

Annexure - I

OSPAI response to TRAI Consultation Paper on “Review of Terms & Conditions for registration of Other Service Providers (OSPs)” dated 29.03.2019.

We welcome the opportunity to submit Other Service Providers Association of India “OSPAI’ comments on the Consultation Paper on Review of Terms and Conditions for registration of Other Service Providers (OSPs) by Telecom Regulatory Authority of India “TRAI” dated 29.03.2019. Top priority was taken into consideration for unhindered growth of the BPO/ITeS sector who operate under the Other Service Providers (OSP) Guidelines issued by DoT, the following are requested.

Q1. Please provide your views on the definition of the Application Service in context of OSP. Whether, the Application Services which are purely based on data/ internet should be covered under Application Service for the purpose of defining OSP.

The existing OSP guidelines should be replaced with new framework which is forward looking, aligned to the frequent change in technology and supportive of growth of IT and ITeS sector. Existing definition is out of sync with latest technology. It should be revised to exclude Application Services and definition needs to be amended to “Outsourcing” and relevant to the intent of the OSP guidelines. OSPs do not provide any Application Service. In view of the original intent of the regulations, such services do not qualify under the definition of BPO, and are solely facilities provided to captive internal users call center services to captive users. Outsourcing companies providing services using Data/Internet/non-voice services should not be covered under OSP registrations. Only voice based outsourcing should be included under category of Outsourcing Services. GICs should be allowed to submit their applications under multiple categories. This will also help TERM cells to have better view of the activities as against clubbing everything under one heading to submit

applications under 'Call Centre' category. The Application Services should exclude all voice and data / internet-based services by the Indian entity to its other group companies within / outside India. Clear classification is required on who is OSP and who is not.

Justification: *Majority of the Multinational Companies (MNCs) have their offshore development centers, back-offices, shared services in India (Global Inhouse Centres ("GIC")). These GICs provide a multitude of support services to the global operations of their group companies. With the existing definition of Application Services nearly all activities/ services to their group companies date fall within the ambit of Application Services. For GICs - their group companies / affiliates are the actual customers. GICs calling activity is incidental to their services to group companies and actual number of resources involved in calling activities (inbound / outbound or both) are relatively low as compared to their overall headcount. Therefore, if the majority of the employees of any OSP are not engaged in 'calling activities' as understood for a typical call centre then such companies should be registered under ITeS category.*

Q2. Whether registration of OSP should be continued or any other regulatory framework should be adopted for OSPs so that the purpose of registration specified by government is met. Please furnish your views with justification.

The Registration of OSPs should be continued but validity period should be unlimited. It should be a one time registration with self regulatory intimations with bona fide intentions. Compliance check should be done through customer CIN. Change the word infringement. Even if an organization is not registered as an OSP but procures services like Leased lines/Bandwidth/ISDN PRI lines from TSPs, the TSPs can be authorized to evaluate the nature of business of the organization and conclude whether it qualifies to be an OSP/non-OSP and provide services subject to the outcome of the evaluation. The rapid change in mode of communication demands for revising rules to make them forward looking and make the rules

enabling for adoption of new technologies easily. Accordingly, the requirement of logical separation of PSTN and IP network should be discontinued. One of the basic philosophies behind the existing rules is not to cause 'infringement' of scope of licensed Telecom Service Provider i.e. TSPs which could result in loss of revenue to the government and the TSPs by merging PSTN network with MPLS / ILL/ Leased Line circuits. As part of the ease of doing business, the Government should promote self-regulation and TSPs can also ensure security compliance by the users. Anyone discontinuing services should intimate voluntarily to the TERM cell.

Justification: *The existing rules are subject to different interpretation by the TERM Cells; there is inconsistent approach for OSP registrations, advancement in the technology has made these rules out of sync / obsolete, there is less flexibility for the companies to adopt new technologies. Inability to deploy technology takes away the source of competitive advantage from India.*

Q3. What should be the period of validity of OSP registration? Further, what should be validity period for the renewal of OSP registration?

