OSPAI
Other Service Providers Association Of India
Fueling ITeS Growth Engine

Annexure-I

OSPAI's response on TRAI CP on Cloud Computing

We welcome the opportunity to submit our comments on the Consultation paper on Cloud Computing issued by Telecom Regulatory Authority of India (TRAI). Cloud Computing is increasingly being adopted by business, including SME's and large enterprises, to benefit from the adoption of technology which is scalable, cost efficient and enhances the end user experience.

Cloud Computing was recognized as an important emerging technologies and services format under National Telecom Policy 2012 (NPT 2012). The Government's prestigious Digital India Program can be realized with widespread adoption of cloud computing. It should be noted that emerging IoT/M2M services also too depend on cloud computing, particularly to store and manage data collected from sensors and machines in a secured manner.

Cloud computing can play an important role for achieving economic development goals in emerging markets like India by furthering public welfare, reducing access costs, and enabling more efficient services delivery. The adoption of these technologies / services will help provide the must needed push to the growth of data and broadband services principally by reducing computing costs for end users.

Impetus to Cloud Computing under National Telecom Policy-2012 (NPT – 2012)

NPT-2012 has recognized the growing importance of cloud-based applications and services in accelerating the design and roll out of the new innovative services on large scale. Importantly, the NPT 2012 has recognized the need to reduce regulatory barriers that could impede the adoption of cloud computing in India.

The policy has further noted that cloud computing will significantly speed up design and roll out of services, enable social networking and participative governance and m-Commerce at scale which were not possible through traditional technology solutions.

10. CLOUD SERVICES

10.1. To recognize that cloud computing will significantly speed up design and roll out of services, enable social networking and participative governance and e-Commerce on a scale which was not possible with traditional technology solutions.

10.2. To take new policy initiatives to ensure rapid expansion of new services and technologies at globally competitive prices by addressing the concerns of cloud users and other stakeholders including specific steps that need to be taken for lowering the cost of service delivery.

10.3.To identify areas where existing regulations may impose unnecessary burden and take consequential remedial steps in line with international best practices for propelling nation to emerge as a global leader in the development and provision of cloud services to benefit enterprises, consumers and Central and State Governments.

11.3. To adopt best practices to address the issues (like encryption, privacy, network security, law enforcement assistance, inter-operability, preservation of cross-border data flows etc.) related to cloud services, M2M and other emerging technologies to promote a global market for India.

The advent of technologies like cloud computing present a historic opportunity to catapult India's vaunted service delivery capabilities to a new level domestically as well globally.

The NPT-2012 further recommends that the government implement measures to facilitate a liberalized regulatory environment that will foster affordable, reliable and secure telecommunication and broadband services across the entire country.

Issues for Consultation:-
The following issues have been identified for the public consultation by TRAI and we would like to submit our responses in-seriatum:

Question 1. What are the paradigms of cost benefit analysis especially of:

a. **Accelerating the design and roll out of services**
b. **Promotion of social networking, participative governance and e-Commerce**
c. **Expansion of new services**
d. **Any other items or technologies. Please support your views with relevant data**

OSPAI Response:
Recent analyst report providers interesting insights on paradigms of cost benefit analysis in terms of expansion of new services. Cloud is now an integral part of enterprise IT and enterprises are looking for cloud solutions that will help make their businesses more efficient, agile, responsive and competitive.

Cloud is now firmly established as a reliable enterprise workhorse, and what's most interesting is how it is driving transformation. Organizations are using cloud to create new customer experiences, re-engineer their business processes and find new opportunities to grow. Organizations are not just using more cloud based technologies; They are using it for applications which are more demanding and more critical to everyday operations and performance. This often includes multiple mission-critical applications. Advances in technology are changing the cost-benefit equation and making it easier for companies to build more powerful environments in the cloud, enabling hem to move more workloads and transform more processes.

