ITI

July 25, 2016

Shri A. Robert J. Ravi
Advisor (QoS)
Mahanagar Door Sanchar Bhawan
J.L. Nehru Marg, (Old Minto Road)
New Delhi – 110 002, India

Via email: advqos@trai.gov.in

Comments of the Information Technology Industry Council (ITI) on TRAI Consultation Paper on Cloud Computing

The Information Technology Industry Council (ITI)[1] welcomes the opportunity to comment on the Telecom Regulatory Authority of India's (TRAI) "Consultation Paper on Cloud Computing," as published on June 10, 2016.

ITI represents the world's leading information and communications technology (ICT) companies, many of which provide products and services that support the global Internet or "Cloud" computing. Our companies also are global, earning a substantial portion of their revenues from foreign markets, conducting extensive cross-border business, and managing global supply chains. As a result, we understand the impact of international policies on ICT innovation, deployment, and use around the world.

ITI applauds the TRAI for holding this public consultation on Cloud computing and seeking stakeholder input on a policy that will significantly impact India's ability to achieve its ambitious goals of a Digital India and will shape how the country competes in the global economy. We support the TRAI's role in clarifying the rules governing Cloud and recognize that this is an essential step to bring predictability to the development of the market. In addition, we note that the Department of Electronics and Information Technology (DeitY) has also been active in this process and we encourage coordination between the agencies and throughout the Government to ensure a clear, consistent approach.

[1] Based in Washington, D.C., the Information Technology Industry Council (ITI) is the global voice of the information and communication technology (ICT) sector. ITI's member companies are some of the largest investors in India, with many having manufacturing facilities in the country. As the premier advocacy and policy organization for the world's leading innovation companies, ITI navigates the relationships between policymakers, companies, and non-governmental organizations, providing creative solutions that advance the development and use of technology around the world. Visit www.itic.org to learn more. Follow us on Twitter for the latest ITI news @ITI_TechTweets.

Realizing the benefits of Cloud computing requires a legal and regulatory framework that promotes innovation and supports development of Cloud infrastructure. It also requires policies that encourage Cloud adoption by giving users confidence that their privacy and security will be protected. More fundamentally, the growth of Cloud computing, and the Cloud's value to nations' businesses, citizens, and economies, will continue only if its development is guided by the same open approach to an international policy framework that has long enabled the dynamic growth of the Internet and ICT more broadly.

ITI recommends that policymakers in all countries adopt Cloud policies that are consistent with and build from more broadly applicable ICT policies. While Cloud technology does represent a shift, many of the ICT policy principles that have been long developed through public-private partnerships remain applicable and indeed vital. The following six recommendations are consistently important across ICT policies and will be critical to realizing the full benefits of Internet as well as Cloud computing:

- **Innovation Policy.** Ensure that policies encourage innovation in ICT, enabling domestic industry and local populations to generate, utilize, and build on top of the latest technologies.
- **International Cooperation**. Promote interoperability and mutual recognition of adequacy in data privacy and security laws and policies.
- **Trade.** Avoid discriminatory market access trade practices and policies that restrict the transfer of information and data across borders.
- **Cybersecurity**. Improve cybersecurity holistically, considering risks to traditional ICT environments as well as to Cloud technologies and applications.
- **Broadband**. Aggressively roll-out high speed broadband networks that are critical to many ICT functions, including connecting to and expanding the Cloud.
- **Standards**. Continue to rely on global ICT standards developed via standard-setting processes that are consensus-based, transparent, and industry-led, with participation open to interested parties.

It is within this context that ITI offers the following comments on the TRAI's Consultation Paper.

ITI and its member companies would like to be an ongoing resource for the government of India, as it addresses the policy challenges necessary to create an ecosystem that fosters Cloud adoption. We have chosen to address those questions posed in the TRAI's Consultation Paper where we can offer recommendations based on our global experience and encourage the development of a robust and secure Cloud framework. Given the short duration of the initial comment period for this Consultation Paper, however, we hope that TRAI provides adequate time beyond the July 25th deadline for all global stakeholders to address the many issues it covers in further detail. In that regard, ITI would welcome opportunities to provide input on this consultation in person to TRAI.

