits
    - Root cause analysis for actual fraud cases above rs. 10 lakhs
    - Reviewing cases with a unique modus operandi
    - Ensuring adequate data/info security measures
    - Following KYC and KY employee/vendor procedures
    - Ensuring adequate physical security
    - Sharing best practices of fraud prevention
    - Creation of fraud awareness
- Fraud detection
    - Setting up transaction monitoring group
    - Alert generation and redressal mechanisms
    - Dedicated email id and phone number for reporting suspected frauds
    - Mystery shopping
    - Reviews
- Fraud investigation
    - Fraud risk management group and special committee to examine suspected fraud or an exceptional transaction or a customer dispute/alert in a bank
- Reporting of fraud
    - Follow guidelines on reporting fraud from RBI circular 2010
    - Reports should be submitted in all cases of fraud of 1 lakh and above perpetrated through misrepresentation, breach of trust, manipulation of books of account, fraudulent encashment of instruments like cheques, drafts and bills exchange, unauthorized handling of securities charged to the bank, misfeasance, embezzlement, misappropriation of funds, conversion of property, cheating, shortages, irregularities, etc
- Customer awareness on frauds
    - Banks should continuously educate its customers and solicit their participation in various preventive/detective measures
- Employee awareness training
    - Training on fraud prevention practices should be provided by the fraud risk management group at various forums

8.5.3 Scope

- The guidelines are meant to be useful for all banks and financial institutions incorporating IT operations and support to meet their business objectives
- May also be used by advisory & auditing firms for consulting and audit purpose

8.6 Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds

8.6.1 Objectives

- To provide a set of guidelines to banks covering the entire gamut of electronic banking which would in part serve as a common minimum standard for all banks to adopt and in other part lay down the best practices which are recommended for adoption by banks in a phased manner for a safer and sounder banking environment
- For banks to follow a consistent approach in each focus area, to minimize differing interpretations

8.6.2 Recommendations/Regulations/Guidelines

Information Security

- Major role of board/top management should involve approving information security policies, establishing necessary organizational processes/functions for information security and providing necessary resources
- Each bank needs to create a separate IS function to focus exclusively on IS management. The organization of the IS function should be commensurate with the nature and size of activities of a bank and extent of IT leverage and e-delivery channels. The function should be adequately resourced in terms of the number in staff, their range and level of skills, and tools or tools or techniques
- A sufficient senior level official of the rank of GM/DGM/AGM needs to be designed as the Chief Information Security Office (CISO) responsible for articulating and enforcing the information security related issues/implementation within the organization as well as relevant external agencies. The CISO needs to report directly to the head of the risk management function and should not have direct reporting relationship with the CIO
- A Board approved Information security policy needs to be in place and reviewed at least annually. The policy framework should take into consideration, inter-alia, aspects like: alignment with business objectives; the objectives, scope, ownership and responsibility for the policy; information security organizational structure; information security roles and responsibilities; exceptions; knowledge and skill sets required; periodic training and continuous professional education; compliance review and penal measures for non-compliance of policies
- Risk assessment is the core competence of information security management for a bank. The risk assessment must, for each asset within its scope, identify the threat/vulnerability combinations that have a likelihood of impacting the confidentiality, availability or integrity of that asset - from a business, compliance and/or contractual perspective.
- Job descriptions, including roles and responsibilities, employment agreements and policy awareness acknowledgements from staff increase accountability for security. Management can communicate general and specific security roles and responsibilities for all employees based on their job descriptions. Management should expect all employees, officers, and contractors to comply with information security and/or acceptable-use policies and protect the institution's assets, including information.
- Digital evidence needs to be considered as similar to any other form of legal proof. It needs to withstand challenges to its integrity, its handling must be carefully tracked and documented, and it must be suitably authenticated by the concerned personnel. A policy needs to be in place in this regard.
- Maintaining detailed inventory of information assets and classification of information/data are among the key components of information security management.
- Banks need to grant authorisation for access to information assets only where a valid business need exists and only for a definite time period for which the access is required.
- Personnel with elevated system access privileges should be closely supervised.
- Information security needs to be considered at all stages of an information asset's (like hardware, software) life-cycle which typically includes: planning and design; acquisition and implementation; maintenance and support; and disposal so as to minimise exposure to vulnerabilities.
- Banks should have a process in place to verify job application information on all new employees. The sensitivity of a particular job or access level may warrant additional background and credit checks.
- Banks should implement suitable physical and environment controls taking into consideration threats, and based on the entity's unique geographical location, building configuration, neighboring entities, etc.
- There is a vital need for initial, and ongoing, training/awareness programmes on information security for employees and vendor personnel. There should also be a mechanism to track the effectiveness of the training programmes periodically through an assessment process designed for testing the understanding of relevant policies.
- A robust incident management process needs to be in place to maintain the capability to manage incidents within an enterprise,

to enable containment of exposures and to achieve recovery within a specified time period. Incidents could include aspects relating to misuse of computing assets, information disclosure or events that threaten the continuance of business processes.

- A bank needs to have clear accountability mechanisms and communication plans (for escalation and reporting to the Board and senior management and customer communication where appropriate) to limit the impact of information security incidents. Institutions would also need to pro-actively notify CERT-In/IDRBT/RBI regarding major cyber security incidents.
- There should be documented standards/procedures for administering an application system, which are approved by the application owner and kept up-to-date. Access to the application should be based on the principle of least privilege and "need to know" commensurate with the job responsibilities. Adequate segregation of duties needs to be enforced.
- Every application affecting critical/sensitive information, for eg. impacting financial, customer, control, risk management, regulatory and statutory aspects, must provide for detailed audit trails/ logging capability with details like transaction id, date, time, originator id , authorizer id, actions undertaken by a given user id, etc. Other details like logging IP address of client machine, terminal identity or location also need to be available. Alerts regarding use of the same machine for both maker and checker transactions need to be considered. The logs/alerts/exception reports with regard to systems should be analyzed and any issues need to be remedied at the earliest.
- The audit trails should satisfy a bank's business requirements apart from regulatory and legal requirements. It should also be facilitating the conduct of audit, serving as forensic evidence when required and assisting in dispute resolution including for non-repudiation purposes. Audit trails should be secured to ensure the integrity of the information captured and preservation of evidence.
- Banks may obtain application integrity statements in writing from the application system vendors providing for reasonable level of assurance about the application being free of malware at the time of sale, free of any obvious bugs, and free of any covert channels in the code (of the version of the application being delivered as well as any subsequent versions/modifications done).
- Data security measures need to be in place. Banks need to define and implement procedures to ensure the integrity and consistency of all critical data stored in electronic form, such as databases, data warehouses and data archives.
- Direct back-end updates to database should not be allowed except during exigencies, in the event of a genuine business need and after due authorization as per relevant policy
- Any changes to an application system/data need to be justified by genuine business need and approvals supported by documentation and subjected to a robust change management process.
- For all critical applications, either source code must be received from the vendor or a software escrow agreement needs to be in place with a third party to ensure source code availability in case the vendor goes out of business. It needs to be ensured that product updates and programme fixes are also included in the escrow agreement.
- Data transfer from one process to another or from one application to another, particularly in respect of critical or financial applications, should not have any manual intervention in order to prevent any unauthorized modification. The process needs to be automated and properly integrated through "Straight Through Processing" methodology with an appropriate authentication mechanism and audit trails.
- In the event of data pertaining to Indian operations being stored and/or processed abroad, for example, by foreign banks, there needs to be suitable controls like segregation of data and strict access controls based on 'need to know' and robust change controls. The bank should be in a position to adequately prove the same to the regulator. Regulator's access to such data/records and other relevant information should not be impeded in any manner and RBI would have the right to cause an inspection to be made of the processing centre/data centre and its books and accounts by one or more of its officers or employees or other persons.
- Robust system security testing needs to be carried out.
- Multi-tier application architecture needs to be implemented for critical e-banking systems like internet banking which differentiate session control, presentation logic, server side input validation, business logic and database access.
- A bank needs to have a documented migration policy specifying

a systematic process for data migration and for ensuring data integrity, completeness and consistency. Explicit sign offs from users/ application owners need to be obtained after each stage of migration and also after the migration process has been completed. Audit trails need to be available to document the conversion, including data mappings and transformations.

- Banks need to carry out due diligence with regard to new technologies/systems since they can potentially introduce additional risk exposures
- Any new business products introduced, along with the underlying information systems, need to be assessed as part of a formal product approval process which incorporates, inter-alia, security related aspects and fulfilment of relevant legal and regulatory prescriptions.
- Cryptographic techniques need to be used to control access to critical and sensitive data/information in transit and storage. Banks should only select encryption algorithms which are well established international standards and which have been subjected to rigorous scrutiny by an international community of cryptographers or approved by authoritative professional bodies, reputable security vendors or government agencies.
- Normally, a minimum of 128-bit SSL encryption is expected. Constant advances in computer hardware, cryptanalysis and distributed brute force techniques may induce use of larger key lengths periodically. It is expected that banks will properly evaluate security requirements associated with their internet banking systems and other relevant systems and adopt an encryption solution that is commensurate with the degree of confidentiality and integrity required.
- Banks need to scan frequently for vulnerabilities and address discovered flaws proactively to avoid the likelihood of having their computer systems compromised. Automated vulnerability scanning tools need to be used against all systems in their networks on a periodic basis.
- Banks need to have monitoring processes in place to identify suspicious events and unusual behavioural patterns that could impact the security of IT assets. The strength of the monitoring controls should be based on the criticality of an IT asset. A bank would need to establish a clear allocation of responsibility for regular monitoring mechanism, and the tools and processes in this regard need to be commensurate with the level of monitoring required.
- Critical functions , for example relating to financial, regulatory and legal, MIS and risk management, need to be done through proper application systems and not manually or in a semi-automated manner through spreadsheets which pose risks relating to data integrity and reliability. Use of spreadsheets in this regard should be restricted and should be replaced by appropriate IT applications in a phased manner within a definite timeframe.
- A robust process needs to be in place for “effective malware control”. Typical controls to protect against malicious code use layered combinations of technology, policies and procedures and training. The controls are of the preventive and detective/corrective in nature.
- Establishing a robust network protection strategy and layered security based on the principle of defence-in-depth is an absolute necessity for banks.
- There should be arrangements for monitoring and reporting of the information security condition of the organization, which are documented, agreed with top management and performed regularly. Security related metrics can be used to measure security policy implementation.
- Given the multiplicity of devices and systems, banks should deploy suitable automated tools for log aggregation and consolidation from multiple machines/systems and for log correlation and analysis.
- Security and Audit Processes of Critical service providers/vendors need to be assessed regularly since ineffective third-party controls can weaken the ability of a bank to achieve its control objectives.
- Commercial banks should implement ISO 27001 based Information Security Management System (ISMS) best practices for their critical functions. Additionally, other reputed security/IT control frameworks may also be considered by banks.
- Strong controls need to be initiated against any remote access facility. The management should establish policies restricting remote access and be aware of all remote-access devices attached to the bank’s systems. These devices should be strictly controlled.
- Events that trigger the implementation of a business continuity plan may have security implications. Risk assessments should consider the changing risks that appear in business continuity scenarios and

different security postures that may need to be established.

- Information security assurance needs to be obtained through periodic penetration testing exercises, audits and vulnerability assessments. The assurance work needs to be performed by appropriately trained and independent information security experts/auditors. The strengths and weaknesses of critical internet-based applications, other critical systems and networks needs to be carried out before each initial implementation, and at least annually thereafter. Any findings needs to be reported and monitored using a systematic audit remediation or compliance tracking methodology.
- Provision of various electronic banking channels like ATM/debit cards/internet banking/phone banking should be issued only at the option of the customers based on specific written or authenticated electronic requisition along with a positive acknowledgement of the terms and conditions from the customer. A customer should not be forced to opt for services in this regard. Banks should provide clear information to their customers about the risks and benefits of using e-banking delivery services to enable customers to decide on choosing such services.
- In view of the proliferation of cyber attacks and their potential consequences, banks should implement two-factor authentication for critical activities like fund transfers and changing customer related details through internet banking facility.
- The implementation of appropriate authentication methodologies should be based on an assessment of the risk posed by the institution’s internet banking systems. The risk should be evaluated in light of the type of customer (e.g., retail or corporate/commercial); customer transactional capabilities (e.g., bill payment, fund transfer), the sensitivity of customer information being communicated to the bank and the volume of transactions involved.
- While not using the asymmetric cryptosystem and hash function is a source of legal risk, the banks, at the least, need to implement dynamic two-factor authentication through user id/password combination and second factor like (a) OTP/dynamic access code through various modes like SMS over mobile phones or hardware token or (b) a digital signature, through a card/token containing a digital certificate and associated private key (preferably for corporate customers).
- To enhance online processing security, confirmatory second channel procedures(like telephony, SMS, email etc.) should be applied with regard to transactions above pre-set values, creation of new account linkages, registration of third party payee details, changing account details or revision to funds transfer limits. In devising these security features, the bank should take into account their efficacy and differing customer preferences for additional online protection.
- Based on mutual authentication protocols, customers could also authenticate the bank’s web site through security mechanisms such as personal assurance messages/images, exchange of challenge response security codes and/or the secure sockets layer (SSL) server certificate verification. In recent times, Extended Validation Secure Sockets Layer (EV-SSL) Certificates are increasingly being used. It should, however, be noted that SSL does not provide end-to-end encryption security at the application layer but is only designed to encrypt data in transit at the network transport layer.
- A risk based transaction monitoring or surveillance process needs to be put in place. The banks may consider dynamic scoring models and related processes to trigger or alert transactions which are not normal to improve preventive/detective capability. Study of customer transaction behavioral patterns and stopping irregular transactions or obtaining prior confirmation from customers for outlier transactions may be incorporated as part of the process.
- Chip based cards house data on microchips instead of magnetic stripes, making data more difficult to steal and cards more difficult to reproduce. It is recommended that RBI may consider moving over to chip based cards along with requiring upgradation of necessary infrastructure like ATMs/POS terminals in this regard in a phased manner.
- For debit / credit card transactions at the POS terminals, PIN based authorization system needs to be put in place (without any looping) in place of the existing signature based system and the non-PIN based POS terminals need to be withdrawn in a phased manner.
- Given that control, security and legal issues on cloud computing are still evolving, a bank needs to be cautious and carry out due diligence to assess the risks comprehensively before considering cloud computing.
- There needs to be forum of CISOs who can periodically interact

and share experiences regarding any information security threats. It is reported that a CISO forum is already functional under IDRBT. The forum may, among other functions, endeavour to share good practices, identify any specific information security issues and flag them to appropriate stakeholders like the regulator, IBA etc.

- There is a need for a system of information sharing akin to the functions performed by FS-ISAC (Financial Services Information Sharing Agency) in the US. IDRBT as a subCERT to the banking system can function as a nodal point for information sharing.
- Accreditation and empanelment of security audit qualifications/certifications and security audit vendors can be considered at a wider level by the Government of India/CERT-In or by IDRBT for the banking sector.
- In order to reduce the time, cost, and complexity of software assurance and to ensure its security, sustainability and resilience and increase the effectiveness of the methods used by the banking industry for software assurance, an initiative similar to FSTC Software Assurance Initiative (SAI) in the US can be considered in India, possibly under the aegis of IDRBT along with various stakeholders.
- There is a need for IBA, IDRBT and reputed institutions like DSCI to collaborate and develop security frameworks and detailed implementation methodologies and procedures for the benefit of the banking sector, based on the information security related aspects covered in this report.
- There is an increasing need for specific detailed research in security of banking technology and bringing out innovative and secure banking products in collaboration with reputed academic bodies like the IITs. IDRBT can expand its activities/initiatives in this regard.
- Given the nature of the problem of cyber security, there needs to be engagement at a wider level nationally and internationally, with the government, law enforcement agencies, various industrial associations and academic institutions.
- RBI can consider having a multi-disciplinary Standing Committee on Information Security with representation from various stakeholders to consider new security related developments and also legal developments, and based on the same, provide recommendations for suitable updation of guidelines on periodic basis.
- Collaborative efforts may also be made by reputed bodies like IDRBT, IIBF and DSCI coordinated by IBA to create customized indigenous certification courses to certify specific knowledge and skillsets in IT/information security areas for various categories of bank personnel at operational and managerial levels so as to create a large and diverse pool of requisite talent within the banking system.

IS Audit

- To meet the responsibility to provide an independent audit function with sufficient resources to ensure adequate IT coverage, the board of directors or its audit committee should provide an internal audit function which is capable of evaluating IT controls adequately.
- Banks should enable an adequately skilled composition of the Audit Committee to manage the complexity of the IS Audit oversight. A designated member of the Audit Committee needs to possess the relevant knowledge of Information Systems, IS Controls and audit issues. The designated member should also have relevant competencies to understand the ultimate impact of deficiencies identified in IT Internal Control framework by the IS Audit function. The Board or its Audit Committee members should seek training to fill any gaps in the knowledge related to IT risks and controls.
- The Audit Committee should devote appropriate and sufficient time to IS audit findings identified during IS Audits and members of the Audit Committee would need to review critical issues highlighted and provide appropriate guidance to the bank’s management.
- Banks should have a separate IS Audit function within the Internal Audit department led by an IS Audit Head, assuming responsibility and accountability of the IS audit function, reporting to the Chief Audit Executive (CAE) or Head of Internal Audit. Where the bank uses external resources for conducting IS audit in areas where skills are lacking within the bank, the responsibility and accountability for such external IS audits still remain with the IS Audit Head and CAE.
- IS Auditors should act independently of the bank’s management. In all matters related to the audit, the IS Audit should be independent of the auditee in both attitude and appearance. IS Auditors should be professionally competent, having the skills, knowledge, training and relevant experience to conduct an audit. IS Auditors should exercise due professional care, which includes following professional auditing standards in conducting the audit.
- Banks may decide to outsource the execution of segments of the

audit plan to external professional service providers, as per the overall audit strategy decided in co-ordination with the CAE and the Audit Committee. The work outsourced shall be restricted to execution of audits identified in the audit plan. Banks need to ensure that the overall ownership and responsibility of the IS Audit including the audit planning process, risk assessment and follow up of compliance remains within the Bank. External assistance may be obtained initially to put in place necessary processes in this regard, if required.

- An Audit Charter / Audit Policy is a document which guides and directs the activities of the Internal Audit function. IS Audit, being an integral part of the Internal Audit function, should also be governed by the same Audit Charter / Audit Policy. The audit policy should be documented to contain a clear description of its mandate, purpose, authority and accountability (of relevant members/officials in respect of the IS Audit i.e. IS Auditors, audit management and the audit committee) and the relevant operating principles. The document should be approved by the Board of Directors.
- IS Audit policy/charter should be subjected to an annual review to ensure its continued relevance and effectiveness.
- The IS auditor should consider establishing a quality assurance process (e.g., interviews, customer satisfaction surveys, assignment performance surveys etc.) to understand the auditee's needs and expectations relevant to the IS audit function. These needs should be evaluated against the policy with a view to improving the service or changing the service delivery or audit charter, as necessary.
- Banks need to carry out IS Audit planning using the Risk Based Audit Approach. The approach involves aspects like IT risk assessment methodology, defining the IS Audit Universe, scoping and planning the audit, execution and follow up activities.
- The IS Audit Universe can be built around the four types of IT resources and various IT processes like application systems, information or data, infrastructure(technology and facilities like hardware, operating systems, database management systems, networking, multimedia, etc., and the environment that houses and supports them that enable the processing of the applications) and people (internal or outsourced personnel required to plan, organize, acquire, implement, support, monitor and evaluate the information systems and services).
- The IS Auditor must define, adopt and follow a suitable risk assessment methodology. A successful risk-based IS audit program can be based on an effective scoring system arrived at by considering all relevant risk factors. Banks should develop written guidelines on the use of risk assessment tools and risk factors and review these guidelines with the Audit Committee or the Board of directors. Risk assessment related guidelines will vary for individual banks depending on their size, complexity, scope of activities, geographic diversity, and various technologies/systems used.
- The IS Audit Plan (either separately or as part of the overall internal audit plan) should be a formal document, duly approved by the Audit Committee initially and during any subsequent major changes. The Audit plan should be prepared so that it is in compliance with appropriate external regulatory/legal requirements, in addition to well-known IS Auditing Standards.
- The IS Audit Head is responsible for the annual IS Audit Plan which is prepared based on the scoping document and risk assessment. The Audit plan typically covers the overall audit strategy, scoped audit areas, details of control objectives identified in the scoping stage, sample sizes, frequency of audit based on risk assessment, nature and extent of audit and IT audit resources identification. A report on the status of planned versus actual IS audits, and any changes to the annual IS audit plan, needs to be presented periodically to the Audit Committee and Senior management.
- IT governance, information security governance related aspects, critical IT general controls like data centre controls and processes and critical business applications/systems having financial/compliance implications including MIS and regulatory reporting systems and customer access points (like delivery channels) need to be subjected to IS Audit(or integrated audit) atleast once a year (or more frequently, if warranted by risk assessment).
- IS Audits should also cover branches, with focus on large and medium branches, in critical areas like password controls, control of user ids, operating system security, antimalware controls, maker-checker controls, segregation of duties, rotation of personnel, physical security, review of exception reports/audit trails, BCP policy and testing etc.

- Detailed pre-implementation application control audits and data migration audits with regard to critical systems need to be subjected to an independent external audit.
- Banks also need to conduct a post-implementation detailed application control audit. Furthermore, banks should also include application control audits in a risk based manner as part of the regular Internal Audit/IS Audit plans with focus on data integrity (among other factors). General internal auditors with requisite functional knowledge need to be involved along with the IS Auditors in the exercise to provide the requisite domain expertise.
- IS Auditors should periodically review the results of internal control processes and analyze financial or operational data for any impact on risk assessment or scoring. Accordingly, various auditee units should be required to keep auditors up to date on all major changes in departments or functions, such as the introduction of a new product, implementation of a new system, application conversions, significant changes in organization or staff , new regulatory and legal requirements, security incidents etc.
- IS Auditors should be reasonably conversant with various fraud risk factors and should assess the risk of occurrence of irregularities connected with the area under audit. IS Auditor should also consider Fraud Vulnerability assessments undertaken by the Fraud Risk Management group, while identifying fraud risk factors as part of IT risk assessment and audit process.
- Banks should consider using testing accelerators — tools and techniques that help support the procedures IS Auditors will be performing — to increase the efficiency and effectiveness of the audit.
- Auditors need to enhance utilization of CAATs, which may be used effectively in areas such as detection of revenue leakage, assessing impact of control weaknesses, monitoring customer transactions under AML requirements and generally in areas where a large volume and value of transactions are reported. Suitable “read-only” access rights should be provided to auditors for enabling use of CAATs.
- Banks may consider, wherever possible, a continuous auditing approach for critical systems, which involves performing control and risk assessments on a more frequent basis by using technology suitably.
- The Board (or the Audit Committee) should be informed of Senior Management’s decision on all significant observations and recommendations. When IS Auditors believe that the bank has accepted a level of residual risk that is inappropriate for it, they should discuss the matter with Internal Audit function and Senior Management. If the IS Auditors are not in agreement with the decision regarding residual risk accepted by the bank, IS Auditors and Senior Management should report the matter to the Board (or the Audit Committee) for resolution.
- Services provided by a third party are relevant to the scope of IS Audit of a bank when those services, and the controls within them, form part of the bank’s information systems. These need to be adequately assessed as part of the IS Audit process.
- In order to provide assurance to management and regulators, banks are required to conduct a quality assurance, at least once every three years, on the Banks Internal Audit including IS Audit function to validate the approach and practices adopted by them in the discharge of their responsibilities as laid out in the Audit Policy.
- Accreditation and empanelment of IS audit qualifications/certifications and IS audit vendors/firms can be considered by the Government of India.

Cyber Fraud

- Most retail cyber frauds and electronic banking frauds would be of values less than Rs.1 crore and hence may not attract the necessary attention of the Special Committee of the Board. Since these frauds are large in number and have the potential to reach large proportions, it is recommended that the Special Committee of the Board be briefed separately on this to keep them aware of the proportions of the fraud and the steps taken by the bank to mitigate them. The Special Committee should specifically monitor the progress of the mitigating steps taken by the bank in case of electronic frauds and the efficacy of the same in containing fraud numbers and values.
- The activities of fraud prevention, monitoring, investigation, reporting and awareness creation should be owned and carried out by an independent fraud risk management group in the bank. The group should be adequately staffed and headed by a senior official of the bank, not below the rank of General Manager/DGM.
- Fraud review councils should be set up by the fraud risk management group with various business groups in the bank. The council

should consist of the head of the business, head of the fraud risk management department, the head of operations supporting that particular business function and the head of information technology supporting that business function. The councils should meet at least every quarter to review fraud trends and preventive steps taken that are specific to that business function/group.

