USINDIA BusinessCouncil

August 8, 2016

Shri R.S. Sharma, Chairman
Telecom Regulatory Authority of India (TRAI)
Mahanagar Doorsanchar Bhawan
Jawaharlal Nehru Marg
New Delhi 110 002

Subject: ***Comments on TRAI's Consultation Paper on Cloud Computing***

Dear Chairman Sharma,

Thank you for providing industry an opportunity to comment on TRAI's consultation paper on cloud computing ("the TRAI paper"), which was released on June 10, 2016.

With the growth in telecommunications and IT services, India stands uniquely poised to capitalize on new technologies and business models. Given India's enormous success with the IT services industry, it already has important experience with the benefits of distributed computing. With the right approach, India could fulfill the Prime Minister's vision to become a global hub for cloud and cloud-enabled services. The adoption of new technologies will also lead to growth in India's $150 billion IT services industry and will help achieve the Prime Minister's vision of a "*Digital India*" and his desire to take the IT-BPM industry to the hinterlands of the country.

USIBC urges the Government of India to take a light-touch and flexible approach to new and emerging data-driven services such as cloud computing in order to ensure that India can become a market leader in this sector.

Please find our answers to TRAI's questions below. We look forward to meeting with you to discuss this paper and the cloud-related opportunities for India.

Sincerely,

Dr. Mukesh Aghi
President
U.S.-India Business Council

Question 1. ***What are the paradigms of cost benefit analysis especially in terms 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.

The benefits of the Cloud are many while the costs—typically associated with security risks—can be managed. Start up and e-commerce companies leverage the Cloud to quickly develop and deploy the applications that allow them to scale up rapidly and cost-effectively in ways that simply would not be possible without the Cloud. This has real-life benefits for entrepreneurs in the ICT space.

However, to realize these benefits, India should focus on creating a competitive market for cloud computing services. This means that unnecessary regulatory burdens will be avoided, innovation will be promoted, and internationally recognized standards will be followed. USIBC urges the Government of India to avoid policies that are intended to create advantages for domestic cloud providers at the expense of Indian consumers and businesses that deserve access to the cloud provider of their choice.

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

India should not focus solely on the extent to which the adoption of cloud-enabled services can reduce capital expenditure costs. Instead, it should look at how a competitive global marketplace will help Indian companies take advantage of the Cloud's numerous benefits such as flexibility, collaboration, the ability to access data anywhere, and disaster recovery, *inter alia*.

While economies of scale make cost reduction possible, the extent to which costs are lowered depends on the IT requirements of a particular business. For instance, for some workloads or applications that grow at the same rate as the business, it may be cost effective to keep those applications in on-premise Data Centres, especially if the latest infrastructure models are already being used.

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?***

Enterprises of any size have to manage risks associated with the use of information technology. One approach is to use vendors who may be more capable of managing those risks than the enterprise itself. Some cloud providers offer SMEs with limited IT experience services that help the SME more effectively manage its costs as well as security and even regulatory compliance. For larger enterprises, the key considerations often boil down to security and performance.

Enterprises, big and small, need to understand who is responsible for managing what risks, as well as where an external vendor is responsible and how capable it is of

managing risks. As some experts have noted, security is a journey rather than a destination. It requires an ongoing conversation about how risk is managed, and it requires an understanding of where the "compliance boundaries." Some risks fall on the cloud vendor while others lie with the customer.

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?***

A prescriptive approach will inhibit innovation. Cloud providers should have the flexibility to offer different approaches to migration for their customers, and the government should allow market forces and users' choices to shape the industry. Where appropriate, contractual requirements may be used by the customer to ensure the continuity of operations. That said, innovation would be negatively affected by mandated standards for cloud providers regarding the management of data, migration processes, and virtual machines.

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?***

Data protection and privacy laws and regulations are designed to protect personal data. Non-personal data owned by the user and stored in the cloud are also protected through contractual provisions between the user and the provider of the cloud service. Government mandated provisions inhibit innovation in cloud computing services and should be avoided. Instead, model contractual terms may be offered as a best practice for cloud providers to adopt.

GOI should seek to align data protection regimes with internationally accepted models so that it will ensure continued global data flows with other countries or regions such as the EU or the United States. The government should promote policies that advance the goal of transparency such that purchasers of cloud-based services can make intelligent decisions regarding the risk of lock-in. Moreover, for issues regarding data ownership or residency, we recommend that the Indian government rely on widely accepted industry-led, voluntary, consensus standards rather than developing a new regulatory framework to cover this concern.