The provision related to Registration validity period of 20 years should be discontinued and it should be unlimited. There should be parity for registration with other registrations of DoT.

Justification: *Presently the Bank Guarantee and logging requirements make the setup cost unviable and hinder the Tier-2/3 cities for BPO operations limiting employment opportunity for such locations. With the emerging cloud based telephony solutions, present norms hinder the usage of such cloud based solutions as they could easily use app based voice calls using data thereby reducing telecom costs.*

Q4. Do you agree that the documents listed above are adequate to meet the information requirements for OSP registration? If not, please state the documents which should be added or removed along with justification for the same.

The registration process should be digital and online only and submission of hard copy should be a one time affair. Certificate of Incorporation (CIN) should be treated as proof of identity. Documentations at the time of registration viz., name of company, registered address, CIN, type of connectivity, name of service provider, type of connectivity, clients and bandwidth is sufficient. Application submission should not be linked to one authorized signatory - the companies should be allowed to authorize multiple representatives. To support digitalization, the requirement of submission of physical application should be discontinued and documents uploaded through registration portal only. OSPs with multiple locations should be allowed to register using one license and fees can be based on the number of locations.

Justification: *Registration for every location is a tedious process especially when there is interconnectivity between locations, also dealing with multiple DOT offices is complex due to difference of opinion/understanding and working style among different DOT / TERM Cell official. The Companies Act 2013 has dispensed away the requirement of use of the seal of the company for attestation of agreements and applications.*

Q5: Do you agree with the fee of Rs. 1000/- for registration of each OSP center. If not, please suggest suitable fee with justification.

Yes. Provisions related to fee of Rs.1,000/- is fine for single registration. For multiple OSP centre registrations there should be a consolidate fee of Rs.5,000/- and one single Bank Guarantee for the whole registration.

Q6: Do you agree with the existing procedure of OSP registration for single/ multiple OSP centres? If not, please suggest suitable changes with justification.

Offline process of submission of documents for registration should be abolished. There should be more clarity on OSP registration as far as locations are covered, to include the common infra in a campus. After introduction of Saral Sanchar Portal registration has become much easier. The Application Form should have placeholder for declaration of proposal to start multiple OSP Centres. At the time of filing first application, a complete set of documents are filed, then subsequent registrations should be automatic in nature. A self declaration should be submitted along with application for there is no change in old submissions. Declaration about the bandwidth may also be included in the Annual Return.

Q7: Do you agree with the existing provisions of determination of dormant OSPs and cancellation of their registration? If not, please suggest suitable changes with justification.

Yes. The existing provisions related to Dormant status of the OSP and its cancellation seems to be reasonable. Date for submission of the Annual Return should be extended to November of every year instead of September because the Companies need to provide income and profit & loss details of the OSP activities in the Annual Return and such information has been approved by the shareholders of the company in the Annual General Meeting after audit. Filing of Annual Return should also be enabled in Online registration portal and verification of the return should be by digital signature.

Justification: *As per the Companies Act, the companies are required to hold their AGM by 30th September i.e. 6 months after the closure of Financial Year.*

Q8. Do you agree with the terms and conditions related to network diagram and network resources in the OSP guidelines? If not, please suggest suitable changes with justification.

Yes. Clarity should be provided on what is expected in terms of logical separation of Telecom resources and interconnection of Domestic / International OSP. Look at removing this as it is not clear what is the intent as well, and how it is to be complied to. Mixing of traffic of OSP/non-OSP resource has to be identified for the purpose. The rapid change in the mode of communication demands for revising rules to make them forward looking and make the rules enabling for adoption of new technologies. Accordingly, the requirement of logical separation of PSTN and IP network should be discontinued. The requirement of logical separation of OSP and non-OSP activities should also be removed. The OSP guidelines need to acknowledge the operating models of the corporate, an element of trust should be reposed in corporates and the OSP guidelines should be enablers in overall economic growth of economy. In OSP guidelines a separate scenario should be mentioned where in OSP's international client is willing to extend their managed telecom backbone to OSP location in India. The guideline should clearly depict that any telecom services delivered at OSP should be invoiced to OSP locally by the Indian entity of Authorized Telecom Service Providers. There shouldn't be restriction of traffic between OSP center located in DoT LSA unit within the same geographical jurisdiction.