- Various fraud prevention practices need to be followed by banks. These include fraud vulnerability assessments(for business functions and also delivery channels), review of new products and processes, putting in place fraud loss limits, root cause analysis for actual fraud cases above Rs.10 lakhs, reviewing cases where a unique modus operandi is involved, ensuring adequate data/information security measures, following KYC and Know your employee/vendor procedures, ensuring adequate physical security, sharing of best practices of fraud prevention and creation of fraud awareness among staff and customers.
- No new product or process should be introduced or modified in a bank without the approval of control groups like compliance, audit and fraud risk management groups. The product or process needs to be analyzed for fraud vulnerabilities and fraud loss limits to be mandated wherever vulnerabilities are noticed.
- Banks have started sharing negative/fraudulent list of accounts through CIBIL Detect. Banks should also start sharing the details of employees who have defrauded them so that they do not get hired by other banks/financial institutions.
- Quick fraud detection capability would enable a bank to reduce losses and also serve as a deterrent to fraudsters. Various important requirements recommended in this regard include setting up a transaction monitoring group within the fraud risk management group, alert generation and redressal mechanisms, dedicated e-mail id and phone number for reporting suspected frauds, mystery shopping and reviews.
- Banks should set up a transaction monitoring unit within the fraud risk management group. The transaction monitoring team should be responsible for monitoring various types of transactions, especially monitoring of potential fraud areas, by means of which, early alarms can be triggered. This unit needs to have the expertise to analyse transactions to detect fraud trends. This unit should work in conjunction with the data warehousing and analytics team within banks for data extraction, filtering, and sanitization for transaction analysis for determining fraud trends. Banks should put in place automated systems for detection of frauds based on advanced statistical algorithms and fraud detection techniques.
- It is widely accepted that fraud investigation is a specialized function. Thus, the fraud risk management group should undergo continuous training to enhance its skills and competencies. • Apart from the categories of fraud that need to be reported as per RBI Master Circular on Frauds dated July 2, 2010, it is recommended that this should also include frauds in the electronic channels and the variants of plastic cards used by banks and their customers to conclude financial transactions.
- It has been noted that there is lack of uniformity regarding the amount of fraud to be reported to RBI. Some banks report the net loss as the fraud amount (i.e. fraud amount minus recovery), while others report the gross amount. Some do not report a fraud if the entire amount is recovered. In the case of credit card frauds, some banks follow the practice of reporting the frauds net of chargeback credit received while others report the amount of the original transactions. To overcome such inconsistency, a uniform rule of reporting amounts involved in frauds is being recommended.
- A special mention needs to be made of frauds done by collusive merchants who use skimmed/stolen cards at the point of sale (POS) terminals given to them by banks and then abscond with the money before the chargeback is received on the transaction. Many banks do not report such cases stating that the banks which have issued the cards are the ones impacted. However, in these cases, the merchants cause undue loss to the bank by siphoning off the credit provided. Hence such cases should be reported as frauds.
- It has been observed that in a shared ATM network scenario, when the card of one bank is used to perpetrate a fraud through another bank's ATM, there is a lack of clarity on who should report such a fraud to RBI. It is the bank acquiring the transaction that should report the fraud. The acquiring bank should solicit the help of the issuing bank in recovery of the money. • Employee awareness is crucial to fraud prevention. Training on fraud prevention practices should be provided by the fraud risk management group at various forums.

- A positive way to create employee awareness is to reward employees who have gone beyond the call of duty and prevented frauds. Details of employees receiving such awards may be published in the fraud newsletters.
- In the case of online frauds, since the jurisdiction is not clear, there is ambiguity on where the police complaint should be filed and customers/banks have to shuttle between different police units on the point of jurisdiction. Cybercrime cells are not present in every part of the country. The matter of having a separate cell working on bank frauds in each state police department, authorized to register complaints from banks and get the investigations done on the same, needs to be taken up with respective police departments.
- To enhance investigation skills of the staff in the fraud risk management group, a training institute for financial forensic investigation may be set up by banks under the aegis of IBA.
- The experience of controlling/preventing frauds in banks should be shared between banks on a regular basis. The standing forum provided by the Indian Banks' Association (IBA) can be used to share best practices and further strengthen internal controls in respective banks.
- At each state, a Financial Crime Review Committee needs to be set up on frauds along the lines of the Security Committee that has been set up by the RBI to review security issues in banks with law enforcement authorities. The Committee can oversee the creation of awareness by banks among law enforcement agencies on new fraud types, especially technology based frauds.
- There needs to multi-lateral arrangements amongst banks to deal with on-line banking frauds. The lack of such an arrangement amongst banks may force a customer to interact with different banks/organizations when more than one bank is involved. IBA could assist in facilitating such a mechanism.

8.6.3 Scope

- The guidelines are meant to be useful for all banks and financial institutions incorporating IT operations and support to meet their business objectives
- May also be used by advisory & auditing firms for consulting and audit purpose

8.7 Report of the Group on Enabling PKI in Payment System Applications. March 2014

8.7.1 Objectives

- The policy provides guidelines on PKI implementation for banks to secure digital transactions

8.7.2 Recommendations/Guidelines

- Customers should be informed of risks, existing security measures and also be given a choice of different methods of authentication to be able to select a system that matches their security requirements.
- All banks' internet banking applications should mandatorily create authentication environment for password-based two-factor authentication as well as PKI-based system for authentication and transaction verification in online banking transactions
- DBOD may review the KYC process in banks to meet the requirement of verification prior to issuance of Digital Signature Certificates (DSCs) by Banks
- CCA may examine may examine to permit banks to act as Registration Authority for their customers for issue of DSCs. CCA can also examine exception to all CAs from the circular/guidelines issued by Government of India on physical verification of forms of subscriber as it is involved with banks regulated under RBI
- Physical form verification should rest at Registration Authority (RA) level
- CCA by consider the following points for DSCs
- Validity period for DSCs may be increased from 3 years to 5 years
- The cost of DSC to be brought down
- Renewal process for DSC to be made simple and same way be renewed with digitally signed message prior to expiry. If DSC expires, physical verification may be followed
- CCA may examine issues of DSCs on various form factors
- A group under IDRBT may be setup to study and include alternative techniques/technologies used in Internet Banking Applications.
- In online banking transactions, banks should provide the option to its customers for enabling PKI for its online banking transactions as

optional feature for all customers

- Implementation strategy for PKI-based system environment for authentication and transaction verification by banks may be carried out in three phases:
- Short-term implementation strategy (phase 1): implementation of DSC as an optional feature for certain role holders in Corporate Internet Banking for login as additional authentication
- Medium-term implementation strategy (phase 2): implementation of DSC as an optional feature for authorizers in corporate internet banking for authorizing transactions
- Long-term implementation strategy (phase 3): implementation of DSC as an optional feature for Personal Internet Banking Users for authorizing the transactions
- After PKI infrastructure is enabled in all banks, a review may be taken for mandating digital signature for large value payments

8.7.3 Scope

- The policy is applicable to the Financial sector (banks)

8.8 Core Banking Solution Requirements for Urban Cooperative Banks: Functional and Technical. June 2016

8.8.1 Objectives

- IDRBT prepared the document to detail the requirements of CBS (Core Banking Solution) in the case of UCBs (Urban Cooperative Banks), relying on inputs from functional and technical experts of CBS.
- The document is intended to serve as a reference for any UCB that is implementing CBS by an internal team or an external vendor. The document would be useful also in case of change requests, system modifications, vendor management and contract finalization.

8.8.2 Recommendations/Guidelines

- The document provides extensive requirements and guidelines for technical and functional operations. This summary will focus on the IT security aspect under the Technical requirements section. The areas of focus are listed below with the key techniques explored in the document. The link can be seen for more detailed explanations (pg 100 to 104).

Access controls

- Storing information in encrypted form
- Standard RDBMS databases with local support
- Standard error handling procedures with error logging
- Customized error and information messages
- Logging access to PII and confidential information; available in report format
- Audit trail of additions/deletions/modifications
- Automatic generation of indent for supply of security printing items
- Time limit; auto logout for inactive screens
- Unsuccessful login attempts to appear at next login screen
- Support 3rd party single sign-on solutions with active directory and biometric devices
- Upgrade the authentication and authorization mechanisms to accommodate the future use of digital signatures
- Verify digital signatures of data being uploaded in CBS
- Provide authentication/verification mechanisms with use of smart card based digital signatures
- Ability of CBS server to sign the data being downloaded so that user can verify the data integrity while uploading the same
- No database level modification allowed from application front end
- Valid software assurance agreement for patch deployment
- Once user logs on to the system from the client workstation, they should be taken to the banking application menu (possibly using a login script) and once they log out of the application session, they should get disconnected from the database with no command line access/any other means of connecting to the database (say through SQL prompt). All the functionality should be accessible only through online/menu-driven web interfaces
- Application administration only available to the bank and only given on temporary basis with an end date to application service providers for maintenance activities
- Source code of software version including any updates should be deposited with an escrow agent

Password management requirements

- Minimum password lengths
- Alphunemric
- Mandatory change of password for users at the end of preset time intervals
- Password expiration period within 30 days for normal users and 15 days for privileged users
- Usage of passwords such as username and common words not allowed
- System must hide the characters of password while typing in
- Details should be captured in an exception report
- User should be forced to change the password reset by DVA
- Enabling user ID of new employee with dummy password which the user should be forced to change on first login
- Disabling user id of employees on leave/not on computer duty
- Intruder detection should be logged with date and timestamp and terminal should get locked after a number of predefined unsuccessful attempts
- Generation of mandatory log for all activities carried out by highly powerful sers such as System Administrator/DBA
- Generation of access logs with dates and timestamp on processes run user id-wide

Network and endpoint security

- Network security is paramount for UCB-CBS as the UCBs may access the application hosted from 3rd party data centres. the approach should be "deny all and allow only" required ports after consent
- Data center hosting CBS application should have all the required security (firewall, IDS, IPS, SIEM, DDoS protection, etc) in place
- Application should be configured with correct network time to ensure data integrity
- A secured VPN connection or IPSec should be established for accessing CBS software
- Security measures for desktop/virtual machines that would be used for accessing CBS would include
    - Removal of administrator rights from installing any invalid software
    - Removal of internet access
- Harden OS and remove access to pen drive or any other mass storage devices
- Up-to-date antivirus should be available for the servers/virtual machines hosting CBS

Application security requirements

- Should not store any data in cookies/cached memory
- Source files as .java, .cpp, etc should not be available in production
- Do not allow installation of Microsoft office and/or other utility components on production servers
- Unregister/delete "dll" or ".so", other libraries that are not required
- Convert unmanaged (C, C++) code to managed code (like Java, .NET, etc)
- Code to reduce buffer overflow issues
- Allow least-privileged accounts used for running web applications
- Deploy CCA approved SSL certificates on servers for access.; Recycle SSL certificates every two years
- Should not allow system commands calls from user interface
- Encrypt impersonated application id and other config details in the configuration file
- Perform data validation on address, email id, pin code, etc
- Should validate data type, implement required field validator/range checks on client and server side
- Have an allowable character set (numeric, alpha, required, duplicates, special characters, etc.)
- Filter for double and single quotes. Do not allow characters such as "@", "<>", *, etc
- Validate data coming through janascript/php/vbscript/activex/flash, etc
- Should store files and data outside www-root
- Ensure right level of access modifiers at class and method/function level (private/public/protected)
- Remove null bytes from user input
- Create "html attribute allow" and "html tag allow" lists

- Implement html tags as iframe security
- Set debug=false in production environment
- Output validation before displaying on the screen
- Do not allow URL redirection to untrusted (non-HTTPS) site
- Perform validation on both client and server side
- Do not make any decisions based on http header information
- Hash to protect query strings during posting
- Protect “view” state using message authentication code (MAC) and/or high entropy random sequence
- erase/clear the session data after closure of session
- Make session ids random and unpredictable and do not store them on client side. Do not pass session ids in an unencrypted format
- Encrypt cached sensitive data and set cookie expiration date/time. encrypt/hash session data and all data in network by >123 bits encryption algorithm
- Disallow passage of sensitive data across pages for using HTTP, SOAP. HTTP, SOAP/JMS, etc. protocols
- Disable “GET” method for sensitive information
- Disable “GET and PUT” methods at the server level for web services
- Recommended to set 180 seconds session timeout for inactivity
- Limit the number of GET/POST per session
- Do not install of activex, jar, etc on customer machine
- Disable browser back button
- application/shared folder access given based on the need (read/write/execute)
- Have a restriction on fire type/extension for uploads. Do not allow file extensions with .at, .com, .exe, .pif, .vbs, msi, zip, etc for upload
- Input file names should be well-formed and complete with no wild characters
- Check for file integrity before processing
- File transfer should be avoided to the extent possible. If there is an unprecedented file transfer, the files should be encrypted and transferred using Secure FTP
- Restrict access to application configuration file (web.config, web.xml, etc.), registry, system32/kernel, etc.
- Enforce code access security to ensure only required privileges are available
- Do not store password in the database or in application code in clear text
- Upload file (photo, signature, collateral and other documents), size and file type (only allow pdf and jpeg format) restriction.

8.8.3 Scope

- Stakeholders that can leverage the document for functional and technical requirements:
- UCBs
- District Cooperative Central Banks (DCCBs)
- Scheduled commercial Banks (SCbs)
- Payment and Small Finance Banks

8.9 Inte-Disciplinary Standing Committee on Cyber Security (Feb 2017)

8.9.1 Objective

- To review the threats inherent in the existing/emerging technology, study adoption of various security standards/protocols; interface with stakeholders and suggest appropriate policy interventions to strengthen cyber security resilience

9.0 SEBI (Security and Exchange Board of India)

9.1 Circular on: Cyber Security and Cyber Resilience Framework of Stock Exchanges, Clearing Corporation and Depositories

9.1 Circular on: Cyber Security and Cyber Resilience Framework of Stock Exchanges, Clearing Corporation and Depositories

Focus areas

- Governance
- Protection
- Response and recovery
- Sharing of information
- Training
- Periodic audit

9.1.1 Objectives

- To engage in a detailed discussion along with the Technical Advisory Committee (TAC) with MIIS (Market Infrastructure Institutions) to develop necessary guidance in the area of cybersecurity and cyber resilience. Ultimately the goal is to protect interests of investors in securities and to promote the development of, and to regulate the securities market.

9.1.2 Recommendations/Regulations/Guidelines

- MII shall formulate a comprehensive cyber security and cyber resilience policy document encompassing a set framework
- The document should be approved by the board and reviewed annually to strengthen and improve its framework
- The policy should include the process as follows:
  - Identify critical IT assets and their risks,
  - Protect assets by deploying suitable controls, tools and measures
  - Detect incidents, anomalies and attacks through appropriate monitoring tools/processes
  - Respond by taking immediate steps after identification of the incident, anomaly or attack
  - Recover from incidents through incident management, disaster recovery and business continuity framework
- MII shall incorporate best practices from standards such as ISO 27001, ISO 27002, COBIT 5, etc
- MII should designate a senior official as Chief Information Security Officer (CISO) whose function would be to assess, identify and reduce cybersecurity risks, respond to incidents, establish appropriate standards and controls, and direct the establishment and implementation of processes and procedures as per the cyber security and resilience policy approved by the Board of the MII
- Quarterly review the implementation of the cyber security and resilience policy by the Oversight Standing Committee on Technology of the stock exchanges and of the clearing corporations and the IT strategy committee
- MII should establish a reporting procedure
- MII and CISO to periodically review instances of cyber attacks and take steps to strengthen cyber security and resilience framework
- MII must define responsibilities of its staff who may have access or use systems-- towards the goal of cyber security
- MII must identify critical assets based on their sensitivity and criticality for business operations, services and data management and to maintain their systems and info assets
- MII must accordingly identify cyber threats and vulnerabilities
- MII must encourage third-party providers to have similar info security standards
- MII must enforce access controls and to restrict physical access to critical systems for protection
- MII must establish baseline standards for consistent application of security configurations to operating systems, databases and network devices
- Data-in motion and data-at-rest should be encrypted
- Only hardened and vetted hardware/software should be deployed by MII
- Regression testing before new or modified system is implemented
- Patch management procedures to include identification, categorisation and prioritization of security patches
- Suitable policy for disposals of the storage media and systems
- VAPT: vulnerability assessment and penetration testing
- Appropriate security monitoring systems and processes

- Alerts generated from monitoring and detection systems to be suitably investigated, including impact and forensic analysis of such alerts
- Quarterly reports containing info on cyber attacks and threats and what measures were taken to mitigate these threats and vulnerabilities
- Periodic auditing must be conducted

9.1.3 Scope

- This policy would apply to Market Infrastructure Institutions

10.0 National Critical Information Infrastructure Protection Centre National Technical Research Organization Government of India (NCIIPC)

- 10.1 Guidelines for Protection of National Critical Information Infrastructure (NCII)
- 10.2 5-Year Plan to Revamp Cybersecurity in India
- 10.3 Cyber Security in India: THE NCIIPC Road Map
- 10.4 NCIIPC Newsletter

10.1 Guidelines for Protection of National Critical Information Infrastructure (NCII)

- The guidelines are comprised of 40 controls and respective guiding principles for the protection of Critical Information Infrastructures
- Controls and Guidelines: These Controls will be updated periodically by NCIIPC to stay in tune with emerging protocols and technologies. For this purpose NCIIPC will consult and collaborate with all the stakeholders through feedbacks, trainings, workshops, discussions and regular interactions. NCIIPC will also consult domain experts, globally acknowledged professional actors and organisations where deem fit.
- Designed in active consultation with stakeholders with a holistic approach

10.1.1 Objectives

- To strengthen security of cyber infrastructure and protect NCII
- The proposed controls should help Critical Sectors draw a CIIP roadmap to achieve safe, secure and resilient CII

10.1.2 Recommendations/Regulations/Guidelines

Control 1: Identification of Critical Information Infrastructure (CII)

- Each critical sector is responsible to identify and categorize CIIs within their infrastructures
- The identification process is to be reviewed periodically to address changes

Control 2: Vertical and Horizontal Interdependencies

- CII should not be viewed in isolation and all vertical and horizontal interdepencies with other CIIs or resources must be taken into consideration

Control 3: Information Security Department (ISD)

- This department is to be responsible for preventing classified or critical information from being compromised by unauthorized elements and timely dissemination of relevant and valid information to the authorized elements in each identified CII
- It must also study risks, vulnerabilities and their solutions
- It must provide security briefings, securing classified information, teaching and enforcement activities related to information security
- It is responsible for planning, development, management, oversight -- relating to information security
- The document also provides a structure for the ISD

Control 4: Training, Awareness and Skill up-gradation

- CIIS must establish a Centre for Skills Development (CSD), trained and accredited
- Responsibilities of the CDS:-
- Training strategies and policies
- Period review of training strategies
- Coordinating with ISD in identification and evaluation of vulnerabilities
- Evaluating available resources and plan accordingly to examine and evaluate training and other skill programs
- Identifying and assess skills development programs
- Setting up training committee accountable for identification and facilitation of sophisticated trainings
- Timely advising the organization on skills development programs
- Serving as an interface between the organization and the external service providers related to skill development programs
- Ensuring compatibility of organization’s training policies, programs, procedures and strategies in line with the government’s rules and regulations
- Creating a skills performance system for examination and evaluation to ensure credibility of the organization-- and a data record of evidence of trainings for all employees

Control 5: Data Loss Prevention

- This control provides guidelines for battling the risk of data loss, as follows:-
- Identification, authorisation and validation of all the data storage devices
- Sound storeinventory procedure for data storages
- Proper backup plan and policy for protection of data
- Network monitoring tools for monitoring unauthorized flow of data

- Content filtering perimeter protection devices to block the restricted or classified information
- Dedicated information security policy for the management and use of mobile storage decides -- the IS policy of CII should prevent the use of personal input devices in offices
- IS policy to curb the information leakage attempts by detecting, blocking or controlling the usage of specific content based on the organization's rules or policies
- Ensuring proper physical and environmental security along with proper identification and authorization for accessing the classified data
- Only official email id to be used for official communication and correspondence along with digital signatures and encryptions
- Control of PCs/laptops in work placed through endpoint encryption

Control 6: Access Control Policies

- Access control in CIIs should follow a role based approach where roles are created for performing various jobs. All operations are role based so employer/staff is required to get the permission of the computer systems in terms of authentication as set by the access control policies of the organization

Control 7: Limiting Admin Privileges

- In every CII, the usage of admin privileges should be minimized with full checks and balances in place in accordance with the information security policy
- Proper protection mechanism to restrict the use of admin privileges

Control 8: Perimeter Protection

- The CII must ensure proper designing and implementation of the policies for the protection of the perimeter zone
- The CII must deploy of NIDS and NIPs for all the intrusion detection and prevention by blocking on the basis of up-to-date signature database
- CII must block all the connections to malicious IPs with proper ACL implementation following the white list approach
- CII must use firewalls with proper protection policies as per the work requirement of the organisation so as to block the unwanted traffic. Proper web content filtering of ingoing and outgoing traffic must be done
- A sender policy framework for blocking spoofed emails should be devised must be implemented
- Websites should be allowed through domains instead of IP addresses
- All the anti-virus and anti-spyware at the gateways and client machines should be up to data
- All critical changes to the security device infrastructure should adhere to change management process
- CII must implement access control, authorization and auditing logging of all devices under perimeter zone
- CII should implement system, application and database security to all internal infrastructure components
- White listed email content filtering for allowing known attachments
- Clients should access the internet through DNS server, email server, or an authenticated web proxy for effective monitoring and auditing
- DMZ web servers should be allowed to be accessed through proxy for proper tracking of incoming connection

Control 10: Incident Response

- There should be effective Incident Response Strategy to deal with post incident damage handling which if not discovered or detected by the organization or CII in the first place can lead to serious damage to the organization

Control 11: Risk Assessment Management

- Risk assessment management process to go as follows:
  - CII categorization
  - Threat identification
  - Vulnerability identification
  - Risk evaluation
  - Quantitative and qualitative analysis
  - Analysis of implications
  - Risk prevention and recovery
  - Compliance
- Review and feedback

(see original document for more details on each step)

Control 12: Physical and Environmental Security

- Physical security: to protect the organization's assets by properly choosing a secure office location with a proper perimeter security through access control thus protecting the hardware and software equipment
- The document provides guidelines on implementing physical security controls

Control 13: Identification and Authentications

- CIIs should implement proper identification and authorization policies
- CIIs should review all access control for identification and authorization for disabling all those persons not associated with CII
- System access provisions for the terminated employees and contractors and also for the ones who have left the organization
- CIIs should ensure strong password usage policy so as to thwart the attempts of impersonating of users by attackers
- CIIs should ensure proper encryption at transport layer for stopping impersonation attack
- CIIs should store passwords in the strong hash algorithms with salt added to it
- Authorization policies must take into account the role and based assignments so that every action by the user can be correlated to its activities
- All user should be uniquely identifies before performing any task
- There must be procedures to disable lost or stolen user identities including passwords
- Cap on user failure attempts
- Effective monitoring of the accounts and access controls

Control 14: Maintenance Plans

- Maintenance plans should be in place in all the CIIs to deal with maintenance issues
- Annual maintenance can be comprehensive depending on the organizational needs
- In comprehensive maintenance no extra cost of the labour or extra parts is taken whereas in non-comprehensive maintenance labour and extra parts cost is charged on case to case basis
- Implementation types given in the document, view for more details

Control 15: Maintaining, Monitoring and Analysing Logs

- Maintaining and monitoring logs of all activities performed with the assets of CII
- The document provides guidelines for the implementation of these monitoring systems

Control 16: Penetration Testing

- Penetration testing evaluates and tests the preparedness of any organization or CII in fighting threats originated from the weak or flawed implementation of the CIIP program
- Methodology used to validate the overall security of the CII from all the different types of internal and external threats
- Testing aimed to uncover the real time vulnerabilities or loopholes existing in infrastructure which can be manipulated by malicious attackers for launching the attack
- The document provides guidelines for the implementation of penetration testing. Review for details.

Control 17: Data Storage: Hashing and Encryption

- Storage of data should be encrypted using strong encryption algorithms and user credentials including admin are assumed to be hashed with strong hashing algorithms with proper salt added.
- This will render the hacking process slow and time consuming for an attacker, providing ample time to crack even with the high end system which will provide more time to the concerned CII to change and secure the user and admin credentials from further damage
- Data storage: data backup (hashed and encrypted--> access policies (ID, user password)--> switch, firewall, router config→ physical (biometric ICS) → CII (organizational records, copyright, personal records)
- The document provides a list of guidelines for data storage. View document for details.