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?***

Standard setting should be driven by industry using internationally accepted standards established by standards development organizations that seek to promote a global framework. A variety of standard setting organizations may be involved in different aspects of cloud computing. The role of government should be to encourage the development and adoption of open standards relating to cloud computing, and to foster interoperability through open and transparent processes. It is our hope that governments will avoid "picking winners" from among different standards. GOI should participate in

standards setting activities as a convener, a trusted expert, and as a major purchaser of technology and implementer of standards. GOI should rely on voluntary, consensus based standards versus technical requirements set by the government.

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 may be suggested.***

There is a wide range of user requirements and expectations for cloud computing services. Accordingly, QoS parameters should be determined by market forces and not prescribed.

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?***

There is a wide range of user requirements and expectations for cloud computing services. Accordingly, billing and metering requirements should be driven by market forces and not prescribed. Generally speaking, the IT organization that is acting as a cloud service broker should be measuring its own use of cloud and use an automated process to verify that the actual bill is correct. This should include measuring metrics that could inform any calculation of damages in the event of a contractual breach.

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

Approaches to customer complaint and grievances should not be prescribed but driven by market forces.

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

There is no question that a strong security environment will encourage user adoption and further investment in a robust cloud infrastructure. This strong security environment can be best achieved through a flexible policy framework which encourages providers to exercise all due diligence to prevent and expeditiously address threats and illegal activity and protects them from unreasonable liability when they do. Voluntary and self-regulatory efforts play a critical role in implementing such a framework and should be actively encouraged, particularly those recognized by the Government. Policymakers can encourage such efforts by acting as a convener for industry stakeholders to come together and create innovative solutions and being prepared with enforcement actions as necessary. Providers must have the flexibility to evolve preventative measures as the services provided, technologies used and threats to the ecosystem themselves evolve.

There are different approaches to deploy cloud services in a public, private, or hybrid model. The TRAI paper appears to make the assumption that data and processes on the cloud are "online" while data and processes on-premise are "offline". However, an on-premise system that is networked and connected to the Internet can be at as much risk as data or processes stored in the Cloud. In fact, security may be more effectively managed by a sophisticated and experienced cloud provider than by a consumer who works in the IT department of an SME. Keeping data and processes offline can exacerbate availability and reliability concerns.

Using cloud services does not necessarily imply the use of a public and multi-tenanted cloud. The customer's evaluation of risks determines whether data and processes should be stored in a public or private cloud. These risks are for the customer to understand, and it is not practical for a cloud provider to know what is best for individual customers. Responsibilities regarding the managing of risks between the customer and the cloud provider will vary depending on the cloud delivery model. For example, end users have less control over certain risks in a SaaS model compared to an IaaS model; in the latter, the user may be responsible for ensuring that the operating system is patched for security vulnerabilities, while in the former, the operating system is not exposed to the end user. It is not realistic for the government to effectively mandate outcomes across these various models given that they vary widely. Contractual responsibilities and compliance boundaries will vary equally.

The TRAI paper tends to over-simplify and over-generalize the considerations regarding security. For instance, the assumption made at paragraph 4.6 about data streams being visible to the cloud provider in an unencrypted form is not true in all instances. There are implementations of cloud where the storage and transmission of data are protected in a way that only the customer— and not the cloud provider or other vendor—has access to the keys. Whether the government can gain lawful access to such data will also depend on a range of circumstances on how the data is protected.

The consultation document also reflects a misunderstanding of the role of NIST, which sets the security requirements for the United States Government. However, it has **no** role in defining requirements for the private sector, except in the form of voluntary guidance, or through requirements that flow down through contractual arrangements to companies selling to the U.S. Government. Under US law[1],the United States Government must always use voluntary consensus-based standards whenever feasible instead of developing its own standards.

[1] Pub. L. 104-113, the "National Technology Transfer and Advancement Act of 1995." The policy is further explained in a circular from the White House Office of Management and Budget providing that: "All federal agencies must use voluntary consensus standards in lieu of government-unique standards in their procurement and regulatory activities, except where inconsistent with law or otherwise impractical. In these circumstances, your agency must submit a report describing the reason(s) for its use of government-unique standards in lieu of voluntary consensus standards to the Office of Management and Budget (OMB) through the National Institute of Standards and Technology (NIST)." OMB Circular A-119 Revised (Feb. 10, 1998), Source: https://www.whitehouse.gov/omb/circulars_a119.

