BIF

BROADBAND INDIA FORUM

"Think Tank for Digital Transformation"

REVISED BIF RESPONSE TO TRAI CONSULTATION PAPER ON REVIEW OF T & Cs FOR REGISTRATION OF OSPs

We set out below our responses to certain questions raised by the Telecom Regulatory Authority of India ("**TRAI**") in its consultation paper dated 29 March 2019 on the review of terms and conditions for registration of other service providers (the "**CP**").

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.**

BIF Response:

We wish to stress at the outset, that the definition of "Application Service" in context of Other Service Providers ("**OSP**") should be in line with the main objective of the present OSP registration viz.

(i) To