- **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?**

Many of the greatest benefits of Cloud computing systems are derived from cost reductions as a result of their economies of scale. First, costs associated with maintaining data center infrastructure are greatly reduced. Computing systems require cool environments, reliable power, and professional staff for their maintenance and operation. Physically locating large amounts of infrastructure in centralized locations reduces the marginal costs of maintenance per unit by consolidating environmental controls, power distribution, and reducing the cost of professional staff. In addition, when processing power and storage is consolidated, underutilized assets are reduced. Processing power is used in bursts for demanding applications. When processing power is centralized it can be used more consistently, spread between multiple client computers. The same concept also applies to data storage: one computer may underutilize its storage capabilities while another may require continuous upgrading. When all mass storage is moved to the Cloud, this discrepancy is eliminated by sharing storage, each client using as much as they need and no more. This readjustment of the client-server relationship allows organizations to reduce investment costs in individual computers by consolidating efficiencies in server systems.

In addition to physical system efficiencies, Cloud computing also provides significant digital economies of scale. Consolidating processing power not only allows for efficient investment in infrastructure and more consistent usage of assets, but it also allows for faster, more efficient processing of applications and big data. Analysis of large data sets can be incredibly taxing on computing systems and take a significant amount of time, but when done in the Cloud this operation is not only less taxing on any individual systems, it is also completed in a timelier manner. In addition, consolidation of system security into a central facility provides large cost reductions for service providers. Security for distributed systems can be costly and hard to manage when compared to central systems, which, for instance, can more efficiently manage physical security of datacenters and afford to invest in more robust methods of security. In addition, large cloud service providers in particular have much broader visibility of malware threats and the ability to make their customers aware of such malware more efficiently.

Savings as a result of the shift to cloud computing cannot be understated. This shift is a direct result of the economies of scale present in Cloud computing systems as well as how Cloud systems allow organizations to shift to managing services rather than assets, requiring fewer personnel and reducing risk. In addition, Software as a Service (SaaS) cloud deployments reduce distribution costs and underutilized applications as organizations can pay for software as needed. This improves scalability of software and allows software producers to constantly update applications without any action from the consumer. Not only does this provide software security to be seamlessly up to date, it also allows organizations to maintain maximum productivity with limited time and money spent on upgrading software systems.

All of these efficiencies reduce costs for organizations. The U.S. government estimates that its shift to Cloud computing reduced its data center infrastructure budget by 30%,[2] allowing it to shift those funds to high-value activities. Overall reduction of computing costs can also greatly reduce barriers to market entry for SMEs, allowing for greater levels of innovation and growth. Cloud computing allows SMEs to scale more effectively because they can buy computing services as needed instead of making large upfront investments in data center infrastructure. The result is a more vibrant and dynamic economy across all sectors.

- **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?**

"Cloud computing" is not a new technology. It is a new name for distributed, or Internet-based computing – which has been used for decades (web-based e-mail is an example). While it is true that innovations such as faster broadband and greater data storage capacity have allowed new cloud-based business models to flourish and greater use of cloud computing generally, fundamentally these innovations have impacted the broad and explosive growth of the Internet in similar ways. The open, non-regulatory approach to an international policy framework that has long enabled the dynamic growth of the Internet and ICT generally over the past few decades also holds key insights for governments to take to the growth of the cloud.

We advocated earlier in our response against the adoption of cloud-specific regulations that are inconsistent with broader ICT policy principles; with respect to "data control," we similarly counsel against inconsistent, cloud-specific regulatory mandates. First, existing data protections are relevant to data stored in a cloud environment; as stated above, cloud computing is simply the latest evolution of distributed, internet-based computing. Second, as

[2] Kundra, Vivek, U.S. Federal Could Computing Strategy, February 8, 2011. (See https://cio.gov/wp-content/uploads/downloads/2012/09/Federal-Cloud-Computing-Strategy.pdf)

the question implies, data moves in and out of “the cloud” all the time – attempting to mandate requirements regarding the storage or movement of data in the cloud that are somehow different from data traversing the internet or stored locally seems difficult if not impossible to implement – ultimately, because data will move from one environment to another, the government should adopt an approach focused on data more broadly.