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

The exit criteria should be defined upfront so that there are no surprises such as requirements to erase the data footprint in the provider's cloud and the cost ceiling to transfer data from the provider back into the organization.

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

Cloud services are delivered through commercial contracts between customer and providers and are governed by the legal framework, jurisdiction and arbitration clause designated in the contract. Migration provisions should be understood in that context and will vary on a contract by contract basis.

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

Offering / Responsibility		Bare Metal Cloud	Private Cloud (Virtual, Single Tenant)	Public Cloud (Virtual, Multi-Tenant)
Data Center Management		CSP	CSP	CSP
Provisioning	Server	Customer – Request CSP Automation – Perform	Customer – Request CSP Automation – Perform	Customer – Request CSP Automation – Perform
	Operating System	Customer – Request CSP Automation – Perform	Customer – Request CSP Automation – Perform	Customer – Request CSP Automation – Perform
Management	Hypervisor	N/A	CSP Automation – Monitor, Inform, Request, Perform	CSP Automation – Monitor, Inform, Request, Perform
	Hardware	CSP Automation – Monitor Customer – Monitor (optional) CSP Automation – Inform Customer – Request CSP Manual – Perform CSP Automation – Perform Customer - Perform	CSP Automation – Monitor CSP Automation - Inform CSP Automation – Request CSP Automation - Perform CSP Manual – Perform	CSP Automation – Monitor CSP Automation - Inform CSP Automation – Request CSP Automation - Perform CSP Manual – Perform
	Operating Systems	Customer	Customer	Customer
	Applications	Customer	Customer	Customer

CSP – IaaS Cloud Service provider
Monitor – collect statistics on performance and health
Inform – Provide notification of status
Request – Using API or Web Portal, create request for action/task
Perform – Complete requested task/action

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 takes place? What disclosure guidelines need to be prescribed to avoid such incidents?*

The cloud service provider should provide the user with information on their data location policies. The movement of data would be protected both by contractual provisions as well as prevailing data privacy laws. Governments should not limit the

location of data or restrict cross border data flow as such actions would limit the efficiency and efficacy of cloud services and limit user choices. As noted above, GOI should seek to align data protection regimes with internationally accepted models so that it will ensure continued global data flows with other countries or regions such as the EU or the United States.

Indeed, decisions to build data centres and where and in what manner to store data, should be based on market dynamics and client needs, rather than through government mandate. Policies that seek to force the localization of data and data centres also undermine the enormous value that data provides to Indian companies and consumers. Data is the lifeblood of the global economy and a vital source of innovation and competitive advantage for all sectors. Data is not just an issue for technology companies. Companies of all sizes in all sectors rely on communication networks to deliver services to customers, run manufacturing and internal operations, and manage global supply chains. The global economy cannot function without constant streams of data across borders.

Moreover, data analytics provide the tools to solve many of the complex problems identified by the *Digital India* initiative. Data analytics help extract insight from vast oceans of data, enabling the discovery of cures for disease, more efficient energy use, better water management, cleaner air, improved health care, smarter traffic and more efficient government.

At the individual level, access to information and communications via the Internet will help Indians enhance their education, make smarter consumer choices, improve their health and keep in touch with family and friends, wherever they are in the world.

Data also will help India create jobs, increase exports and drive growth. The Internet facilitates exports of goods and services, enables participation in global supply chains and provides access to innovative services at competitive prices, creating growth opportunities for businesses, both large and small. A wide range of services, including education, financial, business, news and health, are increasingly being delivered via the Internet, leading to growth in "digital trade".

Ensuring privacy and data security is essential, but local data requirements would create a self-imposed economic handicap without improving privacy or security. Policies must recognize that the globally integrated economy runs on the Internet. It is important not to conflate two different issues – government access to data and the commercial use of data. Restrictions on the private sector will not resolve issues regarding government access to data but will increase costs, discourage investment and job creation, block access to services, stifle innovation and make the local economy less competitive. Barriers to data flows also set a bad example for other countries, encouraging them to adopt similar restrictions, which will cut off access to export markets.