Justification: *It is not practical to immediately notify the changes in the network diagram because its attestation is dependent upon TSPs.*

Q9. Do you agree with the provisions of internet connectivity to OSP mentioned in the OSP guidelines? If not, please suggest suitable changes with justification.

If the intent of this requirement is for traceability, then this should be to mandate the Company to put in appropriate measures to trace back any internet access to the

source, and do away with the original requirement. As resources are taken from authorized service providers only, need for OSP submitting details of connectivity is necessary. There shouldn't be restriction of traffic between OSP center located in DoT LSA unit within the same geographical jurisdiction.

The existing requirement of separate internet connectivity for every individual locations should be removed. Implementing separate internet stack for each location prevents the small companies, start-ups and companies having small operations in various cities to expand their operations. One common internet connectivity for use by the same group companies should be sufficient. Therefore, the OSPs should be allowed to provide / receive access to their centralized internet stack for its other offices / group companies. To ensure compliance with security requirements (traceability), the companies should have systems in place to track all the users, machines, equipment etc. and their locations connected to its internet stack.

***Justification:** Same as given in para no. 2.*

Q10. Do you agree with the provisions related to Hot Sites for disaster management mentioned in the OSP guidelines? If not, please suggest suitable changes with justification.

This clause should be removed, and the company should be allowed to operate from a Hot Site on demand without any notification. The bona fide use of the central PBX etc. is already reviewed at the time of applying for registration. Also the registration requirements itself need to be reviewed. For clarity on use of the Hot Site, the definition of 'disaster' which can include few events under which the OSPs can operate from other facilities / premises (owned, of group company or a third service provider) for a pre-defined period of during the disaster.

***Justification:** The existing provisions related to 'hot-site' for disaster recovery and business continuity are not aligned to actual business needs and also not commercially*

viaible. Setting up of a dedicated Hot Site with stand-by connectivity along with complete IT infrastructure for use during a disaster requires a huge investment. Which, under the current regime cannot be used for any purpose except in case of a disaster. There are many OSPs which operate from SEZ locations. Under the SEZ rules the companies are allowed to share infrastructure with other SEZ units of the same company or act as disaster recovery sites in case of a disaster event. The OSPs should be allowed to use its other offices (including OSPs / SEZ units) as 'Hot Site' / 'back-up sites'. For clarity on use of the Hot Site, the definition of 'disaster' which can include few events under which the OSPs can operate from other facilities / premises (owned, of group company or a third service provider) for a pre-defined period during the disaster.

Q11. Do you agree with the provisions of logical separation of PSTN and PLMN network resources with that of leased line/ VPN resources for domestic OSP mentioned in the OSP guidelines? If not, please suggest suitable changes with justification.

Logical separation is no longer relevant with access to cheap data and voice connectivity in the country. Considering the current commercial arrangement for the telecom services (low cost for NLD /ILD calls) with options to avail customized plans, logical separation of PSTN and IP network seems to be no longer relevant. Telecom companies are also providing their basic (voice and data) over VoIP network under unified license regime. The requirement for logical separation of PSTN and VPN resources should be removed to keep pace with and to use full potential of technological advancement in the field of telecommunication. OSP should maintain records separately but no need to notify the same. At the time of emergency OSPs must use cloud, data or voice and maintain records. TSPs are more coming on data and no logical portioning is required.

Q12. Do you agree with the provisions of PSTN connectivity/ interconnection of International OSP mentioned in the OSP guidelines? If not, please suggest suitable changes with justification.

This provision should continue. Domestic PSTN should be allowed international operations also. However only Stand Alone connectivity for operations. PSTN should be permitted at the International OSP for OSP activities. Interconnection of OSPs of the same company should not require any specific approval. The interconnection of other OSPs of the same company / group company should be approved without the requirement of submission of same set of documents.