The concept of “data control” is an important, though somewhat novel, concept in data protection law more broadly. Historically, data the concept of “control” over ones data has perhaps been implicit in the data protection/privacy principle of “choice” or “consent” (as found in the FIPPS, APEC privacy principles, etc.) – and the concept of choice/consent has been expressed as giving consumers options to control how their data is used. Specifically, choice relates to secondary uses of information beyond the immediate needs of the company collecting the information to complete the consumer's transaction. The two typical types of choice models have traditionally been 'opt-in' or 'opt-out.'

Regulatory mandates are not required to implement and enforce the principles of notice/choice or control. Indeed, giving consumers “control” over their data – whether in the cloud context, or any other context – can be achieved via company commitments such as privacy policies, provided there is an enforcement backstop (in the U.S., the Federal Trade Commission has such power. This concept can also be achieved via multilateral fora such as APEC – as stated above, the APEC privacy principles embrace the concept of choice. The new Privacy Shield Framework, freshly negotiated between the U.S. and EU, also includes a choice principle.

In order for consumers to widely use Cloud computing for their personal and professional needs, they should be afforded the opportunity to exercise choice or control over what personal data companies collect from them and how they use it, whether that data resides in the Cloud or not. Exercising choice or control over data is a fundamental need in order to build consumer trust, and ultimately providing that choice or control should be the responsibility of Cloud and other companies. However, regulations to require consumer control of data are unnecessary if not redundant; Cloud providers and other companies must provide choice and control over data in order to be successful in a competitive market

Where regulation may play a part is to provide an enforcement backstop behind the user/provider agreements that guarantee consumer choice/control of data. Such regulation would allow for flexible agreements between consumers and Cloud service providers and would encourage consumer confidence in Cloud services, leading to increased Cloud usage. Any potential regulation should map to relevant global standards, such as ISO 27018, which requires that cloud providers operate according to six principles, including explicit customer control of how their personal data is used.

- **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?**

Our industry strongly supports the goal of making IT systems in general, and Cloud systems in particular, interoperable. In fact, that is a key competitive advantage of commercial-off-the-shelf (COTS) technology relative to custom-developed systems. However, we also believe that interoperability can be achieved through the market-based development and adoption of international standards. Standards should not only be interoperable within India, they should also be interoperable globally to keep Cloud services harmonized and easy to navigate. Some relevant global standards and best practices that India may benefit from referencing including ISO 27001, ISO 27018, the NIST Cybersecurity Framework, and the Cloud Security Alliance Framework.

ITI will address the following four questions together:

- **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.**
- **Question 11. What are the termination or exit provisions that need to be defined for ensuring 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?**
- **Question 13. What should be the roles and responsibilities in terms of security of (a) Cloud Service Provider(CSP); and (b) End users?**

Governments should adopt cloud solutions for data services to help ensure public safety, improve the energy efficiency of operations and address domestic and global issues. Governments that move services to the cloud see tangible improvement in interactions with individuals, greater efficiencies and cost savings.

Cloud service providers should rely on globally harmonized, industry-led security best practices and standards, as well as government incentives for organizations to adopt security technologies. These best practices need not and in fact it is preferable that they are not specific to cloud providers, but rather to all companies inhabiting the ICT ecosystem.

Government agencies and organizations should work to ensure an appropriate balance between the number and strength of controls and the risks associated with Cloud computing solutions. The transition to an outsourced, Cloud computing environment is an exercise in risk management. Risk management entails identifying and assessing risk, and taking the steps to reduce it to an acceptable level. Throughout the system lifecycle, risks that are identified must be carefully balanced against the security and privacy controls available and the expected benefits. Too many controls can be inefficient and ineffective.[3]

The increasing number of recent high-profile cybersecurity attacks highlights how critical it is for Cloud service providers to protect the data running applications on their Cloud systems. Users depend on the reassurance of CSPs that they are using the latest technologies and methods to provide this security. However, the mandate of any specific technologies to achieve this goal will stifle innovation, reduce the flexibility of security solutions and, ultimately, make the Cloud less secure. Security and data protection are global issues not limited to the Cloud, and companies must have the freedom to develop appropriate measures to address them globally. There is no one-size-fits-all solution.