Any policies developed by the Indian government related to data, therefore, should adhere to the following broad principles:

- The movement of data across borders is an imperative for today's global economy;
- Data localization requirements disrupt the free flow of data;
- Data localization requirements are incompatible with the Internet's distributed infrastructure that enables optimal system architecture;
- The security of data does not hinge on the national boundaries of where such data resides; and
- Data localization requirements create barriers to market access, particularly impacting small and medium sized enterprises (SMEs) which are eager to attract customers not only domestically, but also in foreign markets;
- Any exceptions to these provisions, such as to protect personal data privacy, should be limited to legitimate public policy objectives and be in full compliance with the provisions of the General Agreement on Trade in Services.

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

Governments should leverage existing mutual legal assistance treaty (MLAT) arrangements and INTERPOL to address lawful intercept requirements beyond national boundaries. Any obligation to be imposed on a cloud provider to decrypt or provide access to data should apply only if the system architecture enables the decryption to take place (e.g., where the vendor or operator holds the key). It should not be required if the architecture does not allow the vendor or operator to perform such a decryption. Access requests should be backed by proper legal authorization. Encryption used by corporate enterprises intended to create a secure private network for corporate communications should not be subject to requests for access to unencrypted data.

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 thereunder? Please comment with justification.***

Cloud computing services should not be subject to a separate law, or licensing, or registration requirements. They are no different from other Internet services and should not be treated any differently.

The scope of cloud services is very broad and ranges from infrastructure to software that is provided as a service to a customer. Accordingly, we believe that cloud service providers should not be subjected to any additional license or registration for the following reasons:

- Any kind of licensing or registration goes against the basic tenets of the current government, i.e., "ease of doing business" and "liberalize" what ought not to be regulated;
- The services rendered via Cloud are dependent on infrastructure owned by private companies. For instance, for cloud services to function successfully, the Cloud Service Provider ("**CSP**") is dependent on telecom operators and internet service providers. As is the case, these industries are already regulated. For this reason,

there is no need for any additional licensing requirements that would regulate the CSP separately.

- There is an urgent need for the creation of a robust IT infrastructure, and cloud services will definitely play an integral part in this program. For micro, small, and medium enterprises, especially the start-up community, it is extremely important to have access to affordable cloud infrastructure such that the public will have access to affordable solutions. Hence, such a move to add additional licensing or registration requirements will impact the scalability of cloud services offerings in India, which will have a negative effect on government programs such as *Digital India* that rely on the same.

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?***

Existing laws sufficiently address the concerns around access to information, and there should not be a separate protocol in this regard. As noted above, the GOI should leverage existing MLAT procedures when seeking data stored in data centres stored beyond its borders.

These issues are not unique to a cloud environment but are applicable to any kind of digitized data. Separately, it is also imperative to note that CSP providers are not the owner of the data shared on a cloud environment but are only the processors. Accordingly, it may be practically impossible for the CSP provider to monitor the veracity of all the data shared on the cloud environment, especially considering the volume of data that is transmitted. It is also estimated that the volume of data would exponentially increase and any general supervision is practically unviable. More importantly, the CSP is not the owner of the data and hence the CSP would not be entitled to access the data as this could potentially raise serious concerns regarding the confidentiality and integrity of data.

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 centres in India.
(c) encouraging business and private organizations utilize cloud services.
(d) to boost Digital India and Smart Cities incentive using cloud.

There should be clear incentives that are easy to participate in—with low levels of reporting.

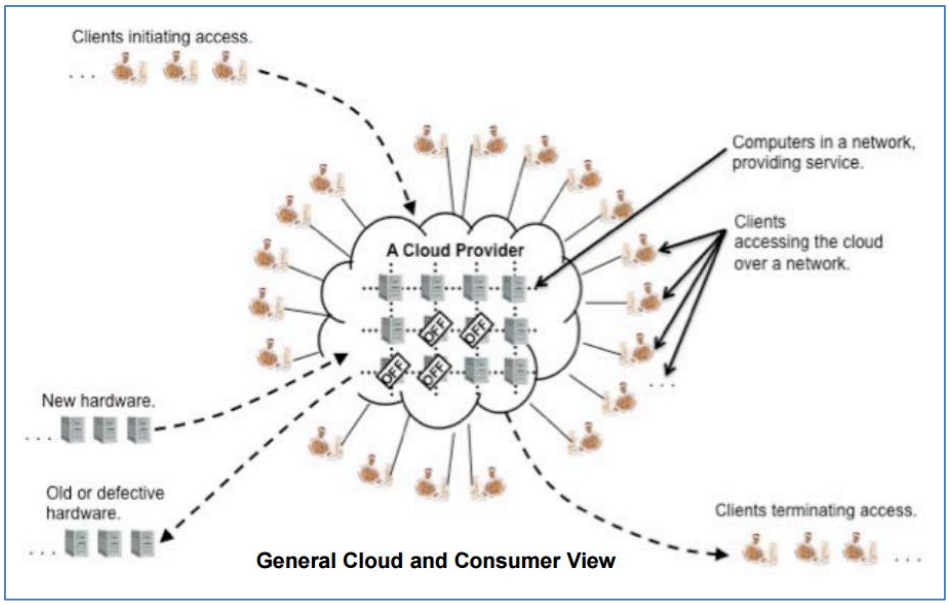
Question 19. ***Should there be a dedicated cloud for government applications? To what extent should it support a multi-tenant environment and what should be the rules regulating such an environment?***