Control 18: Feedback Mechanism for threat reporting to Government Agencies

- Two-way exchange of information between the CIIs and the government agencies regarding possible cyber threat or post analysis of any cyber attack
- CIIs to always maintain a feedback channel with the government agencies so as to get the important information regarding the possible threats on their CII
- The feedback mechanism should include participation of the CIIs in the workshops, training or seminars conducted by government agencies
- Organizations under CIIs to also share incidents related to their to their critical assets so that any big threat planned by attacked can be thwarted
- See list of guidelines pg 41

Control 19: Security Certifications

- Security certifications deals with the validation of the security measures or controls taken by the CII to protect the assets for smooth and error free operation
- Validation done by third party agencies (government or private agencies)
- Certifications also deal with enforcing or implementing any international security standards available globally for the protection of critical assets working in the CII by respective organizations
- See guidelines pg 43

Control 20: Asset and Inventory Management

- Inventory management: correlates all the physical and virtual critical assets owned by CIIs. it Provides information that is important for day to day system management, CIIs asset tracking, and security incident response
- Also important for managing maintenance, servicing, theft prevention, controlling system builds, performing regular audits/reviews, replacing faulty systems and discarding/destroying/auctioning/older/faulty systems
- Every CII must use this system to track unauthorized hardware or software before entering the premises of the organization
- See guidelines pg 45

Control 21: Contingency Planning

- Refers to visionary approach nurtured through proper assessment, policies, plans, procedures and technology involvement aimed for dealing with the adversaries or disruptions due to any disaster or major CII attack
- Deals with the alternate methods of operating the CIIs in case of eventually by using alternate methodologies or alternate sites for operations
- Aim is to reduce the impact of the disaster or any major CII attack to the minimum as it is impossible to completely eradicate the loss caused due to these disruptions caused
- See guidelines page 47

Control 22: Disaster Recovery Site

- Disaster recovery site or backup site where disaster recovery can happen in case the criticality of the CII is high and the resuming operation is going to take the suitable amount of time
- The disaster recovery site will host the essential or bare minimum services to run the highly critical part of the CIIs.
- Hot disaster recovery site: most expensive approach, short recovery time
- Warm disaster recovery: already housed with the appropriate hardware/software but will take some time to operationalise the things as per the latest operating procedures and policies with latest data in usage
- Cold disaster recovery site: least expensive, site has basic amenities in place, the required inventory for recovery still needs to be purchased
- See guidelines page 50

Control 23: Predictable Failure Prevention

- Deals with proactive protection of the critical assets of CIIs from damage by considering all the relevant glitches that can occur during operations in post installation phase
- This control protects the assets from damage taking into consideration Mean time to Failure (MTFR) in specific environments

and operations by providing the substitute of the assets through active and stand-by mechanism

- See guidelines page 52

Control 24: Information/Data Leakage Protection

- Data leakage is the unauthorized transmission of data or information revealed intentionally or unintentionally to unauthorized parties from within the CII or organisation to an outside destination
- Reporting of information leakage to management should be immediate to reduce its impact on the working of the CII
- Refrain from installing unauthorized programs on computers, leaving assets unattended, having unescorted visitors, improper disposals, prey to social engineering, mixing official and personal work
- Must implement encryption hash and back-up plans
- See guidelines 55

Control 25: DoS/DDoS Protection

- DoS/DDoS attack is logical or resource exhaustion attack designed to make a computer or network incompetent of giving normal services
- The most basic DoS attacks will hamper the IT assets network bandwidth or connectivity. The network gets flooded in case of bandwidth attacks with a high volume of traffic consuming all the available network resources are consumed and legitimate user requests are denied whereas in case of connectivity attacks the computer is flooded with a massive volume of connection requests making all the available operation system resources consumed thereby turning down the legitimate user requests
- CII must keep computer hardware, software and data available after and during DoS attack to prevent damages in terms of operations, productivity, availability etc.
- See guidelines pg 57-58

Control 26: Wi-Fi Security

- Need adequate encryption and password protection of networks
- Private access internet instead of public access internet
- Dont provide email access, login privileges sharing of data etc services on public wifi networks
- Do not auto-connect to open wifi networks
- Enable mac address filtering
- information/data on the wifi network should always be encrypted
- Avoid broadcasting on the network
- See rest of guidelines page 59

Control 27: Data Backup and Recovery Plan

- This control covers the back-up policy and procedures ensuring the regular and safe back-up of information which are quite vital for facilitating rapid recovery and protection against loss of information thus maintain the integrity and availability of information
- Data back-up plan is not only about backing up data but also includes deciding and defining a strategy for identification or critical data systems, planning for back-up and its implementation, monitoring and testing.
- Must determine the “recovery time objective” and “recovery point objective”
- See guidelines page 61

Control 28: Secure and Resilient Architecture Deployment

- Refers to the safe and secure establishment and execution of the information architecture in the organization of CIIs in accordance with the IS policy of the concerned CIIs keeping in view the balance between business/service, information, technology and security architectures
- Attain the goal of info security while keeping in view the functional needs of the organization so as to avoid redundancy, overspending, oversight, inadaptability and over complexity in the process and architecture devised for the information security of the CII
- Also includes safe and secure deployment of new technologies like cloud computing, intelligent networks, BYOD and their interconnections for maintaining pace with the rapid change in technology to improve working culture and efficiency
- Should provide a rigorous taxonomy and ontology in clearly identifying roles, responsibilities, processes and networks to be implemented that best suits the IS requirement along with the functional needs of CIIs
- See guidelines pg 64

Control 29: Web Application Security

- Web application security should not be viewed only at the level of website security rather all web based services and applications
- Security guidelines must be applied at each layer of web applications, servers, clients and communication channels
- Life cycle of web applications have different stages each needing to be looked into with an in-depth defence approach to minimise risks and to counter maximum threats
- See guidelines page 67

Control 30: Testing and Evaluation of Hardware and Software

- Must be cautious in procuring and deploying contaminated hardware or software products.
- After procurement and before deployment of hardware there should be an in depth testing and evaluation of hardware regarding any bug in the device
- See guidelines page 69

Control 31: Periodic Audit and Vulnerability Assessment

- Securing the critical information infrastructure makes constant vigilance and review a necessary practice for the organizations
- Must put in place the underlying technology, policies, procedures and mechanisms to secure the information infrastructure be periodically reviewed to validate their continued effectiveness
- Security audit and vulnerability assessment involved examination and evaluation of networks and other cyber/digital resources against the established security norms and best-practices to identify vulnerabilities, unnecessary exposures and subsequent risks. And then provide security recommendations.
- See guidelines page 72

Control 32: Compliance of Security Recommendation

- Practices in accordance to the information security policy and compliance of security recommendations must be ensured by CISO and the allied departments or divisions
- Compliance of security recommendations can be achieved through adequate planning and identification of requirements in accordance with the ascertain applicable laws and security standards
- Includes risk analysis, findings and recommendations
- See guidelines page 75

Control 33: Checks and Balances for Negligence

- Must be alert and attentive to security standards of CIIs as negligence can have a debilitating impact on national security, unity and integrity.
- Negligence must be checked for and dealt with
- Violation of IS policy may result in disciplinary action including warnings, memorandum, suspension or termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion
- See guidelines page 76

Control 34: Advanced Persistent Threat (APT) Protection

- APT refers to long term pattern of targeted attacks generally aimed at governments, financial institutions and political organization's computer resources and websites
- Unlikely to be detected by simple security methods for a reasonably long time which keeps criminals covert
- Defense capability building and shoring up the detection capabilities against APT has become one of the necessary tasks in National Security
- Instead of relying entirely on cyber firewalls, organizations need to equip themselves with the human firewalls (ie employees should be trained enough to become security sensitive and aware)
- See guidelines pg 77

Control 35: Network Device Protection

- Organizations to keep a vigil on the latest threats and prepare themselves to encounter vulnerabilities and mitigate the risks
- Network device protection: routers, switches, servers, desktops, laptops, etc → behavioural based real time signature generation, N/W behavioural analysis, DOS mitigation and string match techniques --> IPS, IDS, Firewall, DOS/DDOS mitigation module → network security framework (see diagram pg 79)
- See guidelines pg 79

Control 36: Cloud Protection

- Concept of cloud computing envisages use of computing resources that are delivered as a service over a network
- Puts data at risk of being accessed by unauthorized remote users
- Need for timely security measures at the organizational, cloud provider, user and other such levels which are involved in this process
- Must ensure that cloud provider is using strong encryption methods
- The hardware where data is stored must be protected
- Backup of data should be managed by organization/enterprise
- Create barriers to keep critical information separate from other information and organizations
- Registration system should be improved so that anonymity can be reduced and fraud detection capabilities enhanced
- See rest of guidelines pg 81

Control 37: Outsourcing and Vendor Security

- Outsourcing involves transferring responsibility for carrying out activity to vendor or 3rd party at an agreed price. While that has benefits, it comes with security risks
- Since all critical sectors inevitably depend on 3rd party solutions, there should be proper policies and procedures adhered to avoid any breach in the CIIs security
- Physical access to any vendor employee to sensitive areas in CII should be governed and monitored accompanied with proper background check including criminal records
- If the contract is terminated with the 3rd vendor, it is important that proter procedures and policies at the CIIs level be in place to avoid the divulgence of classified information by the former partner.
- Outsourcing and vendor security: critical infrastructure support/maintenance/service (softwares, SDLC, hardwares, communication links etc → service licence agreement (SLA), non disclosure agreement (NDA) → contract agreement and legal compliance → outsourcing
- See guidelines page 83

Control 38: Critical Information Disposal and Transfer

- This control encompasses all the electronic hardware, digital media, papers, etc that is capable of storing critical information under any notified CIIs by the NCIIPC, government of india.
- Need proper secure disposal and transfer policy with appropriate safety measures for all the media storing the critical information pertaining to any of the notified critical sectors, outlining the detailed steps for the employees to be followed
- Should be ensured that all users of this information storage media be aware of this control
- See guidelines page 86

Control 39: Intranet Security

- An Intranet is an internal network system which is based on the existing internet protocol technologies and is owned by any single organization to share its information resources through communication between its remote sites, where external network users have strong restricted access to this network
- The number of employees and users with access can be substantial, which can give rise to internal threats
- The administrative privileges for editing and updating the contents on the intranet should be accorded the utmost security with two-tier or multi-tier authentication since these privileges if exposed to unauthorized user can jeopardize the entire functioning of the CIIs
- See guidelines page 89

10.1.3 Scope

- These recommendations apply to Critical Information Infrastructure (CII) organizations

10.2 5-Year Plan to Revamp Cybersecurity in India

10.2.1 Objectives:

- To Revamp cyber security apparatus of critical infrastructures in India, such as power, transportation, water, telecommunication and defence
- To install sensors on all critical systems to give real-time info to its command and control centre about any cyber attacks to formulate quick response

10.2.2 Key Focus Areas

- Cyber security

- National security
- Protecting smart city infrastructure
- Emergency response

10.2.3 Scope

- National Critical Infrastructure

10.3 Cyber Security in India: THE NCIIPC Road Map

10.3.1 Objective

- To facilitate safe, secure and resilient information infrastructure for Critical Sectors of the nation
- To take all necessary measures to facilitate protection of Critical info infrastructure from unauthorized access, modification, use, disclosure, disruption, incapacitation or destruction through coherent coordination, synergy and raising information security awareness among all stakeholders

10.3.2 Key Focus Areas

- Cybersecurity of critical infrastructure
- Interest of national security and economy
- Setting up joint working group
- 24/7 emergency response line

10.3.3 Scope

- National Critical Infrastructure

10.4 NCIIPC Newsletter

- NCIIPC and BPCL jointly organised a one day workshop on “Cyber Security and Critical Information Infrastructure Protection” for Oil and Gas industry, at BPCL Regional Office, Noida, on 30th November 2016.
- NCIIPC and India Smart Grid Forum conducted a survey on the information security posture of the Generation, Transmission & Distribution utilities. Based on the findings a “Manual for Cyber Security in Power systems” was prepared by ISGF.
- Researchers from Nuclear Threat Initiative and SANS recently published a paper on priorities for cyber security at nuclear facilities. Cyber-attacks at nuclear facilities could be used to facilitate the theft of nuclear materials or cause radiological release.
- NCIIPC held a workshop on “Cyber Security & Critical Information Infrastructure Protection” November 30, 2016
- NCIIPC and India Smart Grid Forum (ISGF) undertook a survey of the information security posture of a sample set of the Generation, Transmission & Distribution utilities in order to provide an understanding of the present status, the required secure architecture and existing gaps.

11.0 Information Technology, Electronics & Communications Department of Telangana Government

11.1 Cyber Security Policy 2016 10.2 5-Year Plan to Revamp Cybersecurity in India

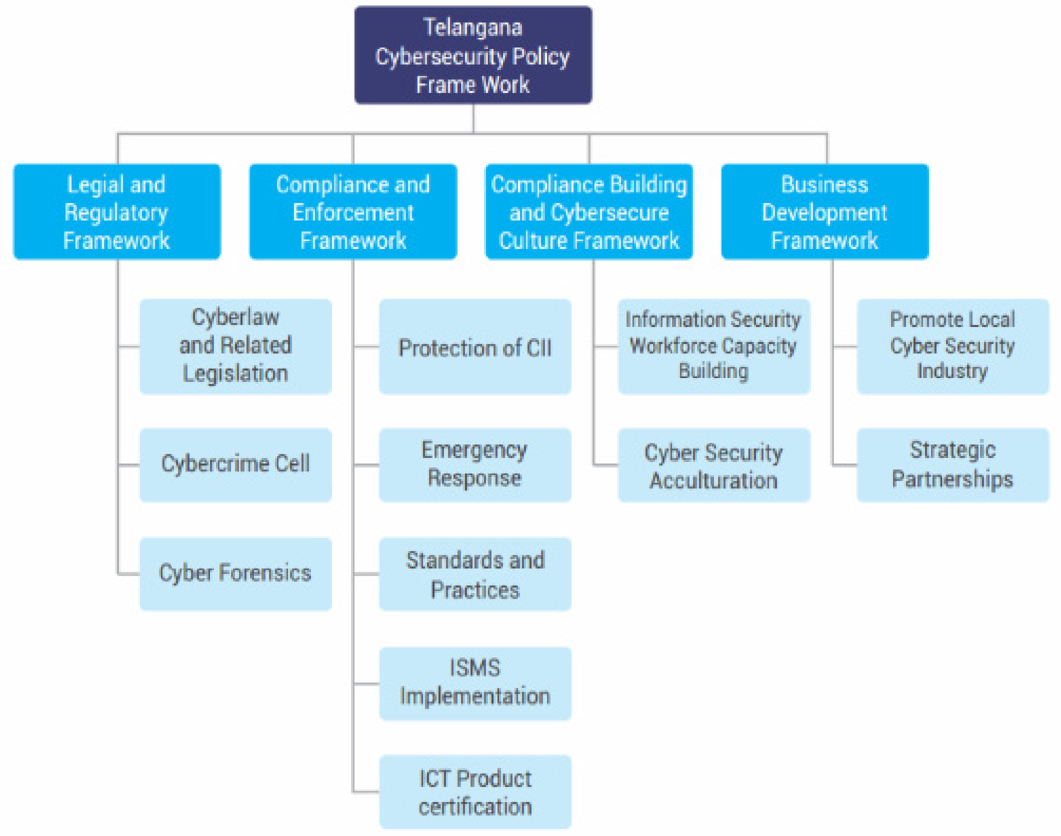
11.1 Cyber Security Policy 2016

11.1.1 Objectives

- To provide a legislative framework addressing specific legislation governing cyberspace activity through various collaborative initiatives
- Demonstrate Telangana's intent to become the go-to hub where all stakeholders work on developing new products, test them, and eventually deploy them
- To provide a legal framework which raises confidence of the private sector in sourcing their cyber security related services from the State
- To encourage other Indian states to adopt their own dynamic approach to maintain safe cyber space through effective and evolving policies
- Encourage state-state and inter-interinstitutional partnerships to promote data sharing and collaborative research efforts
- To equip professionals with requisite cyber security skills and knowledge and establish a pool of "cyber warriors" to work with the state
- Build capacity and protect critical information infrastructure (CII)
- Build cyber security awareness among citizens
- Establish requisite and institutions and legal framework to counter cyber crime

11.1.2 Recommendations/Regulations/Guidelines

An outline of Telangana Cyber Security Policy


Telangana Cybersecurity Policy Frame Work
Legal and Regulatory Framework
Compliance and Enforcement Framework
Compliance Building and Cybersecure Culture Framework
Business Development Framework
Cyberlaw and Related Legislation
Cybercrime Cell
Cyber Forensics
Protection of CII
Emergency Response
Standards and Practices
ISMS Implementation
ICT Product certification
Information Security Workforce Capacity Building
Cyber Security Acculturation
Promote Local Cyber Security Industry
Strategic Partnerships

Legal and Regulatory Framework

- Cyberlaw and related legislation: to address specific legislation governing cyberspace activity through various collaborative initiatives
  - Collaboration to establish robust legal framework: the state to collaborate with NALSAR, legal experts in the area of cyber security, The Hague Security Delta, Cyber Cell, TIPCU, etc to study the existing legal frameworks, identify problems and formulate advocacy laws to tackle real-time issues faced by these entities
  - Non-cyber specific legislation that may be relevant to regulate cyberspace activity whenever applicable such as protection of copyrights, defamation, national security/sedition, anonymity, etc will also be addressed
- Cyber Crime Cell
  - Cyber Grievance Redressal Efforts: investigating complaints pertaining to offenses under the IT Act
  - Efforts against Portnography, Cyber Bullying and Sexual Harassment: the cyber grievance system will lay special emphasis on these crimes to create a cyber space free of these offenses
- Cyber Forensics
  - Establish a digital forensics lab to analyse and investigate cybercrime to assist in the recovery and preservation of digital evidence
  - A data recovery lab to recover corrupted and deleted data as a result of cyber crime
  - A provision for developing data experts who can handle forensic and related requirements
  - Digital evidence preservation facility to secure environment for retention of digital evidence

Compliance and Enforcement Framework

- Protection of CII
  - Risk-based approach in protecting CII, where response is prioritized based on the risk it poses
  - Think Tank for Policy and Design Inputs: comprising of relevant stakeholders to facilitate cooperation and collaboration against cyber threats at the highest level
- Emergency Response
  - Apex Agency for State-wide Coordination: the government to set up T-CERT, a nodal agency for state to coordinate with institutions, organizations and companies and to contribute towards the state's cyber security efforts.
  - Provide CS related actionable information
  - Provide CS protection through intrusion detection and prevention
  - Develop state's crisis management plan to implement the same in coordination with CERT-IN
  - Assist in collaborative efforts to improve CS posture of state
  - Initiate proactive measures to increase awareness and understanding of information security and computer security issues
  - Conduct security audits or assessments of government and constituent IT infrastructure in the state, evolving security policy for the state
  - Business Continuity: the government shall mandate an agency to develop a business continuity plan to ensure continuity in case of incidents, accidents or disasters. Government shall also strive to ensure a culture of issuing and procuring cyber insurance
- Standard and Practices
  - Information sharing and analysis centre to share actionable information, develop capabilities and analyse trends to identify latest opportunities and threats
  - Promotion of open standards to ensure high levels of transparency and collaboration
  - Procurement of safe ICT products by the state by contacting industry experts to frame guidelines for procurement of trustworthy products by the state
- ISMS Implementation
  - Government to encourage implementation of ISMS across organizations in the state. Will also explore the potential of having its own ISMS initiative to help local small and medium scale industries. This will be focused on the practical governance and organizational issues of security information systems and

considering business and organizational challenges, and not address it merely as a tech problem

- ICT Security Certification
  - Certification of Cyber Security Products and Services: establish Telangana State ICT Security Assessment Facility where product certifications and compliance assessment of all sensitive ICT products linked directly or indirectly to CII will be done
  - Common Criteria for Information Technology Security Evaluation (aka CC) is an international standard (ISO/IEC 15408) for computer security certification which will be used as the basis for government driven certification scheme and product testing for government agencies and critical infrastructure
  - The government to introduce kite-marks to help individuals and companies identify cyber security products for procurement at any level-- this certification will be made mandatory

Compliance Building and Cybersecure Culture Framework

- Information Security Workforce Capacity Building
  - Certification programs through TASK: to encourage students to sign up for CS training programs
  - Collaboration with academic and research institutions to set up Centres of Excellence (CoE) to boost research in CS and launch specific R&D projects in CS. The government shall also revamp the curriculum in place for Master’s Degree in CS domain. It shall also enter partnerships with leading institutions around the country by identifying win-win situations for furthering its interests in CS. Special scholarships shall be set up for students pursuing advanced degrees in CS fields.
  - Cyber Warriors: the state shall create a pool of cyber warriors trained in CS to work as part-time security consultants with the government, advising in CS related practices
  - Customized training programs set up with private sector to provide training programs for public agencies associated with critical infrastructure
- Cyber Security Acculturation
  - Multi-channel awareness campaign involving workshops, social, print and digital media to create CS awareness among the public
  - School level CS education: revamp secondary school curriculum to cover CS practices and cybercrime issues
  - Guidelines for Safe practices to help citizens and organizations stay aware of latest developments in cybercrime and address them proactively
  - CS Security Challenge: annual competition to help identify and nurture individual talent-- a statewide drive to increase awareness and build assurance in the community about government initiatives and efforts to secure cyberspace with help of stakeholders.

Business Development Framework

- Promote Local Cyber Security Industry
  - Dedicated incubator for cyber security startups
  - Annual cyber security Expo to showcase the advantages of the State, primarily indigenously developed products by SMEs and Startups and to ensure a platform for CS enthusiasts to interact and discuss the latest developments
  - Promoting SMEs in Cyber Security: award a number of CS contracts annually to SMEs and devise a mechanism to ensure transparency in the allotment procedure.
  - Fiscal and Non-Fiscal Incentives will be given to firms operating in Telangana to boost the local industry
- Strategic Partnerships
  - Collaboration with private sector for R&D projects. Startups incorporated in Telangana will be provided access to government applications to showcase their product as proof of concept (PoC)
  - Partnering with service providers to ensure safety at the supply end and to help individuals assess the existing security levels to protect from future attacks and avoid fraudulent practices
  - Partnering with private sector to set up infrastructure such as CS training and development labs, facilitating the development of new products
  - Partnerships with international agencies such as Israel NAtional Cyber Bureau and the Hague Security Delta to benefit from their infrastructure, skill-set and research capabilities

11.1.3 Scope

- This framework applies to all stakeholders affected by Cyber Security since the policy is very much centred around collaboration
- This includes citizens, private sector organizations, partners and government

12.0 Ministry of Electronics and Information Technology (Meity)

12.1 Standardisation Testing and Quality Certification (STQC)

12.2 e-Governance Standards: eSAFE (e-Security Assurance Framework)

12.3 Lok Sabha: Parliament of India, 16.11.2016 on Cyber Attacks

12.4 Lok Sabha: Parliament of India, 22.03.2017. Promotion of Digital Transactions

12.5 Lok Sabha: Starred Question no. 457. 05.04.2017. Cyber Security

12.6 National eGovernance Division: Cyber Security

12.7 Lok Sabha Unstarred Question No. 1062, 08.02.17: MoU on Cybersecurity

12.8 Lok Sabha Unstarred Question no. 3652, 07.12.16: Cyber Security

12.9 Lok Sabha Unstarred Question no. 106, 23.11.2016: Assistance to states on Cybersecurity

12.10 National Cyber Coordination Centre (NCC (Under Digital India)

12.11 Cybersecurity and Critical Information Infrastructure- Central Workshop (National)

12.12 Advanced Centre for Research, Development and Training in Cyber Law and Forensics at the National Law School of India University in Bangalore

12.13 Cyber Law Centre and Cyber Forensic Lab at the India University's National Law School

12.14 Information Security Education and Awareness (ISEA)

12.1 Standardisation Testing and Quality Certification (STQC)

- STQC is an attached office of the Ministry of Electronics and Information Technology, Government of India.

12.1.1 Objectives

- To provide quality assurance services in the area of Electronic and IT through countrywide network of laboratories and centres. The services include texting, calibration, IT & e-governance, Training and Certification to public and private organizations
- Responsible for maintaining eGov standards

12.1.2 Services

- Testing
- Electronic and electrical testing
- Software and system testing
- Certification
- Management system certification schemes
- Product certification schemes
- Mgmt system, product certification (IT & e-gov)
- IT & e-Governance
- Software and system testing
- E-governance conformity assessment
- Mgmt system, product certification (IT & e-Gov)
- Training
- quality , reliability and laboratory management
- IT and e-governance
- test engineering and skill development
- STQC network
- ERTLs
- ETDCs
- CETEs
- IT Service Centres
- IIQM Jaipur
- CFR Chennai

12.2 e-Governance Standards: eSAFE (e-Security Assurance Framework)

12.2.1 Guidelines for assessment of effectiveness of security controls

Objective

- To provide guidelines for assessment of effectiveness of the selected security controls based on GD200/201/202/203 for information systems for eGovernance of the state and central governments of India. The guidelines apply to all components of an information system that process, store, or transmit information.
- Security controls assessments: the principal vehicle used to verify that the implementers and operators of information systems are meeting their stated security goals and objectives.
- This guideline document is to facilitate security control assessments which will provide evidence about the effectiveness of security controls in organizational information systems and Information about the strengths and weaknesses of information systems which are supporting critical eGovernment applications in a global environment of sophisticated threats.