While we understand that India seeks to provide greater assurance that Cloud computing services provide adequate security, levels of service, and data privacy protections, many of these issues are already addressed in either government policies or by vendor practices (such as contracts). If they seek to supplement these existing policies or practices, governments should ensure that new provisions for security are aligned with global standards and best practices, including ISO 27001 and the NIST Cybersecurity Framework.

- **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?**

While laws restricting cross-border transfer/disclosure of certain information may differ from country to country, the success of Cloud computing depends on the uninterrupted flow of data across national borders. This is one reason ITI consistently advocates against data localization requirements, no matter what form they take. Another is that mandating that data be stored within a jurisdiction does not enable consideration of how to maximize the security of information – the quality of the infrastructure and the technical specifications are important

[3] Source: Federal Cloud Computing Strategy, Office of the U.S. CIO

considerations, and these must be considered without limiting the geographic location. Additionally, storing data in multiple jurisdictions can increase overall security in cases of natural disasters or other occurrences that would require a single data center to be offline for a certain period of time. Thus, as a threshold matter, we would advise the GOI against adopting laws that restrict the cross-border transfer of data – whether in the Cloud context or more broadly.

Nevertheless, we do understand that some countries continue to restrict the cross-border transfers of certain data. For instance, in the EU, Directive 95/46 (to be replaced in 2018 by the EU General Data Protection Directive) makes it unlawful to transfer data from the EU to any third country unless that country's laws have been deemed to provide an "adequate" level of data protection. While the EU's approach is doubtless well-intended, it has threatened real world negative economic impacts on international trade. The potential for the EU model to negatively impact trade is not hypothetical, as we have recently seen play out in the context of the Court of Justice of the European Union's invalidation of the EU-U.S. "Safe Harbor Framework" in the *Maximilian Schrems v Data Protection Commissioner* case. The case has jeopardized the transatlantic trade relationship between the U.S. and EU – the largest trade relationship in the world – and while the two countries recently announced a successor to the Safe Harbor, the Privacy Shield Framework, to attempt to facilitate data flows in compliance with EU law, legal challenges to Privacy Shield are also expected, and a significant amount of business and economic uncertainty is expected for the foreseeable future, impacting all sectors and businesses of all sizes in both the EU and U.S.

The governments of the EU and the U.S. have worked tirelessly over the past two and a half years to negotiate the Privacy Shield framework, which is intended to minimize conflicting legal requirements on companies, including CSPs. However, this example involves just one bilateral relationship, and calls into question whether the EU's "adequacy" requirements are efficient or scalable globally in the digital age. The need for prior approval for transfers is administratively burdensome and does not seem feasible in the context of the global economy and the continued need for international data transfers. Additionally, significant resources are required to implement an EU-style "adequacy" regime for international transfers. Alternatively, flexible mechanisms should be considered to facilitate cross border data transfers, including commercial contractual terms and industry codes and conduct.

A potentially more efficient and productive model can be found in the Asia-Pacific Economic Cooperation (APEC) forum's Cross Border Privacy Rules System (CBPR), which facilitates international data transfers while protecting privacy within the Asia-Pacific region. This executable mechanism allows an efficient basis for international data transfers, while ensuring an appropriate level of protection of personal data[4]. The APEC CBPR system is also far more efficient, in that it allows for countries to designate certification agents within their borders, while at the same time embracing the concept of mutual recognition of such company certifications. This is a more efficient means to facilitate trade relationships between countries, and by which companies can be certified to do business across the entire Asia-Pacific region if certain stringent criteria are met, due to the concept of mutual recognition. The mutual recognition concept also helps facilitate enforcement activities having extraterritorial impact.

In terms of what disclosure guidelines need to be in place, as noted in response to question 5 above what companies' practices are with respect to responsible onward transfer practices can be set forth in companies' privacy policies or terms of service or other accountability mechanisms, and enforced via appropriately empowered institutions. Transparency should be the rule. Clients should be informed in their CSP's terms of service of how data may be transferred or disclosed. This transparency is critical to the increased adoption of Cloud computing, as it gives users the confidence that their information will not be used or disclosed in unexpected ways and it helps identify potential legal conflicts.

- **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.**

India already has sufficient laws in place under the IT Act, Consumer Protection Act, and other related provisions, and market forces and customer requirements can address any gaps that emerge. Over regulation will deter growth of the cloud industry in India. Global companies must act globally, and non-globally standard requirements such as burdensome licensing may outweigh the benefits of serving the market – the result may be less Cloud providers in India. Further, the cost of compliance and penalties will ultimately likely be factored into cloud services, and ultimately passed onto users—further impeding growth.