As discussed above, customers must evaluate their own capabilities for managing cyber risks and compare them to the options that may be available from various cloud service models. Such calculations should take into account the costs and benefits of various models of technology architecture, including on premises storage, private dedicated cloud, hybrid, and public cloud models. These various models will offer various advantages and disadvantages from the standpoint of managing risks associated with expense, confidentiality, integrity, availability, redundancy, resilience, reliability, and security of data and processes stored or operated from such systems.

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

INFRASTRUCTURE NEEDED

The development of a robust cloud ecosystem requires resilient network connectivity on a national and state level. The National Institute of Standards and Technology (NIST)[2] depiction of general cloud environments describes a cloud system as a collection of computing resources the customers can access over a network. They employ a server-side model, which means that customers can send messages over a network to server computers, which then perform work in response to the messages received – see figure below.



India is in a good position to become a regional hub for Asia's cloud and data centre needs. There are opportunities to build economies of size and scale in the country, and integration with the global value chain is easy with its large English-speaking population.

In recent years, there have also been many opportunities to develop large-scale infrastructure projects – such as data centre builds – at a comparatively lower cost to the

[2] NIST, 2012, Cloud Computing Synopsis and Recommendations: Recommendations of the National Institute of Standards and Technology http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-146.pdf

region. In addition, while there are challenges that come with the lack of a cross-country electrical grid at the moment, there has been much progress made in electricity and sustainable power development in India, particularly in the northern States of India.

Other infrastructure challenges center around a range of networking and telecommunication issues, detailed below:

1. *Relaxing rules around access to dark fibre.* There are numerous licenses under which a vendor can lease dark fibre in India, such as IP-I (Infrastructure Provider), UAS (Unified Access Services), NLD (National Long Distance License), ISP (Internet Service Provider) and the latest (which will replace all of the foregoing from 2012 and on), UL (Unified License). These licenses typically include onerous obligations and restrictions on the vendor, and even include restrictions on the types of customers to whom the vendor can lease dark fibre. Because CSP use of connectivity involves use of dark fibre for Amazon's internal purposes to connect our data centres, it is not expressly addressed by applicable law, and thus many carriers take the conservative view that they cannot lease dark fibre to any person that is not a telecom licensee. *This is a regulatory obstacle which should be addressed and removed in order to allow more data centre investors to build and connect data sites in India.*

2. *Develop an open Internet exchange* – India's Internet exchange (the "NIXI") could be improved to be a more open internet exchange. We recommend that a truly open exchange model be implemented for all cloud service providers to interconnect, similar to the AMS-IX exchange (in Amsterdam) and other large and successful peering fabrics. Such a model supports more robust and lower cost exchange of data between content providers and Indian customers and end consumers. A successful exchange will not only make an India investment more attractive to data centre players, but will also bring more local content and allow greater performance.

3. *Allowing and regulating access to telecom or other duct for fibre optic cable, and constructing fibre ducts where none exist* – If a cloud service provider were to build within India and meet with success and increasing demand for their services, they will require additional data centres to be constructed near the initial data centre build. To link these "parent and child" data centres, a cloud provider would use bulk dark fibre, deploying thousands of fibre strands. This bulk fibre reduces the overall cost of data transmission, eliminating costly Dense Wavelength Division Multiplexing (DWDM) equipment and enabling low cost data transmission.

   India should allow cloud providers the ability to license or lease duct or other cable pathways from an Indian Licensed Telecom Operator, or any utility provider and to construct a fibre cable dedicated exclusively for their use between the "parent and child" network nodes and data centre facilities. Duct licenses or leasing rates and terms should be regulated in order to be commensurate with rates for similar services in Frankfurt, Germany, or Dublin, Ireland.