Scope:

- Relevant/Applicable to: Information Security Auditors/Assessors, Managers and concerned employees of Govt. departments and the third party service providers of Information System Security.
- Document should not be considered as a comprehensive document for audit concepts, principles and techniques. It only focuses on the assessment of effectiveness of the security controls listed in the document GD 200 using the well known technique of use of checklist/questionnaire based on the “Look AT” and “Look For” directives.

Guidelines

- Multifactor authentication: application shall support multi-factor authentication mechanism for user authentication
- Re-authentication: application shall re-authenticate the user under the specified conditions (i.e. after specified interval of idleness or inactivity, session timeout, while accessing/modifying sensitive data like credential changing etc)
- The application should not give any hint or information about the authentication during the authentication process to avoid possible exploitation/use of the hint by unauthorized individuals
- The application automatically locks the account until released by an administration when the maximum number of unsuccessful attempts it exceeded
- Maximum password age: enforcing expiry of authentication secret after a time period (typically 30 days)
- Password history: restricting use of specified number (typically 5) of earlier used passwords
- Minimum password age: restricting change of password in quick successions by specifying a min period (typically one day) after which it can be changed
- The application shall provide mechanism to generate secrets that need defined quality metric and to enforce the use of the secret for specified functions
- The application displays an approved, system use notification message before granting access, informing potential users:
- That the user is accessing a government information system
- The system usage may be monitored, recorded and subject to audit
- Unauthorized use is prohibited and subject to criminal/civil penalties
- The use of the system indicates consent to monitoring and recording
- The system use notification provides appropriate privacy and security notices (based on associated privacy and security policies/summaries) and remains on the screen until the user takes explicit actions to log on to the information system
- The application enforces access control to the system in accordance with the applicable policy; cryptography based access control policy
- The application notifies the user, upon successful logon, of the date and time of the last logon and the number of unsuccessful logon attempts since the last successful logon
- The application is capable of limiting the number of concurrent sessions for any users
- The application provides mechanisms to protect the authenticity of sessions during communication
- The application automatically terminates a remote session after specified period of inactivity: automatic session termination applies to both local and remote sessions
- The application allows access from a specific node or equipment identified by suitable identifiers
- The application logs all access events
- Restrict application access to users at authorized time only
- Use CAPTCHA to enforce data input by human only not by computer programs or “bots”
- The application checks validity of the input data to the application
- The application protects the integrity and confidentiality of the transmitted data (authentication credentials only) between the client and the server applications. The application protects all data during transmission using encryption mechanism
- The application separates user functionality (including user interface services) from application management functionality
- The application identifies and handles error conditions in such a manner so that no sensitive information that could be exploited by adversaries is leaked through the error messages
- All computing devices shall uniquely identify and authenticate the user or any process that acts on behalf of users: multi-factor authentication for both remote system access and local system access
- In addition to user authentication, the identification of the equipment from which the remote administration is performed

should be considered as an additional control for authentication, in case remote administration of servers and network devices is permitted

- the user identifier shall be unique for each user so that the activities performed by the user on the info system can be traced back to an individual. There shall be a managed process of handling user account identified by an identifier. The process shall clearly state:
- Approval authority for creation of user accounts for info systems. The org policy shall clearly define approval authority for different info systems, considering their sensitivity
- The user account should be suspended or disabled through a managed process
- The authenticator of the user account shall be strong enough to protect the user account from unauthorized use by means of defining its minimum length and complexity. The minimum length should be in accordance with the org's password policy. The system enforces the realization of the specification of the authenticator as well as its validity through technological means.
- Internationally approved hash function should be used to store authenticators, so that the probability of guessing the authenticator from hash is curtailed
- Use of two factor authentication for accessing systems having greater sensitivity and whether the identity of the user cannot be ensured through other means
- The organization should manage the "information system authenticators" (password) by
- Defining initial authenticator content
- Establishing administrative procedures for distribution of initial authenticator, re-issuing of authenticator in the event of loss or compromise or damage of user authenticator
- Establishing administrative procedures for revoking authenticator
- Changing default authenticators upon info system installation
- changing/refreshing authenticators periodically
- The change of authenticator should be performed after completion of positive identification verification of the requestor
- The users are required to change their default password/ authenticator on first login
- Additional method to be used for the users' requests, originated from a network not under the physical security control of the organization. The clear text protocols like FTP, TELNET, etc shall be strictly avoided especially when transmitting the authentication credentials. Instead suitable secure protocols should be used where threats for unauthorized disclosure data during transmission do not exist
- Use virtual private network (VPN) for remote access from public domain
- Use of two factor authentication mechanism (password plus RSA token) for remote access
- Use of digital certificate as means of authentication to remote users
- Use of dedicated private lines for remote access to ensure the source of connections
- Control all remote accesses through a limited number of managed access control points protected w firewall
- Mandatory logging of all remote access with sufficient detailing
- See the remaining guildelines *here*

12.2.2 Guidelines for Implementation of Security Controls

Objective

- To provide guidelines for implemented the selected security controls based on GD200/201/202/201 for information systems for e-Governance of the state and central governments of India.
- The guidelines apply to all components of an information system that process, store or transmit information
- The guidelines have been developed to help achieve more secure information systems within the government by:
- Facilitating a more consistent, comparable and repeatable approach for implementing the security controls for information systems
- Better understanding of the various aspects related to the security controls

- Creating a foundation for the development of assessment methods and procedures for determining security control effectiveness

Scope

- The guidelines are relevant/applicable to managers and concerned employees of government departments and the third party service providers of information system security

Guidelines

- See guidelines *here*

12.2.3 Guidelines for Security Categorization of Information Systems

Objective

- To provide a guideline to classify information systems based on potential impacts to the organization in case of security breaches
- The guideline can be applied for all information systems to be used for eGovernance by all government departments and third party service providers

Scope

- Managers and concerned employees of government departments and the third party service providers of information system security

Guidelines

- See guidelines in *document*

12.2.4 Guidelines for Information Security Risk Assessment and Management eSAFEGD300

Objective

- To provide guidelines for information security risk assessment and management in eGovernance project, supporting eSAFE
- Can also be used to conduct risk assessment and risk management to comply the requirements of ISO/IEC 27001
- A systematic approach to information security risk management i necessary to identify organizational needs regarding information security requirements and to create an effective information security management system (ISMS).
- This approach should be suitable for the organization’s environment, and in particular should be aligned with overall enterprise risk management
- Security efforts should address risks in an effective and should be an integral part of all information security management activities and should be applied both to the implementation and the ongoing operations of ISMS

Scope

- The document is relevant to concerned managers and staff for information security assessment and management within an organization
- Also relevant for external parties supporting such activities

Guidelines

- See guidelines *here*

12.3 Lok Sabha: Parliament of India, 16.11.2016 on Cyber Attacks

Questions

- Have the incidents of cyber attacks shown a rising trend in recent times and if so, what are the details thereof and reasons therefor?
- Has there been a study conducted to identify the cyber threats from outside the country, particularly from Pakistan and if so, what are the details thereof?
- Has CERT-In issued warning to all banks cautioning of impending attacks by cyber criminals from Pakistan and if so, what are the details thereof and the measures taken by CERT-In in this regard?
- What are the new initiatives taken/proposed by the government to protect cyberspace in the country?

Answers

- See detailed answers *here*

12.4 Lok Sabha: Parliament of India, 22.03.2017. Promotion of Digital Transactions

Questions

- Whether the government is aware that online payment system is not foolproof and open to potential attack by cyber thieves who can wipe out millions of rupees bypassing the weak firewalls and if so, the details thereof;
- Whether the government is planning to float rules for operation of e-wallets;
- If so, the details thereof and the objective behind the move;
- Whether the government has drafted a consultation paper in this regard which will be shared with consumers and merchants so that they could voice their worries about the new payment system; and
- If so, the details thereof

Answers

- See detailed answers *here*

12.5 Lok Sabha: Starred Question no. 457. 05.04.2017. Cyber Security

Questions

- The size of cyber security market in monetary term in the country and its projection by 2025;
- Whether the government and the corporate world have come together to build the first platform for homegrown cyber security companies and if so, the details thereof along with the time by which the cyber security platform is likely to be prepared;
- The solutions available at present to tackle challenges related to cyber security;
- The amount of expenditure being incurred to strengthen the said measures; and
- Whether there are adequate number of cyber security experts in the country and if not, the reasons therefor and the steps being taken by the Government in this regard?

Answers

- See detailed answers *here*

12.6 National eGovernance Division: Cyber Security

12.6.1 Defining Cyber Security

- Does not define cyber security

12.6.2 Objectives

- Putting in place a cyber security framework which ensures end-to-end security of egovernance services

12.6.3 Recommendations/Regulations/Guidelines

- Identification of security elements of an eGovernance services right from conceptualization to implementation and post implementation stages
- Study of best practices on security including those worked out by STQC, DSCI and CERT-IN and adopting/modifying them into eGovernance Security Framework
- Evolve processes and procedures for setting up the mechanism to prevent cyber attack or incidents and then implement the same
- Create awareness and build capacity i the area of information security in eGovernance
- Advise states in setting up new security infrastructure
- Advise states on security enhancement of the e-Gov infrastructure that have been setup for e-gov service delivery
- Advice and help states in implementing the e-gover security policy and the detailed procedure documents that have been prepared
- Liaison with industry to understand new security products, conduct proof of concept for products that can be used in strengthening the security posture of e-gov infrastructure and then advise the states on the same
- Capacity building in cyber security for states, trainings were conducted for the states of Odisha and Uttar Pradesh in their respective state capitals.

12.6.4 Scope

- Government departments/services adopting Egovernance

12.7 Lok Sabha Unstarred Question No. 1062, 08.02.17: MoU on Cybersecurity

Questions

- whether India and USA have signed a Memorandum of Understanding (MoU) on cooperation in the field of cyber security and the MoU intends to promote closer cooperation and the exchange of information pertaining to the cyber security;
- if so, the details thereof;
- the extent to which the aforesaid MoU likely to help achieve the mutual benefits;
- whether India and United States had also signed an MoU to promote a closer cooperation and timely exchange of information between the organizations of their respective Governments responsible for Cyber Security; and
- if so, the details thereof and the success achieved by both the countries to resolve the cyber security related issues?

Answers

- See Detailed answers *here*

12.8 Lok Sabha Unstarred Question no. 3652, 07.12.16: Cyber Security

Questions

- Whether there is steady increase of internet created cyber security risks;
- If so, the details thereof and Government/private reports received in this regard along with the reaction of the Government thereto;
- Whether in India, more and more organisations believe that not all their data stored in the cloud is protected;
- If so, the details thereof; and
- The corrective measures being taken by the Government to adopt next-gen security to minimise cyber threats to transform and upgrade security strategy and systems to ensure the safekeeping of all data?

Answers

- See detailed answers *here*

12.9 Lok Sabha Unstarred Question no. 106, 23.11.2016: Assistance to states on Cybersecurity

Questions

- whether the National Critical Information Infrastructure Protection Centre (NCIIPC) provides expert assistance and technical support to the State Governments in the areas of concerns related to cyber security and if so, the details thereof, State-wise including Kerala;
- whether the Government proposes to share the strategies evolved by NCIIPC, for protection of Critical Information Infrastructure (CIC), with the State Governments, so as to avoid incidents of cyber-security violations including the hacking of the website of the State Governments, and if so, the details thereof and if not, the reason therefor;
- whether the Government is formulating a Cyber Crisis and Management Plan to manage cyber security breaches in departments of the Central and State Governments; and
- if so, the details thereof and if not, the other measures taken to prevent cyber security breaches?

Answers

- See detailed answers *here*

12.10 National Cyber Coordination Centre (NCC (Under Digital India)

- Approved in 2015
- Cannot find their own website
- In 2015, the government approved the setting up of this centre which will screen online threats and coordinate with the intelligence agencies to handle issues related to the national security.

- To operate under the authority of CERT-In
- NCCC is intended to coordinate between intelligence agencies, specifically during network intrusions and cyber attacks.
- It's role may also include cyber intelligence sharing among agencies

12.11 Cybersecurity and Critical Information Infrastructure- Central Workshop (National)

- A one day national level awareness workshop on Cyber Security in e-Governance to discuss common cyber security issues faced by ICT Infrastructure of the government and remedial measures that can be adopted
- No further information available online

12.12 Advanced Centre for Research, Development and Training in Cyber Law and Forensics at the National Law School of India University in Bangalore

- Funded by MEITy[1]
- Works translate laws into technical terms by providing training and education to judicial officers, prosecutors, investigative agencies, cyber security personnel, technologists, and others

12.13 Cyber Law Centre and Cyber Forensic Lab at the India University's National Law School

- Supported by MeitY[2]
- Training prosecutors, lawyers, government officers and bank officers
- Cyber forensic tools procured from the Centre for development of Advanced Computing to provide hands-on experience to participants[3]

12.14 Information Security Education and Awareness (ISEA)

- Launched 2015 by MeitY

12.14.1 Objectives

- Capacity building in the area of information security in order to address the human resource requirements of the country
- Training of government personnel
- Creation of mass information security awareness targeted towards academic users, general users and government users

[1] *http://www.potomacinstitute.org/images/CRI/CRI_India_Profile.pdf*
[2] *http://www.potomacinstitute.org/images/CRI/CRI_India_Profile.pdf* page 11
[3] *http://www.thehindu.com/news/cities/bangalore/nlsiu-gets-its-own-cyber-forensic-lab/article5983200.ece*

13.0 National Institute of Electronics and Information Technology (NIELIT)

13.1 Capacity Building in WSN Security and Training in J&K State

13.2 Creating mass cyber security awareness among school children, college students and the public through appropriate training and campaign mechanism of north eastern states of Mizoram Nagaland

13.3 Creating mass cyber security awareness among schools, colleges and government employees through appropriate training and campaign mechanism in NE states of Manipur and Sikkim

13.4 Enhancement of Cyber Forensics Lab for advanced training to law enforcement agencies to handle emerging cyber crimes and capacity building of youths in the area of cyber security in NE states

13.1 Capacity Building in WSN Security and Training in J&K State

- Objective is to develop improved authentication protocols for WSN applications
- To develop training curriculum, training material on WSN security
- To conduct short-term training program in modular fashion on WSN security, for students of technical institution, research scholars and teachers
- Implemented by NIELIT SRINAGAR

13.2 Creating mass cyber security awareness among school children, college students and the public through appropriate training and campaign mechanism of north eastern states of Mizoram Nagaland

- To partner with schools, colleges and universities to develop and distribute materials in local languages to students with a view to raise awareness of appropriate cyber security behaviour while using computers and internet
- To provide cyber security and ethics curriculum and explore opportunities for introducing awareness contents as part of the courses
- To conduct faculty training programs for schools and colleges
- To set up cyber security web portal and implementing help line through portal
- To organize cyber security awareness articles and advertisements in newspaper and magazines of the northeast
- To develop and distribute audio and video on cyber security
- Implemented by NIELIT

13.3 Creating mass cyber security awareness among schools, colleges and government employees through appropriate training and campaign mechanism in NE states of Manipur and Sikkim

- To partner with schools, colleges and universities to develop and distribute materials in local languages to students with a view to raise awareness of appropriate cyber security behaviour while using computers and internet
- To provide cyber security and ethics curriculum and explore opportunities for introducing awareness contents as part of the courses
- To conduct faculty training programs for schools and colleges
- Setting up cyber security web portal and implementing help line through the portal
- To organize cyber security awareness articles and advertisements in newspapers and magazines of the northeast
- To develop and distribute audio and video CD on cyber security
- Implemented by NIELIT Centre IMPHAL and Gangtok

13.4 Enhancement of Cyber Forensics Lab for advanced training to law enforcement agencies to handle emerging cyber crimes and capacity building of youths in the area of cyber security in NE states

- To provide enhanced forensic training to the law enforcement agencies in the new emerging cyber threats and proper investigation thereof to mitigate the cyber-crimes rising in the NE states
- To provide training on certificate course in the area of cyber security to the youth of NE states
- Implementation of the visualization technology in computer forensic and cyber security lab
- To develop training materials on advanced cyber forensics and cybercrime
- Implemented by NIELIT centres, Kohima

14.0 Ministry of Defence, Government of India

14.1 Annual Report 2014/15 (only noting CS mentions)

14.2 Annual Report 2015/16 (only noting CS mentions)

14.3 Lok Sabha Unstarred Question no. 3975, 09.12.17: Cybersecurity Centre for Mongolian Armed Forces

14.4 Lok Sabha Starred Question no. 400; 08/12/16: Security Threat in Defence Sector

14.5 Lok Sabha Unstarred Question no. 465; 26.02.16: Cyber Security

14.6 Lok Sabha Starred Question no. 603; 08.05.15: Cyber Security

14.7 Lok Sabha Unstarred Question no. 3368; 12.12.14: Cyber Security

14.8 Lok Sabha unstarred Question no. 1080; 28.11.14: Cyber Security

14.9 Lok Sabha: Unstarred question no. 1715; 22.07.14: Cyber Security Policy

14.1 Annual Report 2014/15 (only noting CS mentions)

- Mentions cyber security amongst “nontraditional challenges” that pose serious challenges to India and the surrounding region
- Cyber Security Training for Mongolian Armed Forces: As part of Indo-Mongolian Defence cooperation in IT Security, Project Defence Information Assurance and Research 15 Agency (DIARA), HQ IDS conducted training for officials of MoD, Mongolia and officers of Mongolian Armed Forces in IT Security. As a follow up to the training conducted in year 2013, on request from Mongolia, an advanced level training programme on IT Security was conducted during the current year.
- Directorate of Standardisation (DoS)
- In view of increased cyber threat a Cyber Security Group was created with the aim of sensitizing the defence production agencies about the importance of Cyber Security
- Defense Research and Development (DRDO)
- DRDO’s mandate is to provide assessment and advice on scientific aspects of weapons, platforms and surveillance sensors; to carry out research and to develop cutting edge technologies leading to production of state-ofthe-art sensors, weapon systems, platforms and allied equipment for our defence Services. In the recent past, **the mandate has been widened to support national cyber security architecture which includes testing capabilities, security solutions, networking systems and cyber defence tools**. In this process, it has also established national infrastructure, enhanced defence industrial capability and developed committed quality human resources.
- In the area of Cyber Security, DRDO has developed a number of high assurance security technologies for securing information in transit, storage and during processing. A number of high grade communication secrecy solutions were delivered to the defence services and other sensitive government agencies.
- To harness the S&T knowledge and practical excellence present in academic institutions and R&D centres, three thrust areas viz. cyber security, space security and low intensity conflicts were included for extramural research funding.

14.2 Annual Report 2015/16 (only noting CS mentions)

- “There is a need to further improve regional responses to challenges such as transnational crime, terrorism, natural disasters, pandemics, cyber security as well as food and energy security.”
- Cyber Security Centre for Mongolian Armed Forces: As a follow up of the training imparted to Mongolian Armed Forces in 2014 in the cyber domain, a MoU was signed between Mongolia and India for establishment 11 of a Cyber Security Centre for the Mongolia Armed Forces during the Honourable Prime Minister of India’s visit to Mongolia in May 2015.

14.3 Lok Sabha Unstarred Question no. 3975, 09.12.17: Cybersecurity Centre for Mongolian Armed Forces

Questions

- Whether the Government has completed the establishment of a Cyber Security Centre for Mongolian Armed Forces and if so, the details thereof;
- If not, the reasons therefor; and
- Whether the Government has helped in establishment of Cyber Security Centres for other countries previously and if so, the details of the countries thereof?

Answers

- See detailed answers *here*

14.4 Lok Sabha Starred Question no. 400; 08/12/16: Security Threat in Defence Sector

Questions

- whether cybercrime is becoming one of the major threats to the National Security;
- if so, the details thereof along with the incidents of cyber attack on the defence establishments reported during the last three years and the current year; and
- whether the Government and Armed Forces have taken adequate

steps to check cyber crime and protect confidential information pertaining to defence sector from cyber attacks and if so, the details thereof?

Answers

- See detailed answers *here*

14.5 Lok Sabha Unstarred Question no. 465; 26.02.16: Cyber Security

Questions

- whether some online spying agents of neighbouring countries are constantly trying to hack the Indian computer network and the intelligence agencies of the said countries have tried to steal secret defence information through the use of Computer Storage Media (CSM);
- if so, whether the Government has information of any such activity taking place within the country; and
- if so, the details thereof and the preventive measures taken by the Government in this regard?

Answers

- See detailed answers *here*

14.6 Lok Sabha Starred Question no. 603; 08.05.15: Cyber Security

Questions

- Whether reports of defence networks being continuously attacked by cyber hackers and foreign intelligence agencies have come to the notice of the Government;
- If so, the details thereof and the number of such incidents reported during the last three years;
- Whether the Government proposes to have a permanent Cyber Command Centre to prevent such incidents and if so, the details thereof; and
- The steps being taken or proposed to be taken by the Government to ensure the cyber security as well as physical security of defence personnel privy to such classified and sensitive information?

Answers

- See detailed answers *here*

14.7 Lok Sabha Unstarred Question no. 3368; 12.12.14: Cyber Security

Questions

- The total expenditure made for strengthening cyber security in the country during the last 3 years and current year
- Whether there exists any international collaboration to tackle defence related cybersecurity threats and
- If so, the details thereof?

Answers

- See detailed answers *here*

14.8 Lok Sabha unstarred Question no. 1080; 28.11.14: Cyber Security

Questions

- Whether incidents of cyberattacks in defence sector have increased over the years
- If so, the details thereof along with the estimated loss/damage caused as a result thereof;
- Whether the government has enacted a national policy framework on cyber security to protect confidential information pertaining to defence sector from cyber attack
- If so, the details thereof including the salient features and aims of the policy and;
- Whether the government proposes to join the European Convention on Cybercrime as observer and if so, the details thereof?

Answers

- See detailed answers *here*

14.9 Lok Sabha: Unstarred question no. 1715; 22.07.14: Cyber Security Policy

Questions

- Whether incidents of breach in cyber network of the country by foreign intelligence agencies have been reported in the recent past;
- If so, the details thereof; and
- The measures taken by the government to ensure that cyber security of the country is not compromised

Answers

- See detailed answers *here*

15.0 Ministry of Home Affairs, Government of India 15.0 Ministry of Home Affairs, Government of India

- 15.1 Lok Sabha: Unstarred question no. 830 to be answered on March 1st 2016: Cyber Security Policy
- 15.2 Lok Sabha: July 19th 2016, Cyber Security
- 15.3 Lok Sabha: Unstarred Question no 1408. July 26th 2016: Cyber Security Deal with UAE
- 15.4 Presentation on Cyber Crime and Security on April 12th and April 19th 2016
- 15.5 Bharat Sarkar/Government of India. Grih Mantralaya/Ministry of Home Affairs Jan 10th 2017
- 15.6 Modernization of State Police Forces
- 15.7 Cyber Training at Sardar Vallabhbhai Patel National Police Academy

15.1 Lok Sabha: Unstarred question no. 830 to be answered on March 1st 2016: Cyber Security Policy

Questions

- a) What are the details of the cyber-security policy and the agencies responsible for cyber-security in the country along with their roles and responsibilities?
- b) What is the number of cases of cyber crimes including online frauds reported along with the number of persons arrested and convicted during each of the last three years and the current year, state-wise?
- c) Has the government launched cyber crime helpline keeping in view the internal security of the country and if so, what is the number of crimes that came to light in the country as a result?
- d) What are the measures taken to curb cyber crime and tackle cyber hacking in the country?

Answers

- a) National Cyber Security Policy 2013 has been released by Dep of Electronics and IT with the objective of protecting 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. The framework for enhancing cyber security of indian cyber space, has allocated the responsibility of overall cyber security amongst:
- NTRO: responsible for protection of identified CII initially within government
- MoG/Defence Service/DRDO: responsible for defence related cyber threats, vulnerability, detection and mitigation
- DeitY/CERT-IN: responsible for non-critical government sectors and CII in the private sector
- The ministry of home affairs would be responsible for framing policies related to classification, handling and security of information relating to government in consultation with other stakeholders and monitoring its implementation, The national Information Security Policy Guidelines (NISPG) has been issued by the MHA in the m/o july 2014, to the ministries/departments for the implementation

- b) As per the data made available by the national crime record bureau, a total number of 3477 cases, 5693 cases and 9622 cases were reported under cyber-crime including online frauds. The state/UT wise cases registered, cases charge sheeted, cases convicted, persons arrested, persons charge sheeted and persons convicted under cyber crime during 2012-2014.