Question 2. Please indicate with details how the economies of scale in the cloud will help cost reduction in the IT budget of an organization?

OSPAI Response:

While business of all size benefit from the efficiencies of cloud services, the most impactful dimension of cloud services in cost reduction is actually the benefit to small businesses, where cloud services can spare these businesses from incurring the upfront cost of building an IT infrastructure and enable them to use standard application off the cloud.

Question 3. What parameters do the business enterprises focus on while selecting type of cloud service deployment model? How does a decision on such parameters differ for large business setups and SMEs?

OSPAI Response:

Several factors influence business enterprise decisions, depending on which on type of solution is preferred, capital and expense budgets and the degree of in-house technical expertise. As with any enterprise grade service, security, resilience, scale, flexibility and cost are important factors.

There are various other parameters that the business enterprises focus or while selecting type of the cloud service deployment mode. As per a recent study, Hybrid cloud deployment model is now the mainstream. The decision to move to hybrid is influenced by several considerations.

Advances in technology are changing the cost-benefit equation and making it easier for companies to build more powerful environments in the cloud, enabling them to move more workloads and transform more processes.

It’s been suggested that hybrid cloud which is the use of a mix of models, including on-premises and public and private cloud will become mainstream within five years. We think that it already is, especially for large organizations. There are already services that enable companies to create a sophisticated environment made up of multiple clouds from multiple providers, but make it look like a seamless part of the enterprise infrastructure.

Question 4. How can a secure migration path may be prescribed so that migration and deployment from one cloud to another is facilitated without any glitches?

OSPAI Response:

Encryption is one of the critical components of digital security which is the ability to use robust encryption. Therefore the government should adopt a flexible approach to encryption that help security of data transfer, processing and storage. Telecom licensees should similarly be allowed the flexibility to use higher encryption to build security into the core of their network and services.

Question 5. What regulatory provisions may be mandated so that a customer is able to have control over his data while moving it in and out of the cloud?

OSPAI Response:
The regulatory provisions should offer complete flexibility to move the data as the ability for information to flow across borders will be increasingly important to economic growth as all businesses are dependent on the flow of digital, cloud-based information.

As recognized worldwide, the ICT services have important multiplier effects across other economic sectors and thus play an important role in simulating broader economic activity. As digital services and global access to the Internet expand, there are enormous opportunities for economic growth. Thus the regulatory provisions should not require ICT service suppliers to use local infrastructure, or establish a local presence, as a condition of supplying services. In addition, governments should not give priority or preferential treatment to national suppliers of ICT services in the use of local infrastructure, national spectrum, or orbital resources. The same should be based on user preference and choice depending the individual parameters and technical competence.

Given the rapid pace of innovation in digital technology and services, governments are urged to maintain a light touch regulatory approach to avoid stifling growth in the digital economy. It is important that governments find a balance that enables adequate protection for data without burdening industry with unworkable data privacy and protection obligations.

Question 6. What regulatory framework and standards should be put in place for ensuring interoperability of cloud services at various levels of implementation viz., abstraction, programming and orchestration layer?

OSPAI Response:
Cloud services as a new sourcing and delivery model is being adopted on a global scale and is becoming a business transformation technology. The regulatory framework and standards should promote open standards based cloud infrastructure that will help increase software and data interoperability. Governments should take a light touch approach that enables industry to invest and develop new and innovative cloud technologies. Technical standards should be the domain of industry and locally prescribed standards should be avoided to enable global interoperability.

Question 7. What shall be the QoS parameters based on which the performance of different cloud service providers could be measured for different service models? The parameters essential and desirable and their respective benchmarks my be suggested.

OSPAI Response:
Cloud service providers typically provide their services to other businesses rather than end users directly. As such, QoS is a matter of contractual negotiation between the two parties. Any disputes arising over QoS would be settled according to the arbitration arrangements stipulated under the contract. Given the globally competitive marketplace for cloud services, government regulation of cloud computing is not necessary.