India will be a $4.5 billion data center market by 2018. Private Clouds in India are expected to help save Indian companies up to 50 percent on infrastructure costs and will create more than 100,000 jobs by 2016-2017. Demand for Cloud services in India is expected to be strong. Between 2013 and 2017, business-process-as-a-service is expected to grow from $63.6 million to $168 million; software-as-a-service from $174 million to $552 million; and infrastructure-as-a-services from $59.2 million to $156.3 million.

[4] http://www.cbprs.org.

This massive growth would be jeopardized by the imposing of license or registration requirements for CSPs which will add unnecessary costs and delays to Cloud deployment, send the wrong market signal, and act as a disincentive to start or scale up Cloud services. Even without these requirements, CSPs would still be subject to applicable laws. In addition, the rules governing the procurement of Cloud services should not be based on the traditional contract terms and conditions related to the purchase of hardware or software. In order to maximize the benefits of the Cloud, it is necessary to have an environment that supports speed and flexibility in this process.

- **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?**

ITI's companies operate in accordance with the laws of all jurisdictions in which they do business, including India. First, as we have noted repeatedly in our response, it does not seem to us that CSPs should be subject to a different set of laws or rules than any other companies operating in India pertaining to lawful government access to information. While we are not experts in India's laws in this regard, it seems to us that, with few exceptions, any request to CSPs from the government of India for lawful access to data should be made via a formal legal process and be fully transparent. ITI's companies will doubtless respond accordingly, in accordance with India's laws.

Of course, we are aware that, in some cases, the government of India may seek to access data stored in another jurisdiction for lawful investigative purposes. We are also aware that law enforcement requests to access data in other countries often raise complex and difficult jurisdictional and conflicts of laws issues, and that current mechanisms for addressing this problem, such as Mutual Legal Assistance Treaties (MLATs), are not always efficient. We recommend to the government of India, and to all governments, that greater efforts be made to prioritize Multi-Lateral Law Enforcement Cooperation. In order to increase public safety and security and make investigations and prosecutions more efficient, governments should expand investment in cross-border data request mechanisms for law enforcement and counterterrorism purposes, including making MLATs more effective tools for cross-border investigations, and leverage existing multilateral agreements, such as the Budapest Convention on Cybercrime. We support a call to action to all governments to prioritize global law enforcement coordination to better address these issues.

- **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.**

Our answer to this question will focus on part (b) of this question. As a general matter, ITI recommends to governments all over the world, including the United States, to avoid requiring firms to locate computing facilities, including data centers, domestically in the pursuit of their legitimate public policy objectives. We especially advise avoiding data localization requirements as a means to promote the establishment of data centers or to support the development of Cloud computing services. While a regulator or economic planning ministry may believe that a data localization requirement may be an attractive means of forcing firms to build data centers in India, the quantitative and qualitative evidence in markets across the world indicate that such requirements serve as a disincentive for foreign firms to invest domestically and make it more expensive for local firms to enter and compete in the domestic market or compete and enter global or regional markets. A 2015 study by the Leviathan Security Group estimates that for many countries that are considering or have considered forced data localization laws, local companies would be required to pay 30-60% more for their computing needs than if they could go outside the country's borders.

ITI is not alone in taking this view. Globally, the G7 ICT ministers in April agreed to oppose data localization requirements in their joint declaration[5]. The United Nations Conference on Trade and Sustainable Development (UNCTAD) in its recent report on data protection regulations and international data flows argues that data localization requirements pose a barrier to all businesses, particularly small businesses and new entrants to markets, and create unrealistic compliance burdens[6]. In the overview to the report on page xiii, UNCTAD stated: "National data protection laws should avoid (or remove) clear obstacles to trade and innovation. This may involve avoiding or removing data localization requirements that go beyond the basic options for the management of cross border data transfers." The parties to the Trans-Pacific

[5] G7 ICT Ministers Joint Declaration, paragraph 17: "We continue to support ICT policies that preserve the global nature of the Internet, promote the flow of information across borders and allow Internet users to access online information, knowledge and services of their choice. We oppose data localization requirements that are unjustifiable taking into account legitimate public policy objectives."