- c.) Ministry of home affairs has not launched a cybercrime helpline

- d.)The ministry of home affairs has issued an advisory in 2010 to the state governments and union territory administrations on cyber crime. The state governments have been advised to build adequate technical capacity in handling cybercrime including technical infrastructure, cyber police stations and trained manpower for detection, registration, investigation and prosecution of cybercrimes.

15.2 Lok Sabha: July 19th 2016, Cyber Security

Questions

- The number of incidents of cyber attacks/crimes reported along with estimated loss suffered therein during each of the last three years and the current year, state-wise
- Details of instances of misuse of social media for radialisation and propagating terrorism reported during the said period, state-wise
- The number of social media accounts shut down during the said period
- The details of mechanism put in place to monitor the social media to thwart such nefarious activities
- The measures taken by government to ensure safety of security forces and other intelligence agencies from cyber attacks and impart training to deal with cyber crimes along with the action plan for an effective cyber security strategy in the country

Answers

- See detailed answers *here*

15.3 Lok Sabha: Unstarred Question no 1408. July 26th 2016: Cyber Security Deal with UAE

Questions

- Whether the government has signed any cyber security deal with UAE in recent past to strengthen to internal security of the country from growing threat to cyber space from ISIS
- If so, the details thereof
- Whether the government is planning to create any mechanism to ensure cyber filtering of the extremist/anti-national contents present in the cyber world
- If so, the details thereof and the financial allocation made in this regard

Answers

- See detailed answers *here*

15.4 Presentation on Cyber Crime and Security on April 12th and April 19th 2016

- Letter from the Ministry of Home Affairs (MHA) asking companies to make presentations to showcase their expertise in the areas of cybercrime and cyber security, primarily related but not limited to women and child protection.
- Interested countries were asked to present the following
- Forward thinking strategies to handle cyber threats
- Capability in proactive monitoring of cyberspace to prevent crimes against women and children
- Advanced tools and best practices in management of cyber-crime
- Company's cyber crime security practices and consulting experience

15.5 Bharat Sarkar/Government of India. Grih Mantralaya/ Ministry of Home Affairs Jan 10th 2017

- This is a letter from the MHA designating Shri Kumar Alok, Joint Secretary (P-I) as Chief Information Security Officer (CISO) of the MHA

15.6 Modernization of State Police Forces

- Under this scheme, the MHA supported the development of Cyber Crime Police Stations (CCPS) and Cyber Crime Investigations and Forensics Training Facilities (CCIFTC) in each Indian state[4]

15.7 Cyber Training at Sardar Vallabhbhai Patel National Police Academy

- Government set up a state-of-the-art facility for cybercrime investigation at the National Police Academy (NPA) in Hyderabad[5].
- Courses on Right to Information Act, Anti-Corruption Strategies, National Security and on Cyber Crimes for the IAS, IPS & IFS/CPOs & Defence officers.

[4] *http://www.potomacinstitute.org/images/CRI/CRI_India_Profile.pdf*

[5] *http://www.potomacinstitute.org/images/CRI/CRI_India_Profile.pdf*

16.0 Ministry of External Affairs

16.1 Lok Sabha, Starred question no. 212, Nov 30th 2016: Breach in Cyber Security

16.2 Annual Report 2013-2014

16.1 Lok Sabha, Starred question no. 212, Nov 30th 2016: Breach in Cyber Security

Questions

1. Whether the cyber security of the websites of Indian Embassies and High Commissions in various countries have been breached in recent past
2. If so, the details thereof along with the details of the nature and extent of breach
3. Whether any sensitive data has been compromised with and if so, the details thereof
4. The measures being taken to safeguard the sensitive data of Embassies and High Commissions
5. The steps taken to sensitise the staff and officials of Embassies and High Commissions in this regard?

Answers

- (1) to (3) A few Indian Missions and Posts abroad have faced unauthorized intrusion of their respective websites. No sensitive data belonging to the Government of India was compromised.
- (4) & (5) Cyber-security measures are being strengthened to safeguard the data contained in the websites. Instructions/guidelines have been reiterated to all Missions and Posts abroad.

16.2 Annual Report 2013-2014

- (only noting parts mentioning cyber security)
- The Ministry of External Affairs has established mechanisms for cooperation between law enforcement agencies and disaster relief (HADR) and promoted dialogue on maritime security and cyber security with key partners.
- The 9th round of India-Egypt Foreign Office Consultations (FoCs) was held in New Delhi on 24 January 2013. President Mr.Mohamed Morsy visited India from 18-20 March 2013 during which six MoUs and two Letters of Intent (LoI) were signed on IT, **Cyber Security**, Small and Medium Enterprises, Culture, Space and Solar energy. On the sidelines, the IndiaEgypt Joint Business Council (JBC) meeting was held on 20 March 2013.
- The Ministry participated in Inter-Ministerial consultations relating to **Cyber Issues**. India participated in the multilateral discussions relating to global **cyber issues** including the UN Group of Governmental Experts in the field of Information and Communication Technology in the context of International Security, UN-CSTD Working Group on Enhanced Cooperation and UNODC Open Ended InterGovernmental Working Group on **Cybercrime**. Bilateral dialogues on cyber issues were held with Russia and France in February and March 2013 respectively. The Ministry continued to provide special emphasis on **cybersecurity** training to its officers. The EG&IT Division continued to provide all encompassing IT support to the Ministry and support for various e-governance applications running in the Ministry and Missions/Posts abroad.
- From Estonia, Mr. Jaak Aaviksoo, Minister for Education and Research of Estonia visited India on 13-16 October 2013 to attend the **Indian Conference on Cyber Security** and Cyber Governance in New Delhi.
- Cooperation in counter-terrorism continued to strengthen with regular exchanges between law enforcement and intelligence agencies of the two countries. The second Homeland Security Dialogue co-chaired by Home Minister Shri Sushil Kumar Shinde and the-then US Secretary of Homeland Security Ms. Janet Napolitano was held in Washington DC in May 2013 and helped strengthen ongoing operational and capacity-building cooperation. Both sides reviewed cooperation in megacity policing, combating illicit finance and counterfeiting, **cyber security** and port and border security.
- External Affairs Minister Shri Salman Khurshid attended the BRICS Foreign Ministers' Meeting hosted by Brazil on 26 September 2013 on the sidelines of 68th Session of the UN General Assembly in New York. The Ministers reviewed the progress in the implementation of the BRICS Annual Action Plan (eThekwini Action Plan) endorsed by the Leaders at the 5th BRICS Summit, took stock of the preparations for the Sixth Summit to be held in Brazil in 2014 and discussed a range of international issues, in particular the situation in Syria and the Middle East as well as **Cyber Security**. A Media Note was issued after the meeting.
- The other BRICS meetings during this period include Drug Control Agencies of BRICS countries (30 June 2013; Moscow, Russia), Contact

Group on Economic, Trade and Investment Issues (22 November 2013; Pretoria, South Africa), BRICS Cooperative Societies (26-28 October 2013; Cape Town, South Africa), 2nd BRICS Urbanization Forum (26-29 November 2013; Durban, South Africa) and 3rd BRICS Friendship Cities and Local Government Cooperation Forum (26-29 November 2013; Durban, South Africa); the first meeting of the BRICS Working Group on **Cyber Security** (19-21 February 2014:Durban); and meeting of BRICS Statistical Authorities (10-12 February 2014: Rio de Janeiro).

17.0 Central Electricity Authority (CEA)

17.1 Divisions and Placement of Technical Manpower in Central Electricity Authority

17.1 Divisions and Placement of Technical Manpower in Central Electricity Authority POLICY

- Document outlining the organizational structure of the CEA and the executive roles of members of the CEA
- The document mentions “cyber security” once under the role description of the Chief Engineer (Information Technology)
- Implementation of cyber security related policies in Indian Power Sector including implementation of IT Security Standard ISO 27001:2005

18.0 Central Bureau of Investigation (CBI)

18.1 Twenty Fourth Report on: Working of Central Bureau of Investigation (CBI)

(No mentions of “cyber security” to be exact, but a few mentions on cyber-related topics)

- The CBI has evolved into a multi-faceted, multi-disciplinary investigative agency, its role expanding from the corruption cases to other cases viz- *cyber crimes*, terrorist crimes, wildlife crimes, narcotics, etc.
- The CBI through its Policy and Coordination Division, coordinates investigation for the members of INTERPOL. The CBI has also set up a Cyber Crime Investigation and Research Cell which besides doing research in this field caters to the long felt need for investigating agencies also. It has also set up Criminal Intelligence Cell
- Section on Cyber Crimes
- CBI asking for consent of State Governments under section 6 of DSPE Act and corresponding notification by Central Government under section 5 of the Act to investigate offences (because cyber crimes currently fall outside the power jurisdiction of the CBI). Obtaining this consent on case-to-case basis is inefficient process and slows down the fast action needed to address/investigate cyber crimes
- It was also stated that though the CBI has been mandated by the Ministry of Home Affairs to build national capability in imparting training in cybercrime investigation and have also been made authorized agency of Central Government to investigate computer related crimes and to initiate investigation into all cases of hacking and cyber crimes vide letter dated June 3, 2002 of the Cabinet Secretariat, it has not been able to perform that role.
- The CBI recommends that the existing law should be amended to enable the CBI to undertake investigation into cyber crimes without going for lengthy processes of obtaining the sanction of governments of states in such cases
- Also recommends that the Cyber Crime Unit which is presently functioning in CBI should be adequately supported by a well equipped technical unit with adequate cyber investigation/forensic tools and related infrastructure
- CBI to be given the requisite legal mandate and should be equipped to monitor the cyber traffic traversing through various gateways in the country

18.2 Cybercrimes

- To combat computer-related crimes, the CBI has the following specialized structure
- Cyber Crimes Research and Development Unit (CCRDU)
- Cyber Crime Investigation Cell (CCIC)
- Cyber Forensics Laboratory; and
- Network Monitoring Centre

18.3 Cyber & Hi-Tech Crime Investigation & Training (CHCIT) Centre

- Set up and functioning at the CBI academy
- A number of courses have been conducted at CHCIT for the CBI officers including TASFU units, State Police Officers and Foreign Police Officers (African Nations, Nepal, Myanmar, Vietnam, etc)
- Technical and forensic assistance has been provided during investigation of various hi-profile cases
- Their aim is capacity building in the areas of investigation of cybercrime
- Established at CBI Academy, Ghaziabad since June 2010
- Equipped with the latest gadgets and cyber forensic tools
- Manned by highly trained and cyber forensic certified investigators
- Provides assistance in on going investigations with real time cyber and mobile forensic analysis
- Facilities at the CHCIT Center
- Search and seizure of digital all types of digital media and mobile/pda services
- Cloning, imaging and forensic copying of all types of digital media
- Image analysis and recovery of deleted data
- Hardware and software based imaging
- Mobile phone investigation, call detail records analysis and mobile forensic
- Network forensics and live forensics/preview/triage tools
- Recovery of hidden data from any digital media; Steganography

detection tools

- Email investigations and forensics/e-discovery tools
- Hardware and software based passwords recovery tools
- SIM Card data recovery and forensic cloning
- Forensic specialized courses conducted
- Search and Seizure in digital environment
- Advanced concepts in cybercrime investigation and cyber forensics
- Course on cyber crime investigation - best practices exchange (FBI, USA)
- Mobile phone investigation, call analysis and mobile forensic
- Network forensics and live forensics/preview
- Recovery of hidden data from digital media
- Email investigations and forensics/e-discovery tools
- Password cracking and recovery
- Call detail records analysis
- SIM Card data recovery and forensic cloning
- Cyber forensic tools and gadgets available in CHCIT centre
- State-of-the0art forensic workstations & FREDs with hi-end processors equipped with internal write blockers
- Hardware based imaging tools
- Forensic softwares for image analysis viz. Encase, FTK, WinHex, Paraben, CyberCheck, etc
- Internet investigation tools
- Steganography detection and analysis tool
- Relationship analysis/call data analysis software
- Password recovery software tools
- Forensic tools for cellular and PDA analysis; SIM Card and phone memory analysis
- Media wiping devices
- Triage tools
- Field forensic devicer
- Forensic tools for in-situ examination
- Tools for live system imaging and analysis
- Social networking analysis tool

18.4 MoU between CBI and DSCI to fight Cybercrime

- The MoU seeks to establish collaboration between Law Enforcement Agencies through Cyber and Hi-Tech Crime Investigation and Training (CHCIT) Centre of the CBI and the IT industry through Data Security Council of India (DSCI) and NASSCOM.
- 18.4.1 Objectives
- sharing awareness on:
- the emerging technologies
- security standard
- best practices amongst various enforcement agencies globally
- newer challenges in managing cyber crime
- preparing the stakeholders in their ability to educate and update themselves in emerging cyber technologies leading to cyber crime investigation and computer forensics

18.5 Cyber Forensic Laboratory

- The Cyber Forensic Laboratory and Digital Imaging Centre functioning under CFSL assists enforcement agencies in the collection and forensic analysis of electronic evidence.
- CFSL experts are summoned for appearing before courts. Their services are also utilised by investigating agencies for the inspection of scenes of crime.

19.0 Association of Unified Telecom Service Providers of India (AUSPI)

19.1 News Bulletin July 2015

19.1 News Bulletin July 2015

- July 27th 2015, ASSOCHAM Cyber Security Committee Meeting
- July 15th 2015, Meeting of the JWG on PPP on Cyber Security was held in NSCS Secretariat

20.0 Ministry of Petroleum and Natural Gas

20.1 Induction Material Ministry of Petroleum and Natural Gas, updated by General Coordination Section (May 2014)

20.1 Induction Material Ministry of Petroleum and Natural Gas, updated by General Coordination Section (May 2014)

- Work allocation amongst Addl. Secretary / Addl. Secretary & FA/ Senior Economic Adviser/ Joint Secretaries/ Economic Advisor/ Finance Division in the Ministry of Petroleum & NG.
- IT Policy of Government of India, its implementation, e-governance and Cyber Security
- Policy of Government of India, its implementation, e-governance and Cyber Security.

21.0 Central Electricity Regulatory Commission

21.1 Report of the Task Force on Communication System in Power Sector

21.1 Report of the Task Force on Communication System in Power Sector

- In regard to cyber security aspects, it was decided that the CEA standards for communication system should cover this aspect as well. Members were also of the view that NLDC may frame guidelines in regard to interfacing requirements for the communication system which should be followed by all users, ISTS licensees, SLDCs and RLDCs for seamless integration.
- Cyber security of communication systems
- It is imperative to plan a reliable and a robust communication network at the Central as well as the State level to meet all the functional requirements of the grid efficiently while also considering the features of Wide Area Measurement System (WAMS), smart grid, Advanced Metering Infrastructure (AMI) and cyber security.
- The Report covers only the communication requirements of the ISTS network
- The planning of a communication network involves planning the development of an adequate and reliable communication network commensurate with the growth of the power system network and in accordance with the specified planning criteria/guidelines--redundancy, safety requirements and cyber security requirements may be considered while planning such a system
- Safety of equipment as well as cyber security may be an inherent feature of the planning and implementation of communication systems
- Need to ensure cyber security for Smart Grid as it makes considerable use of IT systems. With automated operation of grid elements, the cyberspace in the power sector has increased and so have cyber security vulnerabilities as increased number of entry points and paths have become available for potential adversaries with automation. An attack on smart meters and smart appliances may lead to commercial loss apart from breach of privacy to individual consumers at the distribution level
- Cyber security must be planned and designed into systems from the very beginning and security needs to be addressed at all levels of architecture. The Task Force is in the view that CEA is the appropriate authority to formulate standards including cyber security for communication system for power sector in the country and grid integration with the neighbouring countries.
- Accordingly, CEA may formulate and notify the standards for cyber security for power system operation and control
- A nodal agency, preferably NLDC, may monitor cases of cyber-attack and discuss at PRC forum for necessary preventive and remedial action
- CEA shall formulate communication planning criterion/guidelines for development of reliable communication system for power system, duly considering requisite redundancy as well as requirements of smart grid and cyber security
- CEA shall formulate and notify technical standards, cyber security requirements, protocol for the communication system for power sector within the country including the grid integration with the neighbouring country's grid
- Task Force suggests that CEA may notify cyber security requirements and protocol for the power sector. NLDC is the appropriate agency to monitor the cyber incidents which may be discussed at RPC level. Non-compliance of cyber security requirements be reported to the commission by the Member of Secretary of RPC
- The representative of Indian Wind Power Association (IWPA) is also of the view that cyber security is important and there is need for standards for cyber security and its compliance when setting up a communication system from plant to control centre.
- At the end of the discussion while emphasizing the cyber security requirement, perceived threats and protection in the Power transmission and Communication sector, Chairperson urged all the participants to give their suggestion with reference to terms of references of the Task Force so that draft regulations could be finalized with clear perceptions of the present and upcoming trends in the Communication system in Power sector.

22.0 Controller of Certifying Authorities (CCA)

22.1 RCAI CPS

- The document provides an overview of the CCA's history, roles, responsibilities, etc
- The only mention of "cyber" refers to the cyber appellate tribunal for dispute resolution procedures

22.2 FAQs

1. Q: What is the difference between RA(Registration Authority) and CA(Certifying Authority)?

   Interacts with the subscribers for providing CA services. The RA is subsumed in the CA, which takes total responsibility for all actions of the RA.

2. Q: When you cancel an earlier communication you can get it back, how does this work in e-environment?

   New message saying that the current message supersedes the earlier one can be sent to the recipient(s). This assumes that all messages are time stamped

3. Q: If CA is out of business then if the subscriber is told to move to another CA then the subscriber has to get a new digital certificate. What happens to his/her earlier transactions ? Does this not create a legal and financial problem?

   Prior to cessation of operations the CA has to follow procedures as laid down under the IT Act. Such problems should not therefore exist

4. Q: Does CCA enforce Disaster Recovery Centre for CAs?

   Yes, it is a mandatory requirement under IT Act 20

5. Q: If somebody uses others computer, instead of his own computer, then is there any possibility of threat to the security of the owners/ users digital signature?

   No, there is no threat to the security of the owner / users digital signature, if the private key lies on the smartcard /crypto token and does not leave the SmartCard/cryptotoken.

6. Q: Does one require multiple certificates for different banks?

   Ideally, not within the same class.

7. Q: Can digital signature be employed in wireless network?

   Yes

8. Q: Is there a "Specimen Digital Signature" like paper signature?

   No. The Digital signature changes with content of the message.

9. Q: One can sign a paper without the knowledge of a signer. Is it possible in digital signature also?

   It depends upon the how the subscriber has kept his private keys. If private key is not stored securely, then it can be misused without the knowledge of the owner of the private key.

10. Q: Can a person have two digital signatures say one for official use and other one for personal use?

    Yes

11. Q: What is the extent of liability of a CA in case of antinational activities performed by a subscriber using digital signature and secure encrypted communication?

    CA has no liability, since CA is only facilitating endtoend secure communication using digital signature.

12. Q: In paper world, date and the place where the paper has been signed is recorded and court proceedings are followed on that basis. What mechanism is being followed for dispute settlements in the case of digital signatures?

    Under the IT Act, 2000 Digital Signatures are at par with hand written signatures. Therefore, similar court proceedings will be followed.

13. Q: In what format the public key should be given to CA for certification?

    In PKCS #10 format

14. Q: If a person is transferred from one post to another (say in govt. department), the digital signature will also change (yes/no)? Please explain?

    Yes. On moving from one department to another, if the procedures in place so demand, then the existing certificate will be revoked and a new one issued. In any case, the digital signature generated is different each time, even if the same key has been used.

15. Q: Can CA have sub CA? Or can there be a concept of root CA, CA and sub CA?

    No. As per IT Act, 2000 there is no provision of a sub CA. All CAs must be granted license by CCA, India. In case of any dispute, the CA licensed by CCA will be answerable.

16. Q: What is the legal sanctity of a certificate issued by outside CA (CA of a foreign country)?
    The sanctity of such a certificate will be as per the agreement between outside CA and a licensed CA in India. Such an agreement has to be approved by the CCA

17. Q: Whether CPS differs for one CA to another CA?
    Yes

18. Q: What is CPS?
    CPS (Certification Practice Statement): A statement of the practices, which a certification authority employs in issuing and managing certificates. A CPS may take the form of a declaration by the CA of the details of its trustworthy system and the practices it employs in its operations and in support of issuance of a certificate. General CPS framework is given in the guidelines.

19. Q: What types of measures are being executed by CCA for licensing a CA?
    Detailed information, financial, technical and procedural is obtained from the CA as part of the application for license . These are examined and audited. Additionally, the following are done: Supervision of activities of CAs. Auditing of CPS Auditing Hardware/Software Certifying public key of CA. Laying down standards to be maintained by CAs to ensure continues compliance to the requirements of the IT ACT 2000

20. Q: How often is auditing done? (Auditing Cycle Period)? Whether it is continuous process?
    Yes, auditing is a continuous process. According to the Rules under the IT Act 2000. The CA shall get its operations audited annually by an auditor and such audit shall include security policy and planning, physical security, technology evaluation, CA's services administration, compliance to CPS, contracts/agreements, regulation prescribed by CCA, policy requirement of CA Rules, 2000. The CA shall conduct Half yearly internal audit of security policy, physical security and planning of its operation,

21. Q: How does crossborder interoperability work in relation to digital signatures?
    Clearly, all certificates, not to mention technology applications, cannot and would not be issued by a single CA. Multiple CA's do and must exist. Inter operability between CAs national and cross-border has been addressed as Cross Certification. As per Information Technology (Certifying Authority) Rules, 2000. The licensed CA shall have arrangement for cross certification with other licensed CAs within India, which shall be submitted to the Controller before the commencement of their operations as per rule 20. Disputes arising as a result of such arrangements shall be submitted to CCA, India for arbitration or resolution. The arrangement for cross certification by the licensed CA with a foreign CA along with the application shall be submitted to CCA, India. The licensed CA shall not commence cross certification operations unless it has obtained the written or digital signature approval from CCA, India.

22. Q: Does a person require multiple Digital Signatures Certificates for different places or organizations?
    It is not mandatory. However, certificates could be issued for different purposes to the same individual. E.g. by the bank where the individual has an account, by the government to the individual as a citizen etc.

23. Q: What are the different classes of Digital Signature Certificates?
In addition to four classes of certificates given below, the Certifying Authority may issue more classes of Public Key Certificates, but these must be explicitly defined including the purpose for which each class is used and the verification methods underlying the issuance of the certificate. The suggested four classes are the following :

- Class 0 Certificate: This certificate shall be issued only for demonstration/ test purposes.
- Class 1 Certificate: Class 1 certificates shall be issued to individuals/private subscribers. These certificates will confirm that user's name (or alias) and Email address form an unambiguous subject within the Certifying Authorities database.
- Class 2 Certificate: These certificates will be issued for both business personnel and private individuals use. These certificates will confirm that the information in the application provided by the subscriber does not conflict with the information in well recognized consumer databases.
- Class 3 Certificate: This certificate will be issued to individuals as well as organizations. As these are high assurance certificates, primarily intended for ecommerce applications, they shall be issued to individuals only on their personal (physical) appearance before the Certifying Authorities.

24. Q: Is Root Certificate free?
Yes, it can be downloaded from CCA website.

25. Q: Where do I get CCAs Root Certificate?
CCAs Root certificate can be downloaded from CCAs web site cca.gov.in

26. Q: What is the function of the Root certificate?
The RCAI Root certificate is the highest level of certification in India. It is used to sign the public keys of the Licensed CAs in India. The RCAI root certificate is a self-signed certificate.

27. Q: Who are the CAs licensed by the CCA?
Safescrypt, NIC, IDRBT, TCS, GNFC, eMudhraCA

28. Q: How do I get a Digital Signature Certificate?
The Office of Controller of Certifying Authorities (CCA), issues Certificate only to Certifying Authorities. CA issue Digital Signature Certificate to end user. You can approach any one of the seven CAs for getting Digital Signature Certificate.

22.3 Order in the matter of: Yahoo India (Pvt.) Ltd.

- CCA is a statutory authority under the IT Act 2000 and has been given the powers under s. 28 to investigate any contravention of the provisions of the act, rules or regulations made thereunder
- Held that Yahoo India knowingly and wilfully ignored eleven notices sent to it by the Office of CCA under section 28 of the Act. The company knowingly committed multiple failures under section 44(a) of the act by not furnishing information/document as directed by the office of the CCA.
- Such a complete disregard of a statutory authority by the company is reprehensible, condemnable and regrettable.
- Further, the company has committed contempt of the lawful authority of a public servant under section 174 and 175 of the indian penal code, 1860
- The company was ordered to pay the penalty amount of RS 11 lakhs within 20 days from the date of the order and deposit the same in the form of a demand draft in the name of "Pay & Account Officer, DIT" payable at New Delhi

22.4 Office Order; Verification of Credentials prior to issuance of Digital Signature Certificate (DSC)

- The verification process prior to issuance of DSC is not being strictly followed.
- The document provides directions to be followed by Certifying Authorities
- The CAs must confirm that the DSC issuance process does not operate at any time in automatic approval mode
- The CAs must ensure that all supporting documents have been received along with the application form before commencing the

issuance of a DSC

- Application form along with the supporting documents must be available for inspection at CA end within 15 days of issuance of DSC
- CCA will depute Auditors to the CA sites to carry out random checks to ascertain that the above instructions are followed. Any default to be dealt as per relevant provisions of the IT Act.

