PRS LEGISLATIVE RESEARCH

Standing Committee Report Summary

Cyber Crime, Cyber Security and Right to Privacy

- The Standing Committee on Information Technology (Chairperson: Mr. Rao Inderjit Singh) presented its report on Cyber Crime, Cyber Security and Right to Privacy on February 12, 2014.
- Key recommendations of the Committee pertained to:
- **Establishment of protection centre:** The Committee noted the existence of 20 types of cyber crimes, worldwide. With India amongst the top five countries with respect to cyber crimes, a growing need to protect its 11 critical sectors (power, atomic energy, space, aviation, transportation, etc.), is arising. The Committee recommended establishing a National Critical Information Infrastructure Protection Centre to field cyber attacks.
- **Institutions to deal with cyber crime:** The Committee recommended the installation of a single, centralised body to deal with cyber crime. The current setup involves overlapping responsibilities of many departments, agencies and banks. Cyber crime cells should be constituted in each state, district and block, connected to a centralised system.
- **International Standards Organisation certification:** The Committee identified that government organisations should obtain the appropriate certification for best practices related to information security.
- **Shortage of manpower:** Pointing out the inadequacy of existing initiatives, it suggested conducting extensive training programmes to overcome shortage of security experts and auditors, and skilled Information Technology (IT) personnel in the country.
- **Funding for research and development:** The Committee highlighted the need for innovative research and development to enhance security of cyber space. It expressed concern over budgetary cuts in the sector as large funds are needed for the development of key, strategic technologies.
- **External hosting and new technology:** The Committee recommended that despite the cost advantages of hosting websites outside India, internet servers for critical sectors should be hosted within the country to ensure security. Upcoming technologies like cloud computing under the National e-Governance Programme (NeGP) could be risky. The Committee, acknowledging the possibility of cyber security breaches in NeGP, recommended conducting surveys to collect data on the matter and reducing such instances.
- **Information Technology Act, 2000 and National Cyber Security Policy, 2013:** The Committee opined that although the IT Act, 2000 may appear adequate, there is a need for periodic review of its provisions. It also recommended that a more detailed plan of action (deadlines and targets) be constructed with respect to the National Cyber Security Policy, 2013.
- **Miscellaneous legal recommendations:** The Committee's other recommendations relating to the legal aspect of the subject included, (i) signing of MoU's and international treaties to address cross border challenges in cyber security (ii) instituting a legal framework on privacy, which is secure and people friendly, and (iii) setting up of a grievance redressal mechanism by means of Cyber Appellate Tribunal and help line for common public to deal with cyber crime.

DISCLAIMER: This document is being furnished to you for your information. You may choose to reproduce or redistribute this report for non-commercial purposes in part or in full to any other person with due acknowledgement of PRS Legislative Research ("PRS"). The opinions expressed herein are entirely those of the author(s). PRS makes every effort to use reliable and comprehensive information, but PRS does not represent that the contents of the report are accurate or complete. PRS is an independent, not-for-profit group. This document has been prepared without regard to the objectives or opinions of those who may receive it.

Apoorva Shankar
apoorva@prsindia.org

February 26, 2014