Justification: Presently the Bank Guarantee and logging requirements make the setup cost unviable and hinder the Tier-2/3 cities for BPO operations limiting employment opportunity for such locations. With the emerging cloud-based telephony solutions, present norms hinder the usage of such cloud-based solutions as they could easily use app-based voice calls using data thereby reducing telecom costs.

Q13. Please provide your views as to how the compliance of terms and conditions may be ensured including security compliance in case the OSP centre and other resources (data centre, PABX, telecom resources) of OSP are at different locations.

Physical proximity to inspect such resources is no longer necessary in today's environment. Regardless of the location, access to call logs, configuration, remote login for making test calls etc. can all be provisioned for inspection remotely. With latest advanced technology, such solutions are cost effective and ready to use. Providers of such services are accountable for any breach in security and OSP should be liable for providing the data as per request from DOT as and when requested. With the advancement of technology, physical access to the resources / infrastructure seems obsolete. The DoT's online registration portal and application form should be amended to include specific questions on actual location of the

resources; declaration / undertaking by the OSP to provide virtual access to the resources and related records.

Justification: *The existing technology provides for virtual access to the resources located outside the OSP premises / at any other data centre or cloud (within / outside India). This can further be verified from the existing configuration, system logs, call tests and the CDRs.*

Q14. Please provide your views whether extended OSP of existing registered OSP may be allowed without any additional telecom resource. If yes, then what should be the geographical limitation for the extended OSP centre; same building/ same campus/ same city?

Yes. The extended OSP of an existing registered OSP should be allowed without any additional telecom resource within same building/campus/city. In current environment, most companies will have PBX / servers situated centrally in their data centres. The OSPs would typically have only the Media Gateways at their locations, without any additional telecom resources. OSPs should be permitted to setup extended OSP anywhere in India (or at-least within the jurisdiction of the same TERM Cell where the company has its existing OSP). The application form can have questions like if any of the existing or the proposed OSP will act as primary OSP Centre for the company; location of infrastructure / resources; undertaking from the company to provide virtual access to the core infrastructure / resources from any of the extended OSP centers. Considering the OSP in the same city falls under the same LSA and telecom circle so there is no toll bypass if the telecom resources are shared. Therefore, the geographical limitation should at least be the same city and ideally the limit should be national boundary.

Justification: *The company may be required to set-up additional OSPs due to implementation of business continuity / disaster recovery planning for the company or*

expansion of its operations. The ability of OSPs to provide remote access to the EPBAX and other call details would meet inspection and security requirements.

Q15. Please provide your views as to how the compliance of terms and conditions may be ensured including security compliance in case of the extended OSP centre.

If the centers are in the same city, the PSTN circle stays the same and the interests of the TSPs aren't compromised and doesn't seem to be any security threat in such scenario. The security requirements can be complied with by having virtual access to OSPs infrastructure. Since the infrastructure remains shared between an OSP and its extended arm and telecom resources of an OSP centre can only be taken from authorized telecom service providers so the compliance of terms and conditions, including security compliance, does not put additional overhead.

***Justification:** As mentioned above with ability to provide virtual / remote access to the infrastructure, call and login records, the requirement of physical access seems to be irrelevant and could result in increase in infrastructure cost for the companies.*

Q16. Do you agree with the provisions of general conditions for sharing of infrastructure between International OSP and Domestic OSP mentioned in the OSP guidelines? If not, please suggest suitable changes with justification.

The companies should be permitted to share infrastructure for their Domestic, International OSP operations and other office use without additional approvals and/or Bank Guarantee. By self-governance, the TSPs and the companies can ensure compliance with the security requirements. As part of application process, a declaration and undertaking from the companies to ensure monitoring of both Domestic and International traffic be added and separation of voice and data traffic should be removed. The data traffic flow is between domestic and international OSPs and should not have any restrictions on domestic and international data.

Justification: Present requirement for submission of Bank Guarantee make the setup cost unviable for small companies and also affect growth of ITeS sector. This should be aligned with Government of India's initiative of 'ease of doing business' for promoting more business and investment.