23.0 Centre for Development of Telematics (CDoT)

23.1 Annual Report 2014-2015

- No mention of “cyber security” or “information security” or “cloud security”
- Noting the most relevant parts of the report:
- C-DOT has been active in the area of providing telecom software solutions. C-DOT’s umbrella NMS (Network Management System) solutions have made it possible to manage heterogeneous networks with elements from multiple vendors. C-DOT is also entrusted with the projects of national importance, like Central Monitoring System for telecom security and Secure Network for strategic applications.
- CDoT projects where progress has been made:
- **Communication and Security Research and Monitoring**: Centralised Monitoring System (CMS) infrastructure rollout, which include installation of Central Monitoring Centre (CMC) data centre at Delhi, Regional Monitoring Centre (RMC) data centre in 21 Licensed Service Areas (LSA), International Long Distance (ILD), Interception Store-and-Forward Server (ISF), etc, for lawful interception of voice and data by LEAs (Law Enforcement Agency).
- **Next Generation Security for Telecom and Data Networks**: Development of an Advanced Intelligent Monitoring System (AIMS) to scale up the architecture framework of the present CMS, development of interception solutions for new technologies like LTE/LTE-A, IMS-compliant FMCP, integration with other security agency solutions, like, content analysis, integration of satellite and marine interception and advance intelligence manager with AI (Artificial Intelligence) techniques.

23.2 C-DoT Network Management Solution (CNMS)

- C-DoT offers service providers a comprehensive suite of Network Management Solutions (NMS) which satisfies the service provider’s needs for managing and monitoring the networks effectively

24.0 Ministry of Finance

24.1 Lok Sabha, Starred question no. 39, 03.02.2017: Secured ATMs

24.2 Lok Sabha: Unstarred Question no. 5016. Standing Committee on Cyber Security

24.3 Lok Sabha: Unstarred Question no. 1812. 10.03.17. Cyber Security Incidents

24.4 Lok Sabha Starred Question no 199; 29.07.16: Cyber Security Policy

24.5 Medium Term Recommendations to Strengthen Digital Payments Ecosystem (Digital Payments Committee) December 2016

24.1 Lok Sabha, Starred question no. 39, 03.02.2017: Secured ATMs

Questions:

- Whether the Government is aware that over 70% of Automated Teller Machines (ATMs) are not secured on account of lack of upgradation of ATM software;
- If so, the details thereof and the reaction of the Government thereto;
- Whether the RBI has directed banks for upgradation of ATM softwares;
- If so, the details thereof and the response of the banks thereto; and
- The corrective steps taken/being taken by the government to strengthen/secure ATMs in the country?

Answers

- See detailed answers *here*

24.2 Lok Sabha: Unstarred Question no. 5016. Standing Committee on Cyber Security

Questions

- Whether the RBI proposes the constitution of an interdisciplinary Standing Committee on Cyber Security to review the threats inherent in the existing and emerging technologies in banks;
- If so, the details of the Committee along with its terms and reference;
- The time by which the Committee is likely to submit its report to the government;
- Whether the government should ensure that the banks in private sector and other non-banking financial companies would also be provided cybersecurity; and
- If so, the details thereof?

Answers

- See detailed answers *here*

24.3 Lok Sabha: Unstarred Question no. 1812. 10.03.17. Cyber Security Incidents

Questions

- whether the Reserve Bank of India has issued instructions to banks to report any cyber security incident within maximum six hours;
- if so, the details of cyber incidents came to the notice of the various banks in the past six months and reported to RBI;
- whether there is sharp increase in cyber incidents in banks in the past few months ; and
- if so, the details thereof and the reasons therefor and the steps taken by the RBI/other banks to provide fool proof security to bank account holders?

Answers

- See detailed answers *here*

24.4 Lok Sabha Starred Question no 199; 29.07.16: Cyber Security Policy

Questions

- whether Reserve Bank of India (RBI) has noticed any cyber attacks in the banking industry in the recent past and if so, the details thereof;
- the details of financial loss to banks/ individuals by the said attacks during the last three years and the current year;
- whether RBI has asked banks to put in place a cyber security policy to combat cyber threats;
- if so, the details thereof along with the action taken by the banks in this regard; and
- the steps taken / being taken by RBI to strengthen the cybersecurity of financial system in banks?

Answers

- See detailed answers *here*

24.5 Medium Term Recommendations to Strengthen Digital Payments Ecosystem (Digital Payments Committee) December 2016

- The report makes no direct recommendations or policy towards strengthening cyber security. The topic is only covered once throughout the document. The relevant excerpt follows:
- “With respect to the security of the payment system, cyber security framework has been put in place by the RBI. In pursuance to this, the RBI issued instructions to banks to prepare a cyber crisis management place and place a board-approved cyber security policy, prepare a cyber crisis management plan.115 The present framework on cyber security also requires banks to share unusual cyber security incidents with RBI.116 Apart from this, various guidelines have issued for ATM and White Label ATM to adhere to the security measures.”

25.0 National Payments Corporation India

25.1 NPCI Information Security Discipline

- The NPCI Information Security Discipline is a risk management discipline, whose job is to manage the cost of information risk to the business
- Information Security ensures the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity and availability
- Designed a "set of policies and embraced design, implementation and maintenance of these policies, processes, standards and guidelines to manage risks to its information assets, thus ensuring acceptable levels of information security risk."
- They ensure that processes must remain effective and efficient and also adapt to changes that occur in the internal organization and external environment."

25.2 Operational Risk Management

- Defines operational risk as the potential for loss arising from inadequate internal processes, people and systems or from external factors
- Operational Risk Management -> part of the NPCI's Risk Management Framework.
- Its objective is to identify, evaluate, control, measure and report operational risks across the organization
- With operational Risk Management at the centre, the process is as such: identify risk, evaluate risk, control risk, measure risk, monitor risk, report risk.
- This is a framework that applies to NPCI's information security discipline

25.3 Request for Proposal (RFP) for Cyber-Risk Insurance

25.3.1 Objective

- The RFP was published to solicit offers from General Insurers for obtaining a cyber insurance for organization covering all its operations, systems and NPCINET network
- Intends to have a cyber insurance policy to cover first-party and third-party liability coverage to organization when cyber-risk materializes and or cyber security controls at organization fails

25.3.1 Key Focus Areas

- Property and theft
  - Destruction of software system and network
  - Unrecoverable loss of information of organizations stored data
  - Recovery from malware or other malicious codes
  - Business interruption due to cyber incidents
  - Denial of service
  - Information theft- loss of control of customer's data/records
  - Breach of intellectual property
  - Cyber extortion and cyber espionage
  - Losses due to cyber-terrorist acts
  - Harm to electronic media or data contents
  - terrorism/war exclusion with carve back for cyber terrorism
- Liability
  - Network security
  - Private confidential breach/data liability
  - Reputational damage
    - Notification and monitoring
  - Crisis management and response to data theft
  - Cost of repairing, replacing and upgrading computer systems

25.4 Cyber Risk Management and 10 Essential Security Tools 2016-17

25.4.1 Objective

- To discuss the current cybersecurity challenges in the banking and financial institutions in India
- To provide information about the major threat indicators and the risk of data loss

- Present some governance framework to help institutions maintain compliance with the many regulations governing businesses
- Discuss the best possible controls by way of developing essential tools to prevent the organizations from potential cyber security threats which can help organizations defend against threats and mitigate risk

25.4.2 Guidelines/ Recommendations/ Policy

- Cyber risk management must take the following steps to implement successful cyber risk governance:
    1. Establish cyber risk governance
    2. Define cyber risk boundary
    3. Identify critical business processes and assets
    4. Assess cyber threats
    5. Collection, analysis and reporting of information
    6. Plan and respond
- Ten essential security tools
    1. Firewall
    2. Network access control (NAC)
    3. Intrusion prevention system (IPS) / Intrusion Detection System
    4. Advanced Persistent Threat (APT) prevention
    5. Anti-Virus/Anti Malware protection
    6. Web proxy & content filtering
    7. Security incident and event management (SIEM)
    8. Anti-Distributed Denial of Service (DDoS)
    9. Data Loss Prevention (DLP)
    10. Data Backup and Recovery Solution

See link above for detailed descriptions of each recommendation/ guidelines

25.5 Privacy and Security Policy of NPCI

25.5.1 Objective

- To maintain and protect the privacy, secrecy, security and integrity of the information received by it from persons accessing its website, its members and their customers in accordance with applicable statutes, rules, regulations and directions issued thereunder.

25.5.2 Relevant Policy

- Privacy and Security of Websites:
    - When a person visits NPCI's website, the website administrator uses cookies to monitor the edit facility used by NPCI and to collect statistics by browser users, including information about the time and date when a visitor accessed the site, the pages he visited, the Internet domain and IP address from which he accessed the site and information on the browsing software he/ she used to access the site.
    - No attempt is made to gather or keep personal details to identify users except, in an unlikely event of an investigation, where a law enforcement agency may exercise a power to inspect activity logs.
- Protection of Information:
    - Use of firewalls, encryption and data leakage prevention technologies to protect information
    - Audit of all vendors and service providers and execution of non-disclosure agreements before availing their services;
    - Continuous monitoring of NPCI's physical and technical environment for vulnerabilities and potential intrusions and implementation of controls to identify and address any concern related to protection of data.
    - NPCI has comprehensive documented information security policy & procedures and certified for Payment Card Industry – Data Security Standard (PCI-DSS), ISO27001 – ISMS to ensure that the information provided to it is reasonably secure, available and with assured quality

26.0 Electronics and Information Technology Department Government of Odisha

26.1 Crisis Management Plan For Cyber Security in Odisha (2016)

26.1 Crisis Management Plan For Cyber Security in Odisha (2016)

26.1.1 Objective

- To ensure that interruption or manipulations of critical functions/ services in critical sector organizations of the state are brief, infrequent and manageable and cause least possible damage.
- To enable respective administrative Departments to draw-up their own contingency plans in line with Crisis Management Plan for countering cyber-attacks and cyber terrorism, equip themselves suitably to implement, supervise implementation and ensure compliance among all the organizational units within their domains.
- To assist organizations to put in place mechanisms to effectively deal with cyber security crisis and be able to identify responsibilities and accountabilities right down to individual level

26.1.2 Guidelines/ Recommendations/ Policy

- Below are the main focus areas for which the plan provides recommendations/guidelines. The document can be viewed at the link given above.
- Cyber crisis and contingencies
- Prevention strategies and plans
- Crisis recognition and mitigation plan

26.1.3 Scope

- The policy/plan is intended to cater for the whole spectrum of ICT users and providers including small/home users, medium and large enterprises, and government and non-government entities

27.0 National Technical Research Organization (NTRO)

27.1 Inter-ministerial Task Force on Cyber Defence and Preparedness (2010)

27.1 Inter-ministerial Task Force on Cyber Defence and Preparedness (2010)[6]

- One of the earlier multi-stakeholder initiatives on cyber defence
- Helped inform india’s cyber policy and future organizations
- No further information available online, this was mentioned briefly in the CRI report.

[6] *http://www.potomacinstitute.org/images/CRI/CRI_India_Profile.pdf* page 6

28.0 Participation in International efforts (summits, conventions, standards, working groups, discussions, agreements etc)

28.1 “MoU of Obligations” with the Council of the SCO Heads of States[7]

- India is not yet a member of the Shanghai Cooperation Organization (SCO) “Agreement on Cooperation in the Field of Ensuring International Information Security”
- However, the Indian government signed an MoU with the intention of gaining full-fledged membership, which is likely to be accepted at the CSO summit in June 2017.

28.2 UNGGE (United Nations Group of Government Experts)

- India has participated in the United Nations Group of Government Experts (UN GGE) in the context of international security and ICT
- Attended by Mr. B. J. Srinath, Senior Director of the Indian Computer Emergency Response Team Department of Information Technology India
- Focus areas:
  - Threats, risks and vulnerabilities
  - Cooperative measures
  - Recommendations

28.3 United Nations Commission on Science and Technology Working Group on Enhanced Cooperation

- “Statement by India at 15th session of United Nations Commission on science and Technology for Development, at the briefing meeting on open consultation on Enhanced Cooperation on Public Policy issues related to Internet, delivered by Smt. Alpana Dubey, First Secretary (Economic), on May 22, 2012”
- *“We would strongly urge that the process of discussion on all aspects of internet governance that have been raised so far, should continue. That would aim at keeping the Internet sustainable, robust, secure and stable and promoting a developmental agenda through the Internet.”*

28.4 United Nations Office on Drugs and Crime Open Ended Intergovernmental Working Group on Cybercrime

- According to the CRI Report, India participated in the United Nations Office on Drugs and Crime Open Ended Intergovernmental Working Group on Cybercrime[8]

28.5 India’s MoU’s and Joint Statements

- India has Joint statements/MoUs, related to cyber security, with several countries listed below. For details on the types of agreements and areas of cooperation, please view the CIS spreadsheet linked above:
  - Australia, Bangladesh, Belgium, Brazil, Brunei, Canada, China, Colombia, Egypt, Finland, France, Germany, Indonesia, Israel, Italy, Japan, Kazakhstan, Kenya, South Korea, Malaysia, Mauritius, Mongolia, Myanmar, New Zealand, Portugal, Qatar, Russia, Saudi Arabia, Serbia, Singapore, South Africa, Sweden, Thailand, Tunisia, UAE, UK, USA, Uzbekistan, Vietnam

28.6 India’s Bilateral Cyber Frameworks

- India has established (or discussed establishing) cyber frameworks with USA, UK, Singapore, Russia, Malaysia, Japan, Egypt, China and Australia
- For details on the types of frameworks and areas of focus, please view the CIS spreadsheet linked above

[7] *http://www.potomacinstitute.org/images/CRI/CRI_India_Profile.pdf* Page 12

[8] *http://www.potomacinstitute.org/images/CRI/CRI_India_Profile.pdf* page 16

Cybersecurity Mapping

Mapping of Sections in India’s MLAT Agreements

Mapping of India’s Cyber Security-Related Bilateral Agreements

Mapping of Sections in India’s MLAT Agreements

LEILAH ELMOKADEM

This info-graphic diagram intends to map out and compare the various sections that exist in the 39 MLATs (mutual legal assistance treaty) between India and other countries. An MLAT is an agreement between two or more countries, drafted for the purpose of gathering and exchanging information in an effort to enforce public or criminal laws.

We have found that India’s 39 MLAT documents are worded, formatted and sectioned differently. At the same time, many of the same sections exist across several MLATs. This diagram lists the sections found in the MLAT documents and indicates the treaties in which they were included or not included. To keep the list of sections concise and to more easily pinpoint the key differences between the agreements, we have merged sections that are synonymous in meaning but were worded slightly differently. For example: we would combine “Entry into force and termination” with “Ratification and termination” or “Expenses” with “Costs”. At the same time, some sections that seemed quite similar and possible to merge were kept separate due to potential key differences that could be overlooked as a result. For example: “Limitation on use” vs. “Limitation on compliance” or “Serving of documents” vs. “Provision of (publicly available) documents/records/objects” remained separate for further analysis and comparison.

These differences in sectioning can be analysed to facilitate a thorough comparison between the effectiveness, efficiency, applicability and enforceability of the various provisions across the MLATs. The purpose of this initial mapping is to provide an overall picture of which sections exist in which MLAT documents. There will be further analysis of these sections to produce a more holistic content-based comparison of the MLATs.

🟧 Yes ⬜ No

SECTION	Australia	Azerbaijan	Bahrain	Bangladesh	Belarus	Bosnia & Herzegovina	Bulgaria	Canada	Egypt	France	Hong Kong	Iran	Indonesia	Israel	Kazakhstan	Kyrgyz Republic	Kuwait	Malaysia	Mauritius	Mexico	Mongolia	Myanmar	Russia	Singapore	South Africa	South Korea	Spain	Sri Lanka	Switzerland	Oman	Tajikistan	Thailand	Turkey	Ukraine	UAE	UK	USA	Uzbekistan	Vietnam	Total	
																																								Yes	No
Scope of application	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	⬜	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	38	1
Definitions	🟧	🟧	🟧	🟧	🟧	🟧	🟧	⬜	🟧	⬜	⬜	🟧	⬜	🟧	🟧	⬜	🟧	⬜	🟧	🟧	⬜	🟧	⬜	⬜	🟧	⬜	🟧	🟧	⬜	🟧	⬜	⬜	⬜	🟧	🟧	🟧	⬜	⬜	🟧	23	16
Compatibility with other treaties	🟧	🟧	🟧	⬜	🟧	🟧	⬜	⬜	⬜	⬜	⬜	🟧	⬜	🟧	⬜	⬜	⬜	🟧	🟧	⬜	⬜	🟧	⬜	🟧	🟧	⬜	⬜	🟧	⬜	⬜	🟧	🟧	⬜	⬜	⬜	⬜	🟧	🟧	🟧	18	21
Central authorities	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	⬜	🟧	🟧	🟧	⬜	🟧	🟧	🟧	🟧	🟧	🟧	37	2
Refusal or postponement of assistance	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	⬜	⬜	🟧	🟧	🟧	🟧	🟧	🟧	⬜	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	⬜	🟧	🟧	🟧	🟧	🟧	🟧	🟧	⬜	🟧	🟧	34	5
Contents of requests	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	⬜	⬜	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	⬜	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	36	3
Language	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	⬜	🟧	⬜	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	⬜	🟧	🟧	⬜	🟧	🟧	🟧	🟧	🟧	🟧	🟧	⬜	🟧	🟧	34	5
Execution of requests	🟧	🟧	⬜	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	⬜	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	37	2
Return of material to requested state	🟧	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟧	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟧	⬜	⬜	⬜	🟧	⬜	🟧	5	34
Confidentiality	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	⬜	⬜	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	⬜	🟧	🟧	🟧	⬜	🟧	🟧	🟧	⬜	🟧	🟧	34	5
Service of documents	🟧	🟧	⬜	⬜	🟧	🟧	🟧	⬜	🟧	🟧	🟧	⬜	🟧	🟧	🟧	🟧	⬜	🟧	🟧	🟧	🟧	🟧	🟧	⬜	🟧	🟧	⬜	🟧	🟧	🟧	🟧	🟧	⬜	⬜	⬜	⬜	⬜	🟧	🟧	27	12
Taking evidence (in the requested state)	🟧	🟧	🟧	🟧	⬜	🟧	⬜	🟧	🟧	⬜	⬜	🟧	🟧	🟧	🟧	⬜	🟧	🟧	🟧	🟧	⬜	🟧	⬜	🟧	🟧	🟧	🟧	🟧	🟧	🟧	⬜	🟧	⬜	🟧	🟧	⬜	⬜	⬜	🟧	27	12
Obtaining statements of persons	🟧	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟧	⬜	🟧	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟧	⬜	⬜	4	35
Availability/transfer of persons in custody to give evidence or assist in investigations	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	⬜	🟧	⬜	🟧	🟧	⬜	🟧	🟧	🟧	⬜	🟧	🟧	⬜	🟧	🟧	🟧	34	5
Availability/transfer of other persons to give evidence or assist in investigations	🟧	⬜	🟧	🟧	🟧	⬜	🟧	🟧	🟧	🟧	🟧	🟧	⬜	⬜	⬜	🟧	🟧	⬜	⬜	🟧	🟧	⬜	🟧	⬜	⬜	🟧	🟧	⬜	⬜	🟧	🟧	⬜	⬜	🟧	🟧	⬜	🟧	🟧	🟧	24	15

🟧 Yes ⬜ No

SECTION	Australia	Azerbaijan	Bahrain	Bangladesh	Belarus	Bosnia & Herzegovina	Bulgaria	Canada	Egypt	France	Hong Kong	Iran	Indonesia	Israel	Kazakhstan	Kyrgyz Republic	Kuwait	Malaysia	Mauritius	Mexico	Mongolia	Myanmar	Russia	Singapore	South Africa	South Korea	Spain	Sri Lanka	Switzerland	Oman	Tajikistan	Thailand	Turkey	Ukraine	UAE	UK	USA	Uzbekistan	Vietnam	Total	
																																								Yes	No
Safe conduct	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	⬜	🟧	🟧	🟧	⬜	🟧	🟧	⬜	⬜	🟧	🟧	35	4
Provision of (publicly available) documents/records/objects	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	⬜	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	⬜	🟧	🟧	⬜	🟧	🟧	⬜	35	4
Certification/authentication	🟧	⬜	🟧	🟧	⬜	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	⬜	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	⬜	🟧	🟧	⬜	⬜	🟧	🟧	🟧	⬜	🟧	⬜	31	8
Search and seizure	🟧	🟧	⬜	⬜	⬜	🟧	🟧	⬜	🟧	🟧	🟧	⬜	🟧	🟧	⬜	🟧	⬜	🟧	🟧	⬜	🟧	🟧	🟧	🟧	🟧	🟧	⬜	🟧	⬜	🟧	🟧	🟧	⬜	⬜	⬜	⬜	🟧	🟧	🟧	25	14
Proceeds and instruments of crime	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	⬜	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	⬜	🟧	🟧	🟧	🟧	⬜	🟧	🟧	🟧	⬜	🟧	🟧	⬜	⬜	🟧	🟧	33	6
Representation and expenses	🟧	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟧	🟧	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟧	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟧	5	34
Consultation	🟧	🟧	⬜	⬜	🟧	🟧	⬜	🟧	⬜	⬜	⬜	🟧	🟧	🟧	⬜	🟧	⬜	🟧	🟧	🟧	🟧	🟧	🟧	⬜	🟧	🟧	⬜	🟧	⬜	🟧	🟧	🟧	⬜	⬜	⬜	⬜	🟧	🟧	🟧	24	15
Entry into force/ratification and termination	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	⬜	⬜	🟧	🟧	🟧	🟧	🟧	⬜	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	⬜	🟧	🟧	🟧	🟧	🟧	🟧	⬜	🟧	🟧	🟧	34	5
Presence of persons at the execution of requests	⬜	🟧	⬜	⬜	⬜	🟧	⬜	⬜	⬜	🟧	🟧	⬜	🟧	🟧	⬜	🟧	⬜	🟧	🟧	⬜	⬜	🟧	🟧	🟧	🟧	⬜	⬜	🟧	⬜	⬜	🟧	🟧	⬜	⬜	⬜	⬜	🟧	🟧	🟧	19	20
Providing evidence or assisting investigations in the requesting state	⬜	🟧	⬜	⬜	⬜	🟧	⬜	⬜	⬜	⬜	🟧	⬜	🟧	⬜	⬜	⬜	⬜	⬜	🟧	⬜	⬜	🟧	⬜	⬜	🟧	⬜	⬜	🟧	⬜	⬜	⬜	🟧	⬜	⬜	⬜	🟧	⬜	⬜	⬜	10	29
Funds meant for financing acts of terrorism	⬜	🟧	⬜	⬜	⬜	🟧	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟧	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟧	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟧	5	34
Limitation on use	⬜	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	⬜	🟧	🟧	🟧	🟧	🟧	🟧	🟧	⬜	🟧	🟧	🟧	⬜	🟧	🟧	🟧	🟧	🟧	⬜	34	5
Legalization	⬜	🟧	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	1	38
Expenses/Costs	⬜	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	⬜	⬜	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	⬜	🟧	🟧	🟧	⬜	🟧	🟧	🟧	🟧	🟧	⬜	33	6
Amendment	⬜	🟧	⬜	⬜	⬜	🟧	⬜	⬜	⬜	⬜	⬜	🟧	🟧	⬜	🟧	⬜	⬜	🟧	🟧	⬜	⬜	⬜	⬜	🟧	🟧	⬜	⬜	🟧	⬜	🟧	⬜	🟧	⬜	⬜	⬜	⬜	⬜	⬜	⬜	12	27

