USIBC Response to TRAI Consultation Paper on Cloud Services

Clause	Comment	Recommendations
Q.1 Whether there should be single industry body or multiple industry bodies of cloud service providers which may be registered with Department of Telecom (DoT)? Should the industry bodies be registered based on the category or type of CSPs? Can a CSP be a member of multiple industry bodies? Please suggest with justification.	Given the desire for "light-touch regulation" there is more than sufficient regulation of cloud services in industry absent an additional layer of mandatory industry body(ies) and/or a Mandatory CoC, and thus Indian CSPs should not be subject to new DOT regulation. Contrary to widespread misconception, CSPs in India do not exist in a legal vacuum, and are amply governed by various regulations including MeitY's IT Act and *MeghRaj*, DOT's TSP and OSP regulations, consumer protection via the CPA, contract law via the Indian Contract Act, 1872, and likely compliance with the draft PDPB. Specific details on existing CSP regulation are included in Q.7.	Reconsider the need for mandatory industry body(ies) as there is sufficient regulation of the cloud via the IT Act, CPA 2019, regulation via TSPs, OSP, and other licensed categories.
Q.2 What should be the eligibility criteria for an industry body of CSPs to register with DoT? What is the list of documents that should be required to be submitted as proof of eligibility? What obligations should be cast upon the industry Bod(y)(ies) after registration with DoT? Please suggest with justification.	The composition of the industry body(ies) should be determined on those CSPs that opt to join and fund the organization. Since the make up of the founding members is not known, TRAI should defer these questions to the founding members via a multi-stakeholder discussion. The membership will vary over time, so setting up criteria in advance could pre-determine or undermine the outcome and effectiveness of such industry body(ies).	The industry body(ies) itself should define its own criteria after a multi-stakeholder workshop using an iterative process with leading CSPs, users, and consumers. Ultimately, the criteria the body(ies) create should be flexible, and allow for changes over time as the industry and technology evolve.
Q.3 What may be the threshold value of parameters such as the volume of business, revenue, number of customers etc. or combination of these for a CSP to mandatorily become member of a registered industry body? Please suggest with justification.	Participating in the industry body(ies) should be voluntary and not mandatory because TRAI seeks a light-touch and innovation focused regime. Simply put, forcing companies to join and pay into an industry body(ies) is not light touch. Further, the fees could provide a barrier to entry for smaller, niche, sector-specific CSPs, particularly for start-ups, and innovators that do not fit the common mold of today's CSPs. The industry structure for cloud services is evolving, but to ensure sustainability of the industry body(ies), as well as impact on its members, should be left to the new organization itself. For	Membership should be voluntary, and the industry body(ies) itself should determine the appropriate thresholds and fee structure, which will change over time.
Q.4 Whether entry fee, recurring fee etc., need to be uniform for all members or these may be on the basis of type or category of members? How such type or category can be defined? Should such fee be prescribed by DoT or be left to be decided by the industry body? Please suggest with		

Clause	Comment	Recommendations
justification.	example, there are different models that can coexist based on size, sector, and geographic reach, so the industry body(ies) might include differing products and services for different communities of providers. Likewise, there might be a role of other stakeholders as well around standards, technology, general business associations, consumers, et al. The same can be said for fees and governance. Therefore, a proscriptive structure might not align well with long-term sustainability by reducing effectiveness and utility of the new industry body(ies).	
Q.5 What should be the guiding principles for governance by an industry body? How would these principles/ organisation structure ensure fair, reasonable and non-discriminatory functioning of body? Should structure of Governance be prescribed by DoT or should it left for the industry body to decide? How can the industry body achieve the desired deliverables efficiently and effectively? Please suggest with justification.		
Q.6 What policy may be adopted for initial formation of industry body for cloud services? Please suggest with justification.		
Q.7 Any other issue which is relevant to this subject? Please suggest with justification	1) Given the desire for "light-touch regulation" there is more than sufficient regulation of cloud services in industry absent an additional layer of mandatory industry body(ies) and/or a Mandatory CoC. Contrary to widespread misconception, CSPs in India do not exist in a legal vacuum, and are amply governed by various regulations including MeitY's IT Act and *MeghRaj*, DOT's TSP and OSP regulations, consumer protection via the CPA, contract law via the Indian Contract Act, 1872, and likely compliance with the draft PDPB. A few specific details highlight that CSPs currently have a broad set of regulations, and the government currently has diverse authority to oversee the segment: **IT Act** • Section 43A requires CSPs to implement and maintain reasonable security practices and procedure, which govern collection, disclosure, retention, transfer, security and use of sensitive personal information; • Section 69 requires CSPs to co-operate with authorised	1) Reconsider need for mandatory industry body(ies) as there is sufficient regulation of the cloud via the IT Act and regulation via TSPs, OSP, and other licensed categories. 2) The sector regulator should have precedence over standards. Therefore, in cases where there is a conflict between the industry boy(ies) and regulators, the sector-specific regulator should have precedence over the industry body(ies).