TRAI should avoid any mandated service quality levels for cloud services. These services are different services from traditional Telephone Services, relying on fundamentally different technology and featuring myriad different service attributes and configurations, with different capabilities and limitations and raising different policy considerations.

Question 8. What provisions are required in order to facilitate billing and metering re-verification by the client of Cloud Services? In case of any dispute, how is it proposed to be addressed / resolved?

OSPAI Response:
As noted in the answer to Question 7, Cloud Computing services are generally provided to business and are the result of negotiated contracts. Any questions regarding billing would be addressed under the contract itself. Disputes would be resolved in accordance to the terms of the contract. Given the globally competitive nature of cloud computing, its regulation in this matter is not deemed necessary.

Question 9. What mechanism should be in place for handling customer complaints and grievances in Cloud Services? Please comment with justification.

OSPAI Response:
As addressed above, most cloud computing services are offered to enterprises, but in the instances where cloud services are offered on a retail basis to individual customers, existing consumer protection laws as applicable to ICT sector are sufficient to deal with any complaints or grievances over related to a cloud service.

Additionally in majority of cases these are issues between service providers and enterprise and multinational companies, which are contractual issues that do not require intervention from regulators.

Question 10. Enumerate with detail with justification, the provisions that need to be put in place to ensure that the cloud services being offered are secure.

OSPAI Response:
Need for flexible approach to encryption that allows for use of strong and robust encryption. Flexible approach to encryption that enables the use of strong encryption technologies needed to ensure cloud services are secure. The government should aim at introducing an encryption policy which enables maximum flexibility and empowers the growth of cloud services. We urge the Government to adopt a flexible encryption policy so that cloud service providers can offer services using robust encryption in India.

Question 11. What are the termination or exit provisions that need to be defined for ensuring security of data or information over cloud?

OSPAI Response:

The existing provisions under the Information Technology Act 2000 related to data privacy are sufficient to deal with the security of data or information over cloud.

Question 12. What Security provisions are needed for live migration to cloud and for migration from one cloud service provider to another?

OSPAI Response:
Given the every changing cyber security landscape, contractual arrangements between cloud service providers and enterprises are best suited to provide the flexibility to adopt new security practices in any migration of data between or to a cloud-based service.

Question 13. What should be the roles and responsibilities in terms of security of (a) Cloud Service Provider (CSP); and (b) End Users?

OSPAI Response:
As stated previously, most cloud service providers provide services to an enterprise, not necessarily to an end user directly. As such, contractual arrangements are sufficient to address issues of security. In the instances where a cloud service provider may provide services on a retail basis to individual consumers, the terms of services shall delineate the roles and responsibilities with respect to security. Given the globally competitive nature of cloud based services, in both instances there should be significant competitive market pressures on cloud service providers to ensure robust security.

Question 14. The law of the user's country may restrict cross-border transfer/disclosure of certain information. How can the client be protected in case the Cloud service provider moves data from one jurisdiction to another and a violation take place? What disclosure guidelines need to be prescribed to avoid such incidents?

OSPAI Response:
Seamless flows on information across borders are essential to growth throughout the global economy, since services, manufacturing, and even agriculture increasingly rely on digital communication and other data transfers. The cloud frameworks should avoid and eliminate barriers to these data flows. Further the regulatory framework for cloud and other emerging technologies should be such that it enables the service suppliers of other countries, or customers of those suppliers, from electronically transferring information internally or across borders, accessing publicly available information, or accessing their own information stored in the cloud.

The success of the cloud computing industry depends on the global interoperability of services and the free movement of data across borders, as well as robust protections for the privacy and security of customers' data. Consumers rightly expect that the information they entrust to cloud service providers will be highly secure and that CSPs will be respectful of their privacy. Consumers should have consistent and precictable privacy protections for the information they deem private and sensitive, no matter how or with whom they share it. Establishing this trusted environment for consumers is crucial to the success of the market, separate and apart from the policy frameworks for privacy and security issues.