■ Yes □ No

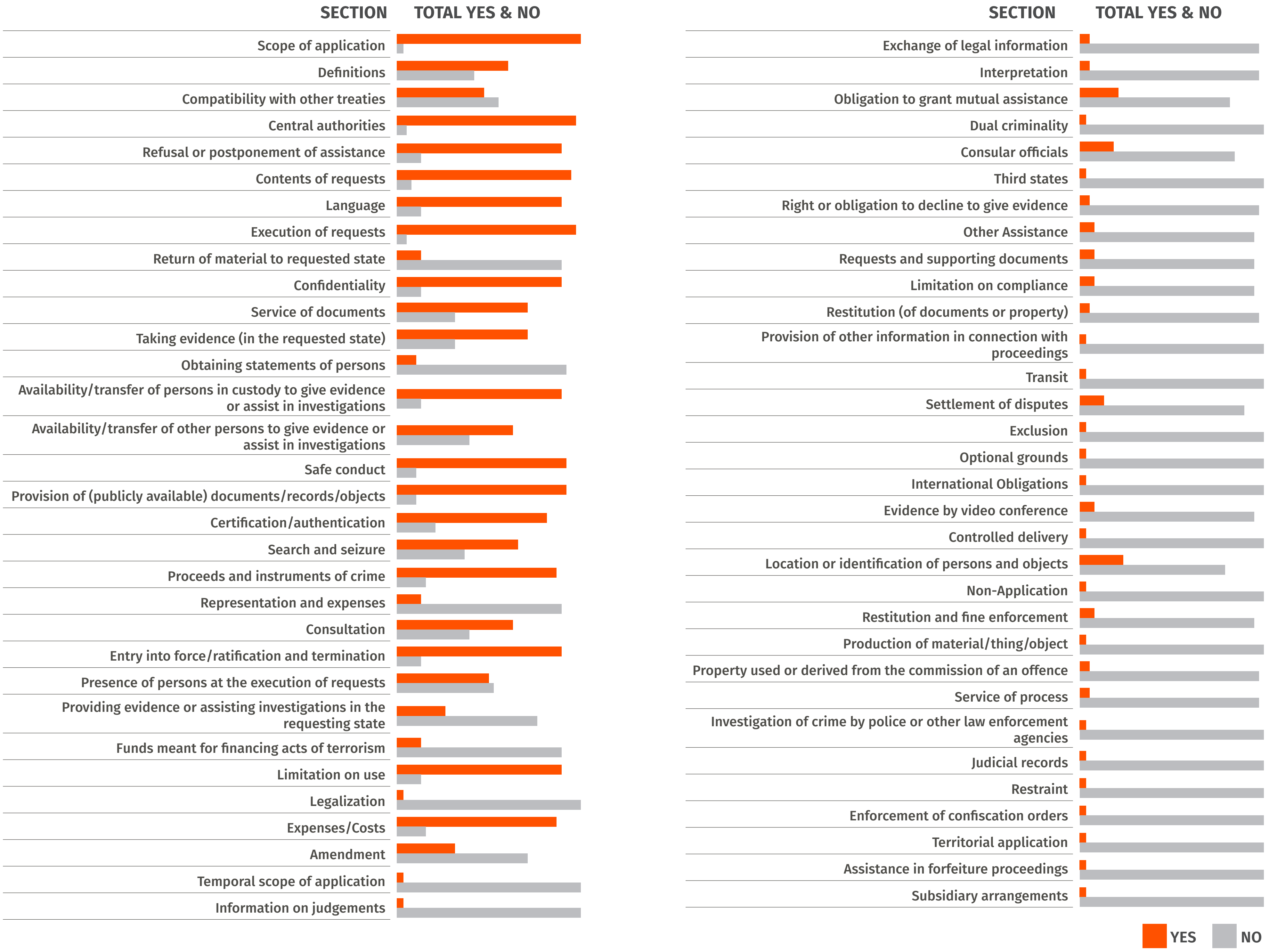
SECTION	Australia	Azerbaijan	Bahrain	Bangladesh	Belarus	Bosnia & Herzegovina	Bulgaria	Canada	Egypt	France	Hong Kong	Iran	Indonesia	Israel	Kazakhstan	Kyrgyz Republic	Kuwait	Malaysia	Mauritius	Mexico	Mongolia	Myanmar	Russia	Singapore	South Africa	South Korea	Spain	Sri Lanka	Switzerland	Oman	Tajikistan	Thailand	Turkey	Ukraine	UAE	UK	USA	Uzbekistan	Vietnam	Total	
																																								Yes	No
Temporal scope of application	□	□	□	□	■	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	1	38
Information on judgements	□	□	□	□	□	□	■	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	1	38
Exchange of legal information	□	□	□	□	□	□	■	□	□	■	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	2	37
Interpretation	□	□	□	□	□	□	■	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	■	□	□	□	□	□	□	2	37
Obligation to grant mutual assistance	□	□	□	□	□	□	□	■	□	□	□	□	□	□	□	■	□	□	□	□	■	□	■	□	□	□	□	□	□	□	■	□	■	□	□	■	□	■	□	8	31
Dual criminality	□	□	□	□	□	□	□	■	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	1	38
Consular officials	□	□	□	□	□	□	□	■	□	□	□	□	□	□	□	■	□	□	□	□	■	□	■	□	□	□	□	□	□	□	■	■	□	□	□	□	□	■	□	7	32
Third states	□	□	□	□	□	□	□	■	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	1	38
Right or obligation to decline to give evidence	□	□	□	□	□	□	□	□	■	□	□	□	□	□	□	□	□	■	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	2	37
Other Assistance	□	□	□	□	□	□	□	■	□	■	■	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	3	36
Requests and supporting documents	□	□	□	□	□	□	□	□	□	■	■	□	□	□	□	□	□	■	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	3	36
Limitation on compliance	□	□	□	□	□	□	□	□	□	■	■	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	■	□	□	3	36
Restitution (of documents or property)	□	□	□	□	□	□	□	□	□	■	□	□	□	■	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	2	37
Provision of other information in connection with proceedings	□	□	□	□	□	□	□	□	□	■	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	1	38
Transit	□	□	□	□	□	□	□	□	□	■	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	1	38
Settlement of disputes	□	□	□	□	□	□	□	□	□	■	■	□	■	□	■	□	□	□	□	■	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	5	34

🟧 Yes ⬜ No

SECTION	Australia	Azerbaijan	Bahrain	Bangladesh	Belarus	Bosnia & Herzegovina	Bulgaria	Canada	Egypt	France	Hong Kong	Iran	Indonesia	Israel	Kazakhstan	Kyrgyz Republic	Kuwait	Malaysia	Mauritius	Mexico	Mongolia	Myanmar	Russia	Singapore	South Africa	South Korea	Spain	Sri Lanka	Switzerland	Oman	Tajikistan	Thailand	Turkey	Ukraine	UAE	UK	USA	Uzbekistan	Vietnam	Total	
																																								Yes	No
Exclusion	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟧	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	1	38
Optional grounds	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟧	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	1	38
International Obligations	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟧	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	1	38
Evidence by video conference	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟧	⬜	🟧	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	3	36
Controlled delivery	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟧	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	1	38
Location or identification of persons and objects	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟧	⬜	🟧	⬜	⬜	🟧	⬜	🟧	🟧	⬜	⬜	⬜	⬜	⬜	⬜	🟧	🟧	⬜	⬜	⬜	⬜	🟧	🟧	⬜	9	30
Non-Application	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟧	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	1	38
Restitution and fine enforcement	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟧	⬜	⬜	⬜	⬜	⬜	🟧	⬜	⬜	🟧	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	3	36
Production of material/thing/ object	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟧	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	1	38
Property used or derived from the commission of an offence	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟧	⬜	⬜	⬜	⬜	🟧	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	2	37
Service of process	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟧	⬜	⬜	⬜	⬜	🟧	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	2	37
Investigation of crime by police or other law enforcement agencies	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟧	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	1	38
Judicial records	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟧	⬜	⬜	⬜	⬜	⬜	⬜	1	38
Restraint	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟧	⬜	⬜	⬜	1	38
Enforcement of confiscation orders	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟧	⬜	⬜	⬜	1	38

🟧 Yes ⬜ No

SECTION	Australia	Azerbaijan	Bahrain	Bangladesh	Belarus	Bosnia & Herzegovina	Bulgaria	Canada	Egypt	France	Hong Kong	Iran	Indonesia	Israel	Kazakhstan	Kyrgyz Republic	Kuwait	Malaysia	Mauritius	Mexico	Mongolia	Myanmar	Russia	Singapore	South Africa	South Korea	Spain	Sri Lanka	Switzerland	Oman	Tajikistan	Thailand	Turkey	Ukraine	UAE	UK	USA	Uzbekistan	Vietnam	Total Yes	No
Territorial application	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟧	⬜	⬜	⬜	1	38
Assistance in forfeiture proceedings	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟧	⬜	⬜	1	38
Subsidiary arrangements	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟧	1	38


SECTION
TOTAL YES & NO
Scope of application
Definitions
Compatibility with other treaties
Central authorities
Refusal or postponement of assistance
Contents of requests
Language
Execution of requests
Return of material to requested state
Confidentiality
Service of documents
Taking evidence (in the requested state)
Obtaining statements of persons
Availability/transfer of persons in custody to give evidence or assist in investigations
Availability/transfer of other persons to give evidence or assist in investigations
Safe conduct
Provision of (publicly available) documents/records/objects
Certification/authentication
Search and seizure
Proceeds and instruments of crime
Representation and expenses
Consultation
Entry into force/ratification and termination
Presence of persons at the execution of requests
Providing evidence or assisting investigations in the requesting state
Funds meant for financing acts of terrorism
Limitation on use
Legalization
Expenses/Costs
Amendment
Temporal scope of application
Information on judgements
SECTION
TOTAL YES & NO
Exchange of legal information
Interpretation
Obligation to grant mutual assistance
Dual criminality
Consular officials
Third states
Right or obligation to decline to give evidence
Other Assistance
Requests and supporting documents
Limitation on compliance
Restitution (of documents or property)
Provision of other information in connection with proceedings
Transit
Settlement of disputes
Exclusion
Optional grounds
International Obligations
Evidence by video conference
Controlled delivery
Location or identification of persons and objects
Non-Application
Restitution and fine enforcement
Production of material/thing/object
Property used or derived from the commission of an offence
Service of process
Investigation of crime by police or other law enforcement agencies
Judicial records
Restraint
Enforcement of confiscation orders
Territorial application
Assistance in forfeiture proceedings
Subsidiary arrangements
YES
NO

Mapping of India’s Cyber Security-Related Bilateral Agreements

LEILAH ELMOKADEM

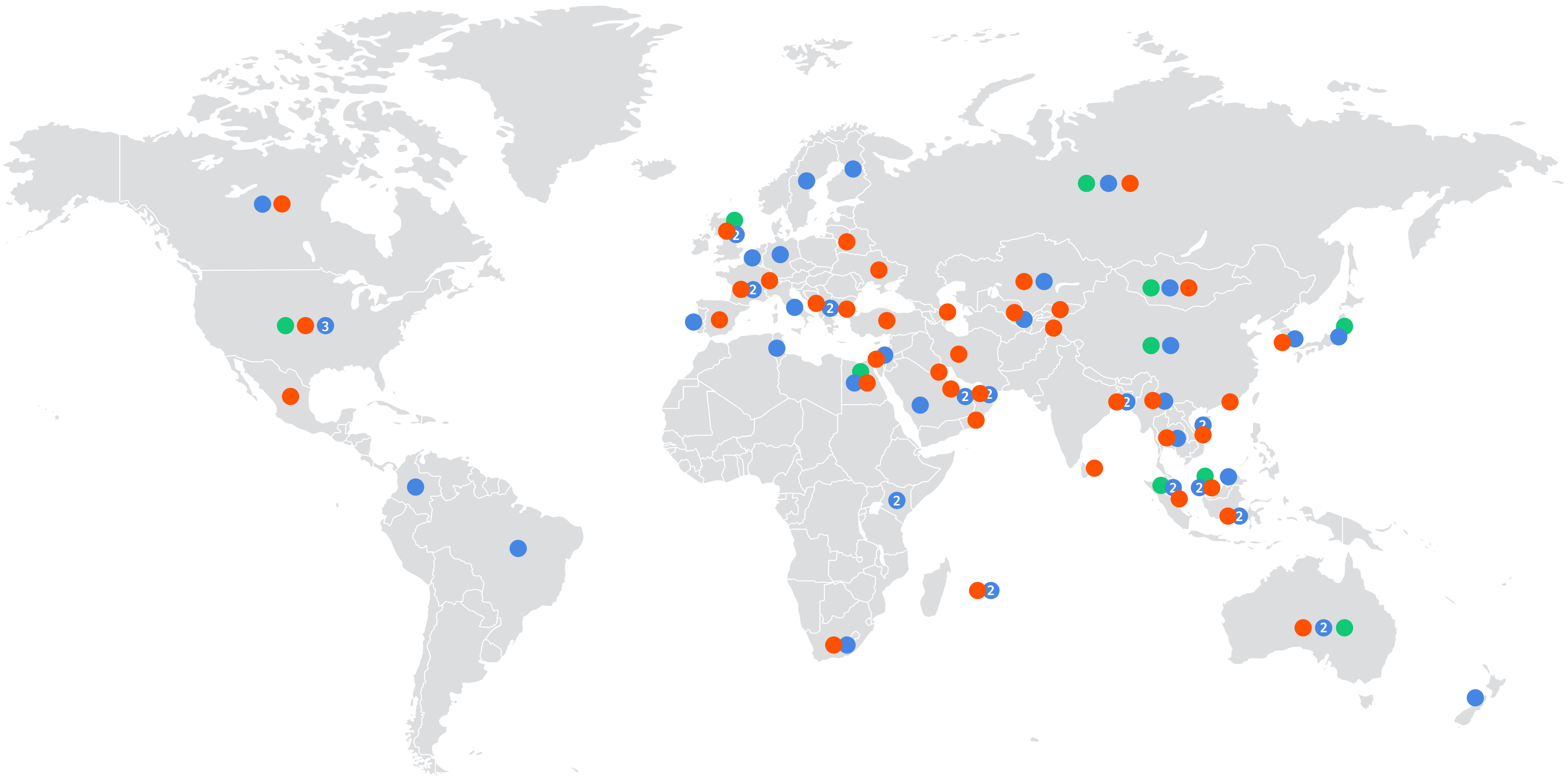
With the rapid spread of cloud computing and the growth of cyber spaces, large masses of information are now easily transmittable transnationally, necessitating the ratification of new agreements and cooperation efforts amongst states in order to secure cyber spaces and regulate exchanges of information. In an attempt to understand the nature and extent of current international collaborative efforts in cyber security, we have compiled the following data regarding India’s cyber security-related bilateral agreements. The intention of this exercise is to offer a dynamic visualization that demonstrates which countries India has collaborated with on cyber security efforts and initiatives. This is an ongoing map that we will be updating as our research continues.

The data used for the info-graphic consists of India’s MLATs, cyber security-related MoUs and Joint Statements, and Cyber Frameworks. An MLAT is an agreement between two or more countries, drafted for the purpose of gathering and exchanging information in an effort to enforce public or criminal laws. A MoU (Memorandum of Understanding) is a nonbinding agreement between two or more states outlining the terms and details of an understanding, including each party’s requirements and responsibility; it is often the first stage in the formation of a formal contract. For the purpose of this research, we have grouped Joint Statements with MoUs, as they both generally entail the informal agreement between two states to strengthen cooperation on certain issues. Lastly, a Cyber Framework consists of standards, guidelines and practices to promote protection of critical infrastructure. The data accounts for agreements centered on cyber security as well as any agreements mentioning cooperation efforts in Cyber security, information security or cybercrime.

● MLAT Agreements with India

● MOUs/ Joint Statements with India

● Cyber Frameworks with India



39
MLAT
AGREEMENTS

54
MOUs/ JOINT
STATEMENTS

10
CYBER
FRAMEWORKS

COUNTRY	MLAT AGREEMENT	MOUs/ JOINT STATEMENTS WITH INDIA	DATES	COMMENTS	CYBER FRAMEWORKS WITH INDIA
Afghanistan	n/a	n/a		n/a	n/a
Albania	n/a	n/a		n/a	n/a
Algeria	n/a	n/a		n/a	n/a
American Samoa	n/a	n/a		n/a	n/a
Andorra	n/a	n/a		n/a	n/a
Angola	n/a	n/a		n/a	n/a
Anguilla	n/a	n/a		n/a	n/a
Antigua & Barbuda	n/a	n/a		n/a	n/a
Argentina	n/a	n/a		n/a	n/a
Armenia	n/a	n/a		n/a	n/a
Aruba	n/a	n/a		n/a	n/a
Australia	http://cbi.nic.in/interpol/mlat/Australia.pdf	http://mea.gov.in/bilateral-documents.htm?dtl/25774/Joint+Statement+Inaugural+IndiaAustralia+Cyber+Policy+Dialogue	Aug 2015	Signed a framework for operational cooperation on cyber security to promote greater cooperation in exchanging information on cyber threats and in responding to incidents.	http://www.regionalsecurity.org.au/Resources/Documents/11-1%20-%20Brewster.pdf
		http://www.dnaindia.com/india/report-india-australia-sign-mous-on-combating-terrorism-civil-aviation-security-2393843	Apr 2017	MoU is about combating terrorism and civil aviation security- but cybersecurity is mentioned	n/a
Austria	n/a	n/a		n/a	n/a
Azerbaijan	http://cbi.nic.in/interpol/mlat/Azerbaijan.pdf	n/a		n/a	n/a
Bahamas	n/a	n/a		n/a	n/a

COUNTRY	MLAT AGREEMENT	MOUs/ JOINT STATEMENTS WITH INDIA	DATES	COMMENTS	CYBER FRAMEWORKS WITH INDIA
Bahrain	http://cbi.nic.in/interpol/mlat/Baharin.pdf	n/a		Signed a pact with Bahrain to fight terrorism, part of it aims to strengthen cooperation and information sharing to ensure speedier investigations and prosecutions of traffickers and organised crime syndicates in either country. There is no mention here of cyber or information security- but information sharing might be relevant to info/cyber security	n/a
Bangladesh	http://cbi.nic.in/interpol/mlat/Bangladesh.pdf	http://www.thehindu.com/news/national/narendra-modis-visit-to-bangladesh-india-to-set-up-it-listening-posts-in-bangladesh/article7257395.ece	May 29	MoU for India to help strengthening IT infrastructure in Bangladesh, much in the name of "security".	n/a
		http://www.thefinancialexpress-bd.com/2017/04/11/66547/List-of-total-MOUs,-agreement,-SOPs-signed-between-BD,India/print http://www.theindependentbd.com/arcprint/details/89237/2017-04-09	Apr 2017	Memorandum of Understanding between the Indian Computer Emergency Response Team (CERT-In), Ministry of Electronics and Information Technology, Republic of India And ICT Division, Bangladesh on Cooperation in the area of Cyber Security.	n/a
Barbados	n/a	n/a		n/a	n/a
Belarus	http://cbi.nic.in/interpol/mlat/Belarus.pdf	n/a		n/a	n/a
Belgium	n/a	http://www.mea.gov.in/bilateral-documents.htm?dtl/26574/IndiaBelgium+Joint+Statement+during+the+visit+of+Prime+Minister+to+Belgium+March+30+2016	Mar 2016	Cooperation on cyber security mentioned under "Energy, Ports, Information Technology" section	n/a
Belize	n/a	n/a		n/a	n/a
Benin	n/a	n/a		n/a	n/a
Bermuda	n/a	n/a		n/a	n/a

COUNTRY	MLAT AGREEMENT	MOUs/ JOINT STATEMENTS WITH INDIA	DATES	COMMENTS	CYBER FRAMEWORKS WITH INDIA
Bhutan	n/a	n/a		n/a	n/a
Bolivia	n/a	n/a		n/a	n/a
Bosnia & Herzegovina	http://cbi.nic.in/interpol/mlat/Bosnia&Herzegovina.pdf	n/a		n/a	n/a
Botswana	n/a	n/a		n/a	n/a
Brazil	n/a	http://mea.gov.in/bilateral-documents.htm?dtl/26045/Joint+Statement+on+the+7th+IndiaBrazil+Joint+Commission+Meeting+and+Agreed+Minutes+November+1819+2015	Nov 2015	Section 49 on Cyber Security	n/a
British Virgin Is.	n/a	n/a		n/a	n/a
Brunei	n/a	http://meity.gov.in/content/asia		Information security and cyber crime amongst ICT areas of cooperation	n/a
Bulgaria	http://cbi.nic.in/interpol/mlat/Bulgaria.pdf	n/a		n/a	n/a
Burkina Faso	n/a	n/a		n/a	n/a
Burma	n/a	n/a		n/a	n/a
Burundi	n/a	n/a		n/a	n/a
Cambodia	n/a	n/a		n/a	n/a
Cameroon	n/a	n/a		n/a	n/a
Canada	http://cbi.nic.in/interpol/mlat/Canada.pdf	http://mea.gov.in/bilateral-documents.htm?dtl/25073	Apr 2015	Intends to promote establishment of a broader framework and exchange of information on cyber security incidents, policies and best practices.	n/a
Cabo Verde	n/a	n/a		n/a	n/a
Cayman Islands	n/a	n/a		n/a	n/a
Central African Rep.	n/a	n/a		n/a	n/a
Chad	n/a	n/a		n/a	n/a

COUNTRY	MLAT AGREEMENT	MOUs/ JOINT STATEMENTS WITH INDIA	DATES	COMMENTS	CYBER FRAMEWORKS WITH INDIA
Chile	n/a	n/a		n/a	n/a
China	n/a	https://internetdemocracy.in/2015/12/with-or-without-us-bilateralism-india-cybersecurity-policies/	Nov 2015	During an official visit of Home Minister Rajnath Singh to Beijing, China and India agreed to set up a mechanism at the Home Minster Level, to strengthen collaboration on, among other things, cybercrime	http://www.hindustantimes.com/india/india-china-to-set-up-framework-on-terrorism-cyber-crime-drug-trafficking/story-kuyAypr8wWKABbue9h0i0L.html
Colombia	n/a	http://www.mea.gov.in/bilateral-documents.htm?dtl/7538/India+and+Colombia+Sign+MoU+for+Cooperation+in+Information+Technology+MoU+to+establish+Bilateral+Task+Force+to+Dentify+Deliverables+in+it+sector+Shri+Pramod+Mahajan+and+Dr+Ngela+Montoya+Holguin+Sign+MoU	Apr 2002	Information Security and Cyber Crime as one of the areas of cooperation	n/a
Comoros	n/a	n/a		n/a	n/a
DRC (Democratic Republic of the Congo)	n/a	n/a		n/a	n/a
Republic of the Congo	n/a	n/a		n/a	n/a
Cook Islands	n/a	n/a		n/a	n/a
Costa Rica	n/a	n/a		n/a	n/a
Cote d'Ivoire	n/a	n/a		n/a	n/a
Croatia	n/a	n/a		MoU on cooperation in Information Technology: signed between Electronics & Computer Software Export Prom - but no agreements on cyber/info security	n/a
Cuba	n/a	n/a		n/a	n/a
Cyprus	n/a	n/a		n/a	n/a
Czech Republic	n/a	n/a		n/a	n/a
Denmark	n/a	n/a		n/a	n/a

COUNTRY	MLAT AGREEMENT	MOUs/ JOINT STATEMENTS WITH INDIA	DATES	COMMENTS	CYBER FRAMEWORKS WITH INDIA
Djibouti	n/a	n/a		n/a	n/a
Dominica	n/a	n/a		http://dominicanewsonline.com/news/homepage/news/technology/dominica-embarks-on-major-ict-project/ No agreements ON Cyber security but: the India and Dominica signed a MOU for the development of the center and Permanent Secretary in the Ministry of Information, Science, Telecommunications and Technology - and the article indicates that cyber security is one of the areas for this ministry	n/a
Dominican Republic	n/a	n/a		n/a	n/a
East Timor	n/a	n/a		n/a	n/a
Ecuador	n/a	n/a		n/a	n/a
Egypt	http://cbi.nic.in/interpol/mlat/Ezypt.pdf	http://techmoran.com/egypt-signs-5-mous-with-india-on-it-cyber-security-space-education-to-launch-a-nano-egyptian-satellite-soon/	Mar 2013	Not much detail provided online; generally MOUs cover cyber security, information technology, space and education in a move that will increase co-operation in science and technology between the countries.	http://mea.gov.in/press-releases.htm?dtl/27890/First_Dialogue_between_India_and_Egypt_on_Cyber_Issues_held_in_New_Delhi_December_2022_2016
El Salvador	n/a	n/a		n/a	n/a
Equatorial Guinea	n/a	n/a		n/a	n/a
Eritrea	n/a	n/a		n/a	n/a
Estonia	n/a	n/a		http://www.ega.ee/news/indian-digital-developer-gathering-from-estonia-ideas-for-digital-india/	n/a
Ethiopia	n/a	n/a		n/a	n/a

