

# Centre Of Excellence For Cyber Security Research And Development In India (CECSRDI)

Exclusive Techno Legal Cyber Security Research And Development Centre Of India (TLCSRDCI)

## National Cyber Security Policy Of India 2013 (NCSP 2013)



The [National Cyber Security Policy of India 2013 \(NCSP 2013\)](#) (PDF) was [recently declared](#) by Indian Government. It is a Good Policy on many counts but it also failed to address many crucial aspects as well. For instance, the National Cyber Security Policy of India has [failed to protect](#) Privacy Rights in India. Nevertheless, this is a good step in the right direction and it must be updated and improved as the time passes

A sound Cyber Security Policy must be Techno Legal and Holistic in nature. It must be Techno Legal in nature so that it can accommodate both Technological and Legal aspects. It must be Holistic as it should cover as much areas as possible. It must be realistic as well as a single Policy cannot be considered to be Panacea for all Cyber Crimes and Cyber Attacks against India.

Thus, the Indian Cyber Security Policy must be supplemented by other Techno Legal Policies. For instance, the [E-Mail Policy of India](#) must supplement the Cyber Security Policy. The Cyber Security Policy must also be supplemented with the [Telecom Security Policy of India](#) and [National Telecom Policy of India 2012 \(NTP 2012\)](#). In fact, the [National Security Policy of India](#) must have the Cyber Security Policy as an essential component.

This NCSP 2013 intends to protect information and information infrastructure in Cyberspace, build capabilities to prevent and respond to cyber threat, reduce vulnerabilities and minimise damage from cyber incidents through a combination of institutional structures, people, processes, technology and cooperation.

The NCSP 2013 aims at facilitating creation of Secure Computing Environment and enabling adequate trust and confidence in electronic transactions and also guiding stakeholders' actions for protection of Cyberspace. It outlines a road-map to create a framework for comprehensive, collaborative and collective

response to deal with the issue of Cyber Security at all levels within the country. It also recognises the need for objectives and strategies that need to be adopted both at the National level as well as International level.

The NCSP 2013 envisages a vision and mission statement aimed at building a secure and resilience Cyberspace for citizens, businesses and Government. It strives to enable goals aimed at reducing national vulnerability to cyber attacks, preventing cyber attacks and cyber crimes, minimising response and recover time and effective cyber crime investigation and prosecution. It intends to facilitate monitoring key trends at the national level such as trends in cyber security compliance, cyber attacks, cyber crime and cyber infrastructure growth.

The Objectives of the NCSP 2013 include to create a secure cyber ecosystem in the country, generate adequate trust and confidence in IT system 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 promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment (Product, process, technology and people), to strengthen the Regulatory Framework for ensuring a Secure Cyberspace Ecosystem, to enhance and create National and Sectoral level 24X7 mechanism 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 improve visibility of integrity of ICT products and services by establishing infrastructure for testing & validation of security of such product, to create workforce for 5,00,000 professionals skilled in next 5 years through capacity building skill development and training, to provide fiscal benefit 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 citizen's data and reducing economic losses due to cyber crime or data theft, to enable effective prevention, investigation and prosecution of cyber crime and enhancement of law enforcement capabilities through appropriate Legislative Intervention.

Although the Objectives and Aims of the NCSP 2013 are Laudable yet their "Actual Implementation" is the real problem. India has not been able to achieve these Cyber Security Objectives so far. Since India is a late entrant in the Cyber Security field, it would only be fair to give it some more time to implement these Objectives successfully.

This entry was posted in Uncategorized on December 26, 2013 [<http://perry4law.org/cecsrди/?p=1068>] by Praveen Dalal.

---

One thought on "National Cyber Security Policy Of India 2013 (NCSP 2013)"

Pingback: [Huawei Accused Of Breaching National Security Of India By Hacking Base Station Controller In AP | Centre Of Excellence For Cyber Security Research And Development In India \(CECSRDI\)](#)

Comments are closed.