Government can build trust in the cloud computing industry by ensuring that cloud service providers follow industry best practices and guidelines regarding the use and protection of personal data. The consultation paper cites the frameworks developed by the Asia Pacific Economic Cooperation (APEC), the Organisation for Economic Co-operation and Development (OECD), and the International Conference on Data Protection and Privacy Commissioners (the Madrid Resolution of 2009), which serve as widely accepted international standards for multinational companies that collect, use, and transfer data, as well as for states when facilitating the transfer of data across borders. Rather than erecting barriers to cross-border data flows, the TRAI should ensure that cloud providers in India adhere to principles such as these and provide strong accountability mechanisms for customers and others who wish to challenge data management practices. It will be a paradox like situation, support for open internet while put restriction on cross border data flow or insisting for data localization.

The growth of the internet has also entitled the growing ability of people, businesses, and governments to collect, share, and use data across borders. The development of new technologies, products, and services in recent decades would never have been possible without the ability to freely move data across borders. Combining globalization with new technology and with new business models has dramatically accelerated the pace of change and innovation.

Cross-border data flows have also been a driving force behind the emergence of so-called global value chains in which businesses' operations are fragmented across borders in order to increase efficiency, lower costs, and speed up production.   The flow of data is as important as the movement of goods. Data needs to move to create value. Data sitting alone on a server is like a static / storage library where it's information flow is restricted and against value addition to foster innovation. It may be safe and secure, but largely stagnant and underutilized.

Some may have a belief that Data localization increases security but on the contrary, Data security depends on a plethora of controls, not on the physical location of a server. Businesses often back up data outside the country in which it is collected to help ensure it remains secure in the event of a natural disaster, power outage or other such emergency that could take data center offline. Businesses and consumers benefit when those who maintain data are able to use the best available security measures, regardless of the physical location of the data they seek to protect. Geographic neutrality with regard to data across borders will somehow protect user privacy and improve security, but these well-meaning efforts are ultimately counterproductive. The movement of data is no less important to the global economy than the movement of money. Cross-border data flows, just like cross-border financial flows, allow companies to integrate their personnel, manage their global supply chains and customer networks, and maintain the competitiveness they need to grow and thrive. The free movement of data is fully compatible with legitimate security concerns.

There are people who advocate for Data localization because it will promote domestic industry. On the contrary, data localization requirements reduce competitiveness by walling off domestic businesses from the billons of potential customers outside of the home country's borders. This isolation reduces in vestment and access to capital – the ability to access a potential borrower's creditworthiness or to spot potentially fraudulent activity often depends on the ability to move data across borders.

TRAI consultation paper also indicates the fact that the growth of cloud services in EU is not in line with other countries by having strict regulation in EU in cross border data flow.

Question 15. What policies, systems and processes are required to be defined for information governance framework in cloud, from lawful interception point of view and particularly it is it hosted in a different country?

OSPAI Response:

The institutional framework to access data in other countries should be based on mutuality and reciprocity. The scope of bilateral and multi-lateral agreements may be enhanced for sharing information based on principles of transparency and accountability. Finding a balance is important if the full benefits of international trade in goods, services and e-commerce are to be realized by reducing unnecessary costs of doing business. Transparent and efficient mechanisms based on the rule of law are critical of building trust between countries in this area.

Government should ensure that clear and transparent legal framework address the means by which law enforcement authorities obtain access to data stored by companies. Governments can also foster a successful cloud computing industry by committing to use existing Mutual Legal Assistance Treaties (MLATs) and processes when they seek access to data that is stored beyond their borders.

Question 16. What shall be the scope of cloud computing services in law? What is your view on providing license or registration to cloud service providers so as to subject them to the obligations there under? Please comment with justification.