Clause	Comment	Recommendations
	government agencies by extending all facilities and technical assistance) to facilitate electronic surveillance; and, • Section 79 stipulates that CSPs are categorized under ‘intermediaries’ and are required to comply with a wide range of due diligence requirements. Failure to comply with these requirements will result in CSPs losing safe harbour protection under the IT Act. ***MeghRaj*** • MeitY oversees the empanelment of CSPs with the government under its *MeghRaj* cloud computing initiative.[2] To meet standards of empanelment, CSPs must evince compliance with standards on security, interoperability, data portability, service level agreements, and contractual terms and conditions.[3] Such compliance by CSPs is also thoroughly verified by way of a rigorous audit conducted by the MeitY’s Standardisation Testing and Quality Certification Directorate (STQCD).[4] As the government agency responsible for cloud services, MeitY will step in to govern other aspects related to cloud services as and when needed. ***CPA*** • In Section 2(17), CSPs fall under the definition of an ‘electronic service provider’;	

[2] GI Cloud (Meghraj)- A cloud computing initiative of MeitY, *available at* http://meity.gov.in/content/gi-cloud-meghraj. (“MeitY cloud computing initiative”)

[3] Invitation for application/proposal for empanelment of cloud service offerings of CSPs, Ministry of Electronics and Information Technology, Government of India, *available at* http://meity.gov.in/writereaddata/files/Application%20for%20Empanelment%20of%20CSPs.pdf.

[4] MeitY cloud computing initiative.

Clause	Comment	Recommendations
	- In Section 2(16)ii, buying or selling of cloud-based services would qualify as e-commerce; and, - Section 94 cites that the central government is empowered to take measures for the purposes of preventing unfair trade practices in e-commerce. Such measures may relate to the trade practices of CSPs. ***PDPB*** - CSPs will be subject to a number of obligations as 'data processors' under the PDPB, including: - Clause 37, processing data only as per instructions of data fiduciaries by whom the CSP has been engaged; - Clause 31, implementing appropriate security safeguards through use of methods such as encryption and de-identification of data; and, - Clause 60, possibly complying with 'codes of practice' issued by the Data Protection Authority When added together with DOT TSP and OSP licenses, there currently exist a robust regulatory environment around CSPs that mitigate the need for an additional layer of mandatory regulation via industry body(ies). 2) It is important to note that there could be sub-sector specific requirements that may arise and could be notified by sectoral regulators. In such cases, the standards notified by the sectoral regulators should have precedence.	
Mandatory Provisions of Code of Conduct (CoC) (i)Adopt a constitution that is fair and non-discriminatory towards its members. The constitution should have provision to adopt the directions, orders or guidelines issued by the	TRAI emphasizes the importance of light-touch regulation, which is the opposite of mandating broad-based codes of conduct, particularly when the issues cover quotidian business topics like billing, service level, dispute management, et al. These issues are better left to companies and customers, as there is no one-size fits	CoC should mostly be a voluntary set of guidelines, best practices, certifications, et al.