Q17. Do you agree with the provisions of Technical Conditions under option -1 & 2 for sharing of infrastructure between International OSP and Domestic OSP mentioned in the OSP guidelines? If not, please suggest suitable changes with justification.

Option I is ok. For Option II Bank Guarantee should be reduced to OSP level. Bank Guarantee should be reduced to 10 lakh only. Having separate infrastructure for both Domestic and International operations is not commercially viable. The companies (spl. GICs) having both domestic and international operations should be allowed to use a common infrastructure. The existing rules should also be changed in case of the companies having multiple OSPs, extended OSPs; use of cloud based EPBAXs; and GICs providing services to its other offices / group companies.

Justification: Same as above.

Q18. In case of distributed network of OSP, please comment about the geographical limit i.e. city, LSA, country, if any, should be imposed. In case, no geographical limit is imposed, the provisions required to be ensure compliance of security conditions and avoid infringement to scope of authorized TSPs.

No limit for country level. Given the technological advancements, the distributed network of OSP should not be subject to any geographical restrictions. Technology is best used to its fullest potential. For access to the records / CDRs their ability to provide remote access, copy and share such details should be sufficient as their compliance with the security requirements.

Justification: *Remote access to the infrastructure can be provided to TSPs and DoT at the time of inspection.*

Q19. Do you agree with the provisions including of logical partitioning mentioned in the OSP guidelines for distributed architecture of EPABX? If not, please suggest suitable changes with justification.

There should be no restriction on data. Should continue the portioning for Domestic and International at EPPBX alone. We suggest easing off or removal of logical partitioning as mentioned in OSP guidelines. The existing terms are no more relevant as it only creates barrier in providing better and newer services more effectively. These restrictions are also one of the reasons for BPO companies to move to such countries which provide for unrestricted use of the telecom resources.

Justification: *As mentioned earlier with the change in Indian telecom industry the call rates have become very nominal - one of the best economical rates in the world, the voice quality is better on IP based solution as compared to PS TN network.*

Q20. Do you agree with the monitoring provisions of mentioned in the OSP guidelines for distributed architecture of EPABX? If not, please suggest suitable changes with justification.

Suggest easing off or having pragmatic monitoring conditions by providing remote access. Instead of physical inspection at EPBAX locations, inspection at any OSP centre, the OSP should undertake to provide information such as CDRs and relevant information required for inspection / audit - remote / virtual access to the EPBAX and other call details should meet the monitoring requirements.

Justification: *With the advancement of technology, physical access to the resources / infrastructure seems obsolete. The existing technology provides for virtual access to the resources located outside the OSP premises / at any other data centre or cloud (within / outside India).*

Q21. Please comment on the scope of services under CCSP/HCCSP, checks required / conditions imposed on the CCSP/ HCCSP including regulating under any license/ registration so that the full potential of the technology available could be exploited for both domestic and international OSP, and there is no infringement of the scope of services of authorized TSPs.

The rules should be aligned to the prevailing market conditions, preferred using of cloud than setting up of owned infrastructure, remote access to the infrastructure and preferred use of mobile technologies / applications. There should not be any undue restriction on the scope of services under CCSP/HCCSP, especially since they do not infringe on the scope of TSP services. Should register under OSP registration and also comply terms and conditions under OSP Guidelines.

Justification: The suggested changes will reduce the cost of setting up infrastructure, maintenance, provide flexibility in adopting new technology by the companies.

Q22. Please provide your comments on monitoring of compliance in case interconnection of data and voice path is allowed for domestic operations.

The compliance can be monitored with the help of call flow, call tests, maintaining CDR and system logs. Interconnection of data and voice must be permitted at the discretion of TSPs. It should be modified keeping in to account the new guidelines to be circulated.

Justification: *The distinction between data and voice has already been faded with new technology and preferred use of VoIP based technologies.*

Q23. Do you agree with the provisions for use of CUG for internal communications of OSP as mentioned in the OSP guidelines? If not, please suggest suitable changes with justification.