[6] UNCTAD report on 'Data protection regulations and international data flows: Implications for trade and development', pgs 20 and 60.

Partnership have agreed in the E-Commerce chapter in Article 14.13 not to use data localization requirements as a condition of market access: “No Party shall require a covered person to use or locate computing facilities in that Party’s territory as a condition for conducting business in that territory.”

A recent study indicates that existing data localization requirements in India have resulted in negative economic impacts. A May 2016 study from the Center for International Governance Innovation (CIGI) and Chatham House indicates that India’s data processing regulations (Data retention provision of Information Technology Act, proposed National Security Council Secretariat strategy on cyber security plus proposed licensing requirement by Department of Telecom), has resulted in a .22 total factor productivity (TFP) loss for all sectors of the economy, with a .52 TFP loss for business services and a 1.31 TFP loss for communication services. The study’s authors calculate that India’s data localization requirements have resulted in a .25% decrease in real GDP.

Given the above, further data localization requirements in India would not just dissuade foreign firms from investing in the Indian market; they would also make local tech companies and other users of international Cloud computing services less competitive. According to the Internet & Mobile Association of India[7], Indian entrepreneurs rely on international Cloud service options. Flipkart used data centers in Canada when it was founded. Myntra, an eCommerce platform, and redBus, an online bus ticketing company, have hosted their servers with Amazon Web Services. Zoho Corp, founded in 1996 in Chennai, operates data centers in California and New Jersey. Forcing these companies to repatriate their data to India would impose significant data transfer, infrastructure, and compliance costs on them.

- **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?**

Many of the benefits that are derived from the use of Cloud storage come from the economies of scale that are gained through multi-tenant environments. Cloud service providers plan and allocate their technical resources as efficiently as possible to best serve all of their clients, allowing them to provide the lowest prices possible. Because of this, from an economic standpoint, broadly requiring a dedicated Cloud for an agency, ministry, or government as a

[7] Internet & Mobile Association of India – “Conducive Policy and Regulatory Environment to Incentivize Data Center Infrastructure”

whole may erode the very cost-savings that is often at least a partial motivation for switching to Cloud services in the first place.

Despite this, system security should be the foremost concern for government users of Cloud services. However, security in the Cloud, when handled by a competent Cloud service provider, is not a function of the location of the data. In fully virtualized systems, data is partitioned between clients so that each partition has a different set of security and access settings. If Cloud service providers adhere to security requirements defined by the government entity that is using the Cloud, the number of tenants that use that same Cloud service is not a significant factor. Therefore, government entities do not need dedicated Cloud services in order to maintain security, and accepting multi-tenant environments allows the government entity to receive the lowest price available for its specified security requirements. If governments perceive a need for a dedicated environment, then they should limit the data and services hosted there to those that involve only the most sensitive data; the vast majority of government data and services are suitable for multi-tenant environments.

- **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?**

ITI believes that the most effective incentives to support the promotion of Cloud services in India are generally the same ones that would support the broader goals of Digital India and the Make in India initiatives-- namely those that improve the "ease of doing business" in the country. A recent paper by NITI Aayog outlined how benefits such as tax incentives, clarifying tax obligations, reducing duties on imported inputs, and creating coastal economic zones with well-developed infrastructure can help achieve this goal.[8] Any such incentives should be applied in a non-discriminatory way between domestic and foreign investors.

In addition to these incentives, it is important that the government of India recognize and address current policies that are working against the promotion of Cloud adoption and limiting India's access to and ability to develop cloud technologies. Among others, these policies include:

[8] "Make in India Strategy for Electronic Products," (Draft consultation document as published for stakeholder comment), NITI Aayog, Government of India, May 2016.

- Customs duties of up to 10% on telecom equipment and technology components that drive up the costs for CSPs and users.
- Requirements under the Department of Electronics and Information Technology (DeitY) that servers and storage equipment undergo redundant local testing and certification for product safety.
- Ministry of Environment, Forests and Climate Change (MOEFCC) restrictions on the import of used equipment that limit the ability of manufacturers to service their cloud equipment with spare parts and to conduct R&D to develop improved cloud technologies