Where existing telecom duct is not available for lease (because it either does not exist, or the operator has constrained capacity, or specific routing is needed for diversity), new ducts will need to be constructed as part of site development or expansion, utilizing public land to construct a duct or other cable pathway. These ducts will be dedicated exclusively for the cloud provider's use, and built with the appropriate engineering, consultation with the municipality and other utilities, constructed using quality materials and maintained over its life.

4. *Amending rules around network equipment for cloud providers* – there are many pieces of equipment used by cloud providers which are similar or identical to telecommunications equipment, such as Ethernet and optical switches, routers and transmission equipment. To encourage data centre development, India should permit the importation and use of network equipment that is used by cloud providers elsewhere in the world, irrespective of whether that equipment has a dual-use as telecommunications equipment, provided that the network equipment utilizes a physical medium (copper/fibre) and will not utilize radio spectrum for communications.

Protocol for sharing data between states, and between the state and central government

The more data that can be exchanged securely between states, and between the state and central government, the more efficient a government will be. Different types of data can and should be shared with different protocols. These decisions on data sharing methodologies and protocols should be developed in tandem with a Data Classification regime (see Q14).

A national policy around data sharing on cloud should be discussed and implemented, rather than to have 30 differing state-level policies for data sharing which would be inefficient and undesirable.

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 centres and cloud services platforms in India?***

There are a multitude of reasons to invest in India, and some favourable considerations for private sector investment include the following:

1. *Tax subsidies to building data centres* –Tax subsidies are important because they helpkeep operational costs down for the cloud provider, who can then pass on the cost savings to customers. Some states (such as Tamil Nadu, Maharashtra, Telangana, etc.) have tax incentives for cloud development, which is an incentive that could be deployed on a national level, rather than only limited to the state. These subsidies should be clear and unambiguous, and should not be changed or cancelled with changes in government administrations.

Consider exemptions or rebates of entry taxes, VAT, customs duties, and GST for data centre related equipment (including imported equipment) and ease compliance for existing programs for data centres (i.e., STPI data requirements).

Another tax incentive would be tax benefits associated with employing local staff, and exceptions for importing expatriate expertise when so required. Tax exemptions for initial import and setup of data centre equipment would also be an incentive for data centre providers to set up in India.

Provide tax incentives or grants for educational certifications in the cloud industry to encourage the labour force to become skilled in cloud applications to provide a ready labour force.

2. *Cheaper land and electricity* – Available subsidies and access to land for data centre builds would be desirable, as would guaranteed lower electricity tariffs.

   Provide support for infrastructure investment (energy, water, fibre, etc.) by state and local governments to encourage readiness for data centre investment.

3. *Creating data centre-specific economic zoning and incentives schemes,* as current schemes are often written with manufacturing in mind, and do not lend themselves easily to developing digital services. Consider developing grant programs similar to the Mega and Ultra Mega programs that exist for manufacturing to encourage large scale investment.

   Consider zoning rules that allow for precertification of sites for data centre use to enable the data centre to come on line quickly. Provide single point of contact (one stop provider) at the local level to ease the ability to get permits and approvals for data centre projects.

4. *Creating data centre-specific economic zoning and incentives schemes,* as current schemes are often written with manufacturing in mind, and do not lend themselves easily to developing digital services.

5. *Create incentives for managed services to grow as an industry.* India is also the managed service provider to the world, and should seek to maintain its lead in this sector. One incentive to develop the demand for data centres, and also encourage innovation in cloud service platforms, would be to provide tax and other incentives to local companies (such as Infosys) to develop their managed services capabilities, so that they can use cloud to accelerate their global reach.

6. *Increasing incentives for local cloud demand* - Private sector investment is driven by customer demand, and therefore incentive programmes to increase local appetite and demand for data centre and cloud services should also be put in place. For example, Singapore has a Productivity and Innovation Credit Scheme

(PICS) which allows small and medium enterprises (SMEs) to claim up to 400% in tax rebates for using technologies such as cloud computing.[3]

[3] Inland Revenue Authority (IRAS) Singapore Productivity and Innovation Credit Scheme, 7 Jun 2016, https://www.iras.gov.sg/irashome/Schemes/Businesses/Productivity-and-Innovation-Credit-Scheme/