We suggest easing of provisions related to CUG. Flexibility for using CUG/PSTN should be allowed, interconnection within the country and communications through other means also allowed. Voice or IP should be terminated at EPABX. The companies should be permitted to implement CUG facility for communication between its' and group companies' offices in India and outside India without any specific approval process and BG requirements. The latest technology allows the companies to have voice and data connectivity among its and group companies' offices over P2P circuits / MPLS network. The OSPs may be permitted to use mobile technology for communication with its other offices, group companies CUG and their internal communication, provided they are able to maintain and provide the call records and CDRs, such traffic is only carried on public and private IP.

***Justification:** The quality of voice and video connectivity on private circuit is better as compared to the public network. With the disruption in the telecom industry the calling facility is generally provided free of cost by the TSPs for both mobile and fixed line customers. The TSPs interests are also protected with the increase in demand for high speed internet / private leased line services.*

Q24. Do you agree with the monitoring provisions for use of CUG for internal communications of OSP mentioned in the OSP guidelines? If not, please suggest suitable changes with justification.

Yes. But the players must have full flexibility to deploy CUG and to share infrastructure. Communication between the group companies / GICs, separation of IP and PSTN network; and ability of the companies to provide remote access to the resources be mutually exclusive for the overall benefit of BPO sector.

Q25. Do you agree with the provisions of 'Work from Home' mentioned in the OSP guidelines? If not, please suggest suitable changes with justification.

The rules related to Work From Home (WFH) should be liberalized without the requirement of a service provider VPN, which is not a pragmatic solution and not relevant to Data Application Services. At the same time, it is not at all cost effective. Bank Guarantee is not at all reasonable. Data connectivity to the agents home to the OSP centre position shall have no restrictions. Similarly agents shall connect to PBX and relevant laws shall be only applicable to Data Services only and not to Voice services. WFH provisions should not apply to purely data / internet Application Services (non-voice services) provided by the company (GICs) for their internal captive users. As even the primary references in the guideline and context provided only pertain to the Agents, and Call Centers. In the context of OSP providing Data only/Application Services only i.e. non-voice process, remote connectivity to the company's own infrastructure will traverse via., the company's own remote access infrastructure only, after successful authentication, with the user be authorized to access the resources they are entitled to. With this model, it is not necessary to have a point to point connectivity between the users' home and the OSP Centre, and this requirement should be removed. The OSP guidelines on WFH also need to be aligned with changes brought in by the recent changes to the SEZ rules. Under the current SEZ rules, SEZ units with IT & ITeS operations are allowed to implement WFH policy but for the companies having OSP registration they still need to follow OSP guidelines. The OSPs operating from SEZ locations should be permitted to avail WFH facility without any additional approval and Bank Guarantee. With the technology advancement and extensive use of mobiles and mobile based applications, the existing WFH guidelines seem to be obsolete.

The OSPs with call centers can allow their employees involved in calling activities by use of such mobile applications which allows them to maintain system logs, CDRs at the host location.

Justification: *The WFH policy could be a win-win situation for the companies, its employees and customers. It will also boost employment and economy. WFH can be used for expansion of operations by the OSPs and encourage other companies to start new ventures. By use of mobile devices like laptops and mobile phones, the employees working in IT and ITeS sector can get flexibility of working from home / office without any specific time limitations and also provide better customer support services.*

The OSP guidelines on WFH also need to be aligned with changes brought in by the recent changes to the SEZ rules. The OSPs operating from SEZ locations should be permitted to avail WFH facility without any additional approval and Band Guarantee. With the technology advancement and extensive use of mobiles and mobile based applications, the existing WFH guidelines seem to be obsolete.

Maternity Benefit (Amendment) Act, 2017 also permits the employers to provide work from home facility to women staff after completion of their maternity leave.

Q26. Whether domestic operations by International OSPs for serving their customers in India may be allowed? If yes, please suggest suitable terms and conditions to ensure that the scope of authorized TSP is not infringed and security requirements are met.