OSPAI Response:

In our view for continued adoption of cloud computing services these should be left outside the purview of license or registration. International experience has demonstrated that light touch regulatory framework has fostered the growth of new technology and services.

Specific to the Indian scenario the adoption of cloud computing is still at a nascent stage and catching up with the new set of opportunities and challenges as jurisdiction over data in the cloud has been a cause of concern for regulators globally. However the concerns can be addressed through mutuality and reciprocity rather than prescriptive requirements.

Some of the noteworthy forward-looking government initiatives such as Digital India, MeghRaj, and Smart Cities are a step in the right direction to increase cloud awareness and adoption and any efforts to bring the cloud services under the ambit of a license or registration could be counterproductive and would not be conducive to the growth of the sector.

Question 17. What should be the protocol for cloud service providers to submit to the territorial jurisdiction of India for the purpose of lawful access of information? What should be the effective guidelines for and actions against those CSPs that are identified to be in possession of information related to the commission of a breach of National security of India?

OSPAI Response:

In our view to encourage cloud services, Government of India should look at, Light touch regulations that create and enabling regulatory environment for proliferation of cloud services as per the objectives set out in the National Telecom Policy 2012

The institutional framework to access data in other countries should be based on mutuality and reciprocity. The scope bilateral and multilateral agreements may be enhanced for sharing information based on principles of transparency and accountability.

Government authorities should ensure that clear and transparent legal frameworks address the means by which law enforcement authorities obtain access to data stored by companies. They should also commit to using existing MLAT processes in order to obtain data that is stored beyond their borders.

Question 18. What are the steps that can be taken by the government for:

(a) promoting cloud computing in e-governance projects;
(b) promoting establishment of data centers in India;
(c) encouraging business and private organizations utilize cloud services
(d) to boost Digital India and Smart Cities incentive using cloud.

OSPAI Response:

Some of the noteworthy government visionary initiatives Digital India, MeghRaj, and Smart Cities Mission are a step in the right direction to increase cloud awareness and adoption

In our view, the Government of India should follow International best practices for cloud adoption and applications by government in this regard. There are already Public Private Partnership (PPP) models that demonstrate the value of collaboration with the industry.

We recommend that the Government of India establishes a public private partnership process that helps establish Indian Government security performance expectations in the context of globally recognized information security standards such as ISO 27000, and enables cloud vendors to receive certification by reputable 3rd party auditors (regardless of their nationality)

Question 19. Should there be a dedicated cloud for government applications? To what extent should it support a multi-tenant environment and what should be the rules regulating such an environment?

OSPAI Response:

Generally the answer would b depend on the scope of users (government or public) and the sensitivity of the functions.

Question 20. What infrastructure challenges does India face towards development and deployment of state data centers in India? What should be the protocol for information sharing between states and between state and central?

OSPAI Response:

The availability of robust underlying network infrastructure which is scalable to the cloud requirement is very critical. In addition, the government of India needs to continue to focus on creating an investment climate that addresses key infrastructure improvements in power, land ownership, taxes etc.

Question 21. What tax subsidies should be proposed to incentivise the promotion of Cloud Services in India? Give your comments with justification. What are the other incentives that can be given to private sector for the creation of data centers and cloud services platforms in India?

OSPAI Response:

Government should encourage development of cloud infrastructure by providing tax incentives as well as take a light touch approach to regulation in the ICT sector to enable adoption of cloud across the Indian economy.

It is important that TRAI also develops a light touch regulatory framework for cloud services that can help ensure the on-going robust network deployment necessary to support this technology into the future. TRAI must minimize regulatory burdens, and provide policy certainly that will create the climate to maximize essential infrastructure investment. The key attributes of that framework should include:

- Support for the collaborative, self-regulatory initiatives among industry stakeholders in areas where regulatory action may be justified, use of light touch, flexible, well co-ordinated regime that protects innovation and facilitates rapid cloud market developments.
- Clear and transparent rules governing law enforcement access to data.

****