Clause	Comment	Recommendations
Government from time to time. Constitution should also facilitate provision of sharing information with the Government or TRAI when asked by them from time to time. It should also facilitate investigation of the conduct of such industry body by the Government or TRAI to ensure transparency and fair treatment to all its members.	all approach. Further, proscriptive business policies will prevent innovators from coming into the market, noting that many business innovations are around business operations and processes, and not necessarily technology based.	
(c)Billing models: The code should lay down various credible billing models that can be followed by member CSPs and publish them on its website.	Billing models should be left to businesses to decide. The industry body(ies) as a part of its market research can make available information but this may not be part of Code of Conduct. The market forces should be allowed to decide the pricing and billing models.	
(d)Data security: The code should set out the recommended reasonable cloud security standard(s) to be followed by its members, pertaining to issues such as encryption of sensitive data, backup options, and disaster management strategy to protect information held by CSPs from misuse, interference, unauthorized access, and loss. All such standard information should be published on their website for the purpose of transparency. For instance, in Australia the Office of the Information Commissioner has issued a detailed guidance as to what would constitute reasonable steps" pertaining to data security.[5]	Important that entities be given flexibility to adopt the most suitable security practice, and not be limited or tied down to only certain specified standards. Securing data requires global vigilance and cooperation. It is important that global arrangements such as Security Trust Assurance and Risk (STAR) Program, which outlines key principles of transparency, rigorous auditing, and harmonization of standards are considered. The publicly accessible registry allows cloud customers to assess their security providers in order to make the best procurement decisions. Companies who use STAR indicate best practices and validate the security posture of their cloud offerings. Companies are given ratings, and such global alliances should be relied upon, including recognizing any performance ratings /certifications to avoid duplication of effort and compliance burden.	
(e)Dispute resolution framework: The code should set out a model framework for handling of complaints, including complaints pertaining to billing, metering and QoS, that	There is a possibility of conflict of interest where an industry body(ies) is also asked to adjudicate against one of its funding member. There is a need to have an independent arbitration and	Allow the industry body(ies), along with its members, to determine its

[5] Office of the Australian Information Commissioner ,Guide to information security (2013) , available at https://www.oaic.gov.au/images/documents/privacy/privacy-guides/information-securityguide2013WEB.pdf.

Clause	Comment	Recommendations
should be resolved by CSPs independently. The code may also require CSPs to publish periodic reports on their website of the complaints handled and resolved by them. Procedures may also be prescribed for handling of those grievances which have not been resolved at CSPs level.	resolution and the industry body(ies) may tie-up with an independent third party to perform this function.	role in dispute resolution.
(f)Model SLA: The code should also formulate a model template of SLAs which sets out model clauses pertaining to technical and legal aspects of CC - such as QoS, customer satisfaction, security, data protection, pricing and action in case of SLA violation - for the protection of the customers. This will ensure that safe and fair terms conditions of contract are drawn up by big and small market players alike. For instance, the EC also facilitated an industry group, called CSIG SLA subgroup, which prepared a set of SLA standardisation guidelines for CSPs and professional CC services customers. These guidelines lay down the principles for developing SLA standards for CC services along with objectives to be achieved through these SLAs in terms of performance, security and data protection etc.	Each organizion requires its own set of service levels and quality, so there is not one-size-fits-all. Therefore, any mandatory, industry SLAs are not likely to permit the diversity of customer services requirements. Industry body(ies) should delve into this topic with careful consideration, as very low standardized SLAs service effectively serve limited purposes, while more robust, mandatory SLAs might drive un-needed services, extra costs, and could inhibit innovation. Therefore, USIBC strongly suggests that SLAs be kept out of any mandatory requirement, and any contract or consumer issue should be approached via contract law, *MeghRaj* requirements, or consumer affairs protection.	Model SLAs should be voluntary in nature. Members should be allowed to offer innovative services and cannot be restricted by the SLAs.
(g)Disclosure framework: The code should set out a disclosure mechanism to promote transparency in cloud services. This may include requirements to make disclosures regarding location, migration and outsourcing of cloud data to third parties along with disclosures on security and interoperability. For example, under the New Zealand Cloud Code, a signatory CSP is required to disclose critical details regarding their cloud products and services such as- i. who has ownership of data ii. how data security is ensured iii. where data is located iv. how data can be accessed and used by customers etc. The CloudCode does not impose any legal obligations on the signatories, however non compliance with the code can	The constitution should provide for information sharing only in response to specific requests for information, with clear reasons for the request and how it will be used, with disclosure to the CSP members on information sharing, unless it is a matter of national importance. The disclosure framework should be aligned with the model SLAs and maybe designed to be a voluntary disclosure and certification on compliance to the minimum SLAs as prescribed under (f) above.	Disclosures should be voluntary except for rare requirements tied to law enforcement and national security, and any such request should follow guidelines outlined in the IT Act.

Clause	Comment	Recommendations
attract liability under general law.		