This should be allowed. Domestic operations by International OSPs for serving their customers in India may be allowed with logical partitioning Option 2 (but without submission of additional Bank Guarantees), unless it compromises the security requirements. Indian TSP/ISP resources will be used for connectivity.

Justification: *Currently, the TERM Cells ask the companies to seek Domestic OSP registration if they support any of their Client's Indian operations / customers. Further, the clients of the OSPs require them to host infrastructure / data at one of their selected data centres / cloud in India as part of their business continuity strategy. And, the same is seen as domestic OSP operation. This unnecessarily adds complication, increase infrastructure and compliance costs for the companies. If the*

companies are able meet the security requirements then they should be permitted to provide services to their clients' other offices / operations in India.

Q27. Whether use of EPABX at foreign location in case of International OSPs may be allowed? If yes, please suggest suitable terms and conditions to ensure that the scope of authorized TSP is not infringed and security requirements are met.

If it is owned by OSP own PBX, it may be allowed. If OSPs was owned by foreign agency they require security and related CDRs and other system logs should be provided. Client should provide CDRs, the resource used for carrying such traffic are to be from authorized TSPs so the security aspect is taken care of. There should be an undertaking from customer and to provide CDRs should be the responsibility of Agent. Further the OSPs may give undertaking to provide virtual access to the EPBAX. OSPs should undertake and provide virtual /remote access to the EPBAX and CDRs upon request from the DoT.

Justification: *Having a EPABX at foreign location also eliminates the possibility of merger of PSTN and IP traffic, domestic and international operations and toll bypass. This automatically ensures that the scope of authorized TSP is not infringed. The resource used for carrying such traffic are to be from authorized TSPs so that the security aspect is taken care of. Further the OSPs may give undertaking to provide virtual access to the EPBAX and CDRs to DoT required for inspection and audit by the TSPs. OSPs should undertake to provide virtual /remote access to the EPBAX and CDRs upon request from the DoT.*

Q28. Do you agree with the Security Conditions mentioned in the Chapter V of the OSP guidelines? If not, please suggest suitable changes with justification.

Yes. Guidelines should be defined to provide virtual access to call records. In case of usage of the EPABX at foreign location, physical access may not be possible and in

such a case, virtual access of the system/equipment should suffice for inspection requirements. Protection should be included in the OSP terms and conditions in infrastructure facilities by unauthorized searches by enforcement agencies. Powers of the TERM cell should be streamlined with adequate safeguards.

Justification: *IT companies prefer to use latest technologies and the new equipment allows the users to have remote access and control. Therefore, the requirement of physical access to the infrastructure seems to be irrelevant. OSPs primary obligation of their ability to provide the required CRDs, system logs and the same can be provided with remote / virtual access.*

Q29. Do you agree with the provisions of penalty mentioned in the OSP guidelines? If not, please suggest suitable changes with justification.

Rules relating to penalties should be liberalized, if cannot removed in entirety.

Q30. Whether OSP to OSP interconnectivity (not belonging to same company/ LLP/ group of companies) providing similar services should be allowed? If yes, should it be allowed between domestic OSPs only or between international and domestic OSPs also.

OSP to OSP connectivity interconnectivity should be allowed in all cases. No prior approval for inter connectivity with other OSP / offices of the same company and group companies be required unless it compromises security. OSPs should also be permitted to have connectivity with other OSPs as this will help the companies to enter in IT & ITeS business and enable existing OSPs in expanding their operations.

Justification: *OSP to OSP connectivity will be helping in collaboration of the companies. Like shared cloud environment, there could be segregation of the traffic for the OSPs connected to one infrastructure. In a highly globalized environment where geographical boundaries are blurring, it is but necessary that the regulatory*

framework be an enabler. This will foster a mature commercial environment in India which will result in better contribution to national economy.

Q31. In case OSP interconnectivity is allowed, what safeguards should be provisioned to prevent infringement upon the scope of licensed TSPs.

TSPs and OSPs should be free to negotiate interconnectivity terms, if they adopt terms and conditions of OSP guidelines.

Q32. Do you agree with the miscellaneous provisions mentioned in the Chapter VI of the OSP guidelines? If not, please suggest suitable changes with justification.

With the change in the telecom service domain, availability of telecom services at nominal charges, general use of the mobile applications etc. the concern related to infringement of the scope of TSPs seems to be irrelevant. Ability to provide virtual / remote access to the telecom infrastructure (EPBAX), CDRs, system logs should fulfil the security requirements.

Justification: *With new technologies (virtual access, growth of cloud services) and requirement for having business continuity planning, the dependency upon one location for hosting of the infrastructure is getting obsolete. Today before starting a new business, the companies (specially MNCs) try to seek clarity on compliance obligations and evaluate risk. More the compliance obligations could trigger greater risk for the companies and affect their decision making for business expansion.*

Q32. Do you agree with the miscellaneous provisions mentioned in the Chapter IV of the OSP guidelines? If not, please suggest suitable changes with justification.

No Comments

Q33. What provisions in the terms and conditions of OSP registration may be made to ensure OSPs to adhere to the provisions of the TCCCPR, 2018.

No comments.

Q34. Stakeholders may also provide their comments on any other issue relevant to the present consultation.

To simplify infrastructure requirements, the OSPs should be allowed to have centralized PSTN architecture where in users located across India sites can use the PSTN connectivity from the centrally located trunks in the data center. Doing this would help reduce gateway footprint in branch offices and effectively utilize the media resources in the DC.

Merger and Acquisition - The online registration portal does not allow transfer of the OSP registration from one entity to another entity pursuant to amalgamation /acquisition / de-merger. The online registration portal should allow the companies to submit request for transfer of the registration in case of mergers / acquisition / de-mergers. The administrators in the respective TERM Cells should be allowed to modify the CIN number and name of the company off-line to give effect to the transfer of the OSP registration. Existing OSP registration process requires the companies to obtain new registration and surrender the registration in the name of the merged entity.

Application Form - Only the online application form should be sufficient for submission for OSP Registration. The existing physical application form is a detailed one, as compared to the online registration form but with the changes in the online application form the gaps between physical and online registration forms can be eliminated. In the online application more details pertaining to other offices in India which will leverage IT and Telecom infrastructure of the OSP; connectivity with

EPBAX at foreign end, Work From Home, CUG, details of Indian offices which will be served by the International OSP etc. may please be added.

Category of business activity of the Company - OSPs should be allowed to submit their applications under multiple categories. Character limits for Online application form should be increased.

Bandwidth calculation - The online registration portal does not provide accurate total of previous and revised bandwidth.

Cloud infrastructure / EPBAX location - The existing rules and the list of issues under this consultation paper are silent on use of cloud services as Client's PoP location (except Cloud based EPBAX). With the change in technology and cost pressure, the companies prefer to use Cloud based infrastructure than putting in place their own Data Centre and other hosting infrastructure. As part of revised OSP guidelines, add appropriate details and clarifications for enabling the companies to use cloud-based infrastructure / PoP.

Encryption - Encryption of the data is also relevant to the use of cloud infrastructure. For protection of the data, the companies need to encrypt their data to highest possible levels. Encryption at high level reduces the risk of unauthorised access or hacking of systems. The existing encryption levels do not provide adequate protection to the companies against cyber-attacks. Request the revised OSP guidelines may also add rules related to higher encryption levels.

Customer Provided Links - OSP's (i.e. Outsourcing services providers) should be allowed to use customer ordered/ procured telecom links for provision of services to be provided by the OSPs to such customers. Such customer sponsored / procured telecom links would still be sourced from the licensed TSPs.

Justification: *The guidelines should be forward looking, enable preferred location for MNCs to make investment in India, enable further growth of IT and ITeS business in India and take into account various business scenarios.*

We request to incorporate OSPAI’s views on subjects mentioned in the Consultation Paper. The OSP Guidelines should be simplified and combined to the extent possible to economize by identifying the bottlenecks, hindrances that are making it difficult to do business in India by regulatory bodies. We are hereby submitting Other Service Providers Association of India “OSPAI” comments .

OSPAI