COUNTRY	MLAT AGREEMENT	MOUs/ JOINT STATEMENTS WITH INDIA	DATES	COMMENTS	CYBER FRAMEWORKS WITH INDIA
Faroe Islands	n/a	n/a		n/a	n/a
Fiji	n/a	n/a		n/a	n/a
Finland	n/a	http://www.business-standard.com/article/pti-stories/gfsu-to-ink-mou-with-finland-based-company-for-cyber-security-114120100155_1.html	Dec 2014	Non-governmental: Indian university signs MoU with Finnish cyber security company	n/a
France	http://cbi.nic.in/interpol/mlat/France.pdf	http://meity.gov.in/content/active-mous	Sep 2000	Information security and cyber crime as one of the cooperation areas	n/a
		http://www.thehindu.com/news/resources/Full-text-of-Joint-Statement-issued-by-India-France/article14019524.ece	Jan 2016	The President of France and the Prime Minister of India agreed to intensify cooperation between the Indian and French security forces in the fields of homeland security, cyber security, Special Forces and intelligence-sharing to fight against criminal networks and tackle the common threat of terrorism.	n/a
French Guiana	n/a	n/a		n/a	n/a
French Polynesia	n/a	n/a		n/a	n/a
Gabon	n/a	n/a		n/a	n/a
Gambia	n/a	n/a		n/a	n/a
Gaza Strip	n/a	n/a		n/a	n/a
Georgia	n/a	n/a		n/a	n/a
Germany	n/a	http://pib.nic.in/newsite/PrintRelease.aspx?relid=128443	Oct 2015	Cyber crime as one of the areas covered in the MoU around security cooperation- no mention of cyber security	n/a
Ghana	n/a	n/a		n/a	n/a
Gibraltar	n/a	n/a		n/a	n/a
Greece	n/a	n/a		n/a	n/a
Greenland	n/a	n/a		n/a	n/a

COUNTRY	MLAT AGREEMENT	MOUs/ JOINT STATEMENTS WITH INDIA	DATES	COMMENTS	CYBER FRAMEWORKS WITH INDIA
Grenada	n/a	n/a		n/a	n/a
Guadeloupe	n/a	n/a		n/a	n/a
Guam	n/a	n/a		n/a	n/a
Guatemala	n/a	n/a		n/a	n/a
Guernsey	n/a	n/a		n/a	n/a
Guinea-Bissau	n/a	n/a		n/a	n/a
Guyana	n/a	n/a		n/a	n/a
Haiti	n/a	n/a		n/a	n/a
Honduras	n/a	n/a		n/a	n/a
Hong Kong	http://cbi.nic.in/interpol/mlat/Hongkong.pdf	n/a		n/a	n/a
Hungary	n/a	n/a		n/a	n/a
Iceland	n/a	n/a		n/a	n/a
Indonesia	http://cbi.nic.in/interpol/mlat/Indonesia.pdf	http://mea.gov.in/bilateral-documents.htm?dtl/27805/IndiaIndonesia_Joint_Statement_during_the_State_visit_of_President_of_Indonesia_to_India	Dec 2016	They commended the Joint Working Group on Counter-Terrorism, which has met regularly and took note of the outcome of the last meeting held in October 2015 which discussed issues of mutual interest, including cyber security.	n/a
		http://indianexpress.com/article/india/indianhome-ministry-indonesian-ministry-of-security-and-coordination/	Mar 2017	Decided to enhance cooperation in cyber security and intelligence sharing.	
Iran	http://cbi.nic.in/interpol/mlat/Iran.pdf			Cyber crime as an area of cooperation alongside narcotic trade and money laundring	n/a
Iraq	n/a	n/a		n/a	n/a
Ireland	n/a	n/a		n/a	n/a
Isle of Man	n/a	n/a		n/a	n/a

COUNTRY	MLAT AGREEMENT	MOUs/ JOINT STATEMENTS WITH INDIA	DATES	COMMENTS	CYBER FRAMEWORKS WITH INDIA
Israel	http://cbi.nic.in/interpol/mlat/Israel.pdf	https://www.infosys.com/newsroom/press-releases/Pages/mou-drive-industrial-research-development.aspx	Jun 2012	Non-governmental- infosys is an indian corporation. But the Israeli state is involved. The MoU creates a framework for industrial cooperation between Infosys and Israeli corporations in the emerging technology areas of cloud, information security, sensors, analytics, and sustainability	n/a
Italy	n/a	http://www.business-standard.com/article/companies/italian-firm-e2labs-sign-mou-for-it-security-training-107041201032_1.html	Apr 2007	Non-governmental: Zone-h, an Italy-based independent observatory of server-side cybercrimes, on Wednesday entered into an MoU with Hyderabad-based internet security solutions provider e2Labs, to bring its IT security training to IT and state sectors in the Indian sub-continent.	n/a
Jamaica	n/a	n/a		n/a	n/a
Japan	n/a	http://pib.nic.in/newsite/PrintRelease.aspx?relid=135831	Jan 2016	Aims to further cooperation in the area of cyber security by exchange information on Cyber Security incidents, collaborate in syber security projects, exchange delegates etc.	http://www.soumu.go.jp/main_content/000325863.pdf
Jersey	n/a	n/a		n/a	n/a
Jordan	n/a	n/a		n/a	n/a

COUNTRY	MLAT AGREEMENT	MOUs/ JOINT STATEMENTS WITH INDIA	DATES	COMMENTS	CYBER FRAMEWORKS WITH INDIA
Kazakhstan	http://cbi.nic.in/interpol/mlat/Kazakhstan.pdf	http://mea.gov.in/bilateral-documents.htm?dtl/4845/Bilateral+agreements+concluded+during+PMs+visit+to+Kazakhstan	Apr 2011	MoU no. 4 in the table: envisages cooperation on Information Security and mutual response to cyber security incidents, exchange of information on spam and other cyber-attacks, exchange of information on prevalent cyber security policies and exchange of human resources	n/a
Kenya	n/a	http://www.mea.gov.in/bilateral-documents.htm?dtl/27011/Joint+Communique+between+India+and+Kenya+during+the+visit+of+Prime+Minister+to+Kenya+July+11+2016	Jul 2016	Section 4: The Kenyan side noted India's offer of an LoC for acquisition of defence equipment. Both sides agreed to continue cooperating in this sector and to share information and expertise in counter terrorism, cyber security, combating drugs and human trafficking.	n/a
		https://telanganatoday.news/india-kenya-focus-defence-security-cooperation-pm	Jan 2017	The partnership will focus on cyber security, counter-terrorism, combating drugs, narcotics, human trafficking and money laundering	
Kiribati	n/a	n/a		n/a	n/a
Korea, North	n/a	n/a		n/a	n/a
Korea, South	http://cbi.nic.in/interpol/mlat/SouthKorea.pdf	http://capsindia.org/files/documents/CAPS_Infocus_DR_3.pdf	Jan 2014	To promote closer cooperation and exchange of information pertaining to Cyber Security.	n/a
Kuwait	http://cbi.nic.in/interpol/mlat/Kuwait.pdf	n/a		n/a	n/a
Kyrgyzstan	http://cbi.nic.in/interpol/mlat/Kyrgez.pdf	n/a		n/a	n/a
Laos	n/a	n/a		n/a	n/a
Latvia	n/a	n/a		n/a	n/a
Lebanon	n/a	n/a		n/a	n/a
Lesotho	n/a	n/a		n/a	n/a

COUNTRY	MLAT AGREEMENT	MOUs/ JOINT STATEMENTS WITH INDIA	DATES	COMMENTS	CYBER FRAMEWORKS WITH INDIA
Liberia	n/a	n/a		n/a	n/a
Libya	n/a	n/a		Found MoU that covers exchange of information but nothing about cyber spaces or security.	n/a
Liechtenstein	n/a	n/a		n/a	n/a
Lithuania	n/a	n/a		n/a	n/a
Luxembourg	n/a	n/a		n/a	n/a
Macau	n/a	n/a		n/a	n/a
Macedonia	n/a	n/a		n/a	n/a
Madagascar	n/a	n/a		n/a	n/a
Malawi	n/a	n/a		n/a	n/a
Malaysia	http://cbi.nic.in/interpol/mlat/Malaysia.pdf	http://economictimes.indiatimes.com/news/economy/foreign-trade/india-and-malaysia-sign-3-mous-including-cyber-security/articleshow/49891897.cms	Nov 2015	CERT-In and Cyber Security Malaysia agreed: to promote close cooperation and the exchange of information pertaining to cyber security incident management, technology cooperation and cyber attacks, prevalent policies and best practices and mutual response to cyber security incidents.	https://www.digitalnewsasia.com/malaysia-and-india-cybersecurity-pact
		http://pib.nic.in/newsite/PrintRelease.aspx?relid=135831	Jan 2016	To promote closer co-operation and the exchange of information pertaining to the Cyber Security in accordance with the relevant laws and regulations of each country and this Memorandum of Understanding (MoU) and on the basis of equality, reciprocity and mutual benefit.	
Maldives	n/a	n/a		n/a	n/a
Mali	n/a	n/a		n/a	n/a
Malta	n/a	n/a		n/a	n/a
Marshall Islands	n/a	n/a		n/a	n/a

COUNTRY	MLAT AGREEMENT	MOUs/ JOINT STATEMENTS WITH INDIA	DATES	COMMENTS	CYBER FRAMEWORKS WITH INDIA
Martinique	n/a	n/a		n/a	n/a
Mauritania	n/a	n/a		n/a	n/a
Mauritius	http://cbi.nic.in/interpol/mlat/Maritius.pdf	http://gis.govmu.org/English/Publication/Documents/2015/News%20March%202015%20Web%202.pdf	Mar 2015	Mutual agreement to strengthen cooperation on cyber security as an area of common interest (during the "tête-à-tête")	n/a
		http://indiatoday.intoday.in/story/bse-mauritius-stock-exchange-tie-up-to-promote-financial-mkts/1/723635.html	Jul 2016	New Delhi, Jul 25 (PTI) Leading bourse BSE today said it has entered into an agreement with Stock Exchange of Mauritius (SEM) for collaboration in areas including investments, products and cyber security.	
Mayotte	n/a	n/a		n/a	n/a
Meixco	http://cbi.nic.in/interpol/mlat/Mexico.pdf	n/a		n/a	n/a
Micronesia, Fed. St.	n/a	n/a		n/a	n/a
Moldova	n/a	n/a		n/a	n/a
Monaco	n/a	n/a		n/a	n/a
Mongoila	http://cbi.nic.in/interpol/mlat/Mangolia.pdf	http://mea.gov.in/bilateral-documents.htm?dtl/25252/List+of+AgreementsMoUs+exchanged+during+the+visit+of+Prime+Minister+to+Mongolia+May+17+2015	May 2015	MoU no. 5 in the table: India to establish a Cyber Security Training Centre for the Mongolia's Ministry of Defence and will also undertake the training of personnel in cyber security.	http://www.business-standard.com/article/news-ani/agreements-signed-will-deepen-security-cooperation-between-india-mongolia-pm-modi-115051700076_1.html
Montserrat	n/a	n/a		n/a	n/a
Morocco	n/a	n/a		n/a	n/a
Mozambique	n/a	n/a		n/a	n/a

COUNTRY	MLAT AGREEMENT	MOUs/ JOINT STATEMENTS WITH INDIA	DATES	COMMENTS	CYBER FRAMEWORKS WITH INDIA
Myanmar	http://cbi.nic.in/interpol/mlat/Myanmar.pdf	http://www.mea.gov.in/incoming-visit-detail.htm?27513/IndiaMyanmar+Joint+Statement+during+the+visit+of+State+Counsellor+of+Myanmar+to+India	Oct 2016	No separate MoU on CS. Section 19 of the Joint Statement: India agreed to support Myanmar in creating police training infrastructure and to share expertise in developing training manuals, including in forensics and cyber-security.	n/a
Namibia	n/a	n/a		n/a	n/a
Nauru	n/a	n/a		n/a	n/a
Nepal	n/a	n/a		n/a	n/a
Netherlands	n/a	n/a		n/a	n/a
Netherlands Antilles	n/a	n/a		n/a	n/a
New Caledonia	n/a	n/a		n/a	n/a
New Zealand	n/a	https://www.mea.gov.in/incoming-visit-detail.htm?27535/India++New+Zealand+Joint+Statement+during+visit+of+Prime+Minister+of+New+Zealand+to+India	Oct 2016	Cooperation on "cyber issues" is mentioned under s. 4 - no specification of cyber security	n/a
Nicaragua	n/a	n/a		n/a	n/a
Niger	n/a	n/a		n/a	n/a
Nigeria	n/a	n/a		n/a	n/a
N. Mariana Islands	n/a	n/a		n/a	n/a
Norway	n/a	n/a		n/a	n/a
Oman	http://cbi.nic.in/interpol/mlat/Oman.pdf	n/a		n/a	n/a
Pakistan	n/a	n/a		n/a	n/a
Palau	n/a	n/a		n/a	n/a
Panama	n/a	n/a		n/a	n/a
Papua New Guinea	n/a	n/a		n/a	n/a
Paraguay	n/a	n/a		n/a	n/a

COUNTRY	MLAT AGREEMENT	MOUs/ JOINT STATEMENTS WITH INDIA	DATES	COMMENTS	CYBER FRAMEWORKS WITH INDIA
Peru	n/a	n/a		n/a	n/a
Philippines	n/a	n/a		n/a	n/a
Poland	n/a	n/a		n/a	n/a
Portugal	n/a	http://www.tribuneindia.com/news/business/india-portugal-to-collaborate-in-ites-cyber-security/373666.html	Mar 2017	India and Portugal agreed to set up an institutional mechanism to collaborate in the areas of electronic manufacturing, ITeS, startups, cyber security and e-governance. areas of cooperation are: electronic manufacturing, ITeS, cyber security, e-governance and capacity building	n/a
Puerto Rico	n/a	n/a		n/a	n/a
Qatar	n/a	http://www.pmindia.gov.in/en/news_updates/india-qatar-joint-statement-during-the-pms-visit-to-qatar/	Jun 2016	Section 15: The two sides discussed ways and means to further promote cooperation in cyber security, including prevention of use of cyber space for terrorism, radicalization and for disturbing social harmony	n/a
		http://naradanews.com/2016/12/india-qatar-sign-agreements-on-visa-cybersecurity-investments/	Dec 2016	A protocol on technical cooperation in cyber space and combating cyber crime was signed between the Ministry of Home Affairs of India and the Ministry of Interior of Qatar.	
Romania	n/a	n/a			n/a
Russia	http://cbi.nic.in/interpol/mlat/Russia.pdf	http://www.orfonline.org/expert-speaks/india-and-russia-cyber-agreement/	Oct 2016	Said to pave the way for cooperation in tackling cyber crime and in matters of defence and national security. Establishes a high-level dialogue on cyber issues and allows governmental agencies to start working together on counter-terrorism.	http://rusembindia.com/home/actual-topics/104-actualnews/7470-india-russia-to-set-up-expert-group-on-cyber-security-counter-terrorism
Rwanda	n/a	n/a		n/a	n/a

COUNTRY	MLAT AGREEMENT	MOUs/ JOINT STATEMENTS WITH INDIA	DATES	COMMENTS	CYBER FRAMEWORKS WITH INDIA
Saint Helena	n/a	n/a		n/a	n/a
Saint Kitts & Nevis	n/a	n/a		n/a	n/a
Saint Lucia	n/a	n/a		n/a	n/a
St Pierre & Miquelon	n/a	n/a		n/a	n/a
Saint Vincent and the Grenadines	n/a	n/a		n/a	n/a
Samoa	n/a	n/a		n/a	n/a
San Marino	n/a	n/a		n/a	n/a
Sao Tome and Principe	n/a	n/a		n/a	n/a
Saudi Arabia	n/a	http://www.mea.gov.in/bilateral-documents.htm?dtl/26595/IndiaSaudi+Arabia+Joint+Statement+during+the+visit+of+Prime+Minister+to+Saudi+Arabia+April+03+2016	Apr 2016	Both leaders agreed to promote cooperation in cyber security, including prevention of use of cyber space for terrorism, radicalization and for disturbing social harmony	n/a
Senegal	n/a	n/a		n/a	n/a
Serbia	n/a	https://www.eoibelgrade.gov.in/press.php?id=164	Oct 2016	Cyber security as one of the areas of cooperation of the MOU	n/a
		http://ehub.newsforce.in/cabinet-approves-mou-india-serbia-cooperation-field-electronics/	Jan 2017	This is vaguely a cooperation in IT field, but mentions capacity building institutions which should entail cyber security	
Seychelles	n/a	n/a		n/a	n/a
Sierra Leone	n/a	n/a		n/a	n/a
Singapore		http://www.ndtv.com/india-news/india-malaysia-singapore-and-japan-sign-pacts-for-cyber-security-1270707	Oct 2015		

COUNTRY	MLAT AGREEMENT	MOUs/ JOINT STATEMENTS WITH INDIA	DATES	COMMENTS	CYBER FRAMEWORKS WITH INDIA
	http://cbi.nic.in/interpol/mlat/Singapore.pdf	http://www.businesstimes.com.sg/government-economy/singapore-and-india-strengthen-cooperation-on-cyber-security	Jan 2016	To promote closer co-operation and the exchange of information pertaining to the Cyber Security in accordance with the relevant laws and regulations of each country and this Memorandum of Understanding (MoU) and on the basis of equality, reciprocity and mutual benefit.	http://www.channelnewsasia.com/news/singapore/singapore-india-sign/2288192.html
Slovakia	n/a	n/a		n/a	n/a
Slovenia	n/a	n/a		n/a	n/a
Solomon Islands	n/a	n/a		n/a	n/a
Somalia	n/a	n/a		n/a	n/a
South Africa	http://cbi.nic.in/interpol/mlat/SouthAfrica.pdf	https://sputniknews.com/world/201609161045368613-brics-cyber-security/	Sep 2016	MULTILATERAL: BRICS. No bilateral MoU on CS between India and SA	n/a
Spain	http://cbi.nic.in/interpol/mlat/Spain.pdf	n/a		n/a	n/a
Sri Lanka	http://cbi.nic.in/interpol/mlat/SriLanka.pdf	n/a		n/a	n/a
Sudan	n/a	n/a		n/a	n/a
Suriname	n/a	n/a		n/a	n/a
Swaziland	n/a	n/a		n/a	n/a
Sweden	n/a	http://www.government.se/statements/2016/02/joint-statement-by-prime-minister-stefan-lofven-and-prime-minister-narendra-modi/	Feb 2016	Joint statement Section 22: both sides committed to promote cyber security, combat cybercrime, and develop a common understanding on international cyber issues to support an open, inclusive, transparent and multi-stakeholder system of internet governance as well as the application of international law in cyberspace.	n/a
Switzerland	http://cbi.nic.in/interpol/mlat/Switzerland.pdf	n/a		n/a	n/a

COUNTRY	MLAT AGREEMENT	MOUs/ JOINT STATEMENTS WITH INDIA	DATES	COMMENTS	CYBER FRAMEWORKS WITH INDIA
Syria	n/a	n/a		n/a	n/a
Taiwan	n/a	n/a		n/a	n/a
Tajikistan	http://cbi.nic.in/interpol/mlat/Tajikistan.pdf	n/a		n/a	n/a
Tanzania	n/a	n/a		n/a	n/a
Thailand	http://cbi.nic.in/interpol/mlat/Thailand.pdf	http://www.mea.gov.in/bilateral-documents.htm?dtl/26923/IndiaThailand+Joint+Statement+during+the+visit+of+Prime+Minister+of+Thailand+to+India	Jun 2016	Joint statement; section 18 cyber security; section 20 cybercrime.	n/a
Timor-Leste	n/a	n/a		n/a	n/a
Togo	n/a	n/a		n/a	n/a
Tonga	n/a	n/a		n/a	n/a
Trinidad & Tobago	n/a	n/a		n/a	n/a
Tunisia	n/a	http://meity.gov.in/content/africa		MoU between STPI and Elgazala Technopark, Tunisia for cooperation in the field of Communication & Information Technology named information security as one area of cooperation for the indo-tunis working group	n/a
Turkey	http://cbi.nic.in/interpol/mlat/Turkey.pdf	n/a		n/a	n/a
Turkmenistan	n/a	n/a		Found MoU about defence and security but no mention of cyber or information security.	n/a
Turks & Caicos Is.	n/a	n/a		n/a	n/a
Tuvalu	n/a	n/a		n/a	n/a
Uganda	n/a	n/a		n/a	n/a
Ukrain	http://cbi.nic.in/interpol/mlat/Ukrain.pdf	n/a		n/a	n/a

COUNTRY	MLAT AGREEMENT	MOUs/ JOINT STATEMENTS WITH INDIA	DATES	COMMENTS	CYBER FRAMEWORKS WITH INDIA
United Arab Emirates	http://cbi.nic.in/interpol/mlat/UnitedArabEmirates.pdf	http://www.business-standard.com/article/government-press-release/memorandum-of-understanding-signed-between-india-and-united-arab-emirates-on-116031000703_1.html	March 2016	Both sides would cooperate in cyber space and combating cyber-crime in all forms, particularly through coordination and exchange of information in relation with cyber crime, cooperation and training in cyber-crime investigation, etc	n/a
		http://mea.gov.in/bilateral-documents.htm?dtl/27969/India++UAE+Joint+Statement+during+State+visit+of+Crown+Prince+of+Abu+Dhabi+to+India+January+2426+2017	Jan 2017	On the topic of combatting terrorism, two leaders expressed happiness on the signing of an MOU on technical development and cooperation in cyber space during the visit	
United Kingdom		http://www.bestcurrentaffairs.com/india-uk-mou-cyber-security/	May 2016	Both countries agreed on exchanging information on prevalent cyber security, policies, and best practices. The MoU helps strengthen cyberspace of both countries, capacity building and improving relationship	
	http://cbi.nic.in/interpol/mlat/UnitedKingdom.pdf	http://www.mea.gov.in/bilateral-documents.htm?dtl/27584/indiauk+joint+statement+during+the+visit+of+prime+minister+of+the+united+kingdom+to+india+indiauk+strategic+partnership+looking+forward+to+a+renewed+engagement+vision+for+the+decade+ahead	Nov 2016	Cyber security as one of the areas of cooperation of the MOU	http://economictimes.indiatimes.com/news/defence/theresa-mays-india-visit-india-uk-agree-to-strengthen-defence-and-cyber-security-cooperation/articleshow/55291344.cms
Uniter States of America		https://www.dhs.gov/news/2011/07/19/united-states-and-india-sign-cybersecurity-agreement	Jul 2011	The United States and India signed a Memorandum of Understanding (MOU) today to promote closer cooperation and the timely exchange of information between the organizations of their respective governments responsible for cybersecurity.	n/a

COUNTRY	MLAT AGREEMENT	MOUs/ JOINT STATEMENTS WITH INDIA	DATES	COMMENTS	CYBER FRAMEWORKS WITH INDIA
		http://www.dqindia.com/india-cert-signs-an-mou-with-us-cert/	Jan 2017	Indian Computer Emergency Response Team (CERT- In) under the Ministry of Electronics and Information technology of the Government of India and the Department of Homeland Security, Government of the United States of America on cooperation in the field of cyber Security.	n/a
	http://cbi.nic.in/interpol/mlat/UnitedStatesofAmerica.pdf	http://indiatoday.intoday.in/story/cabinet-apprised-of-indo-us-cyber-security-pact/1/910545.html	Mar 2017	US and India signed an MoU between CERT-In and CERT-US to promote closer co-operation and exchange of information pertaining to cyber security in accordance with relevant laws, rules and regulations and on the basis of equality, reciprocity and mutual benefit.	https://in.usembassy.gov/framework-u-s-india-cyber-relationship/
Uruguay	n/a	n/a		n/a	n/a
Uzbekistan	http://cbi.nic.in/interpol/mlat/Uzbekistan.pdf	http://indianexpress.com/article/india/india-news-india/narendramodi-tashkent-uzbekistan-security-cooperation-2871990/	Jun 2016	To promote closer co-operation and the exchange of information pertaining to the Cyber Security in accordance with the relevant laws and regulations of each country and this Memorandum of Understanding (MoU) and on the basis of equality, reciprocity and mutual benefit.	n/a
Vanuatu	n/a	n/a		n/a	n/a
Venezuela	n/a	n/a		n/a	n/a
Vietnam	http://cbi.nic.in/interpol/mlat/Vietnam.pdf	http://www.mea.gov.in/bilateral-documents.htm?dtl/27362/Joint+Statement+between+India+and+Vietnam+during+the+visit+of+Prime+Minister+to+Vietnam	Sep 2016	Establish a frame/mechanism for future dialogue. Exchange of information on Cyber attacks. Exchange of information on prevalent cyber security policies. Human resource development and capacity building	n/a

COUNTRY	MLAT AGREEMENT	MOUs/ JOINT STATEMENTS WITH INDIA	DATES	COMMENTS	CYBER FRAMEWORKS WITH INDIA
		http://pib.nic.in/newsite/PrintRelease.aspx?relid=157458	Jan 2017	The MoU intends to promote closer cooperation for exchange of knowledge and experience in detection, resolution and prevention of cyber security-related incidents between India and Vietnam.	
Virgin Islands	n/a	n/a		n/a	n/a
Wallis and Futuna	n/a	n/a		n/a	n/a
West Bank	n/a	n/a		n/a	n/a
Western Sahara	n/a	n/a		n/a	n/a
Yemen	n/a	n/a		n/a	n/a
Zambia	n/a	n/a		n/a	n/a
Zimbabwe	n/a	n/a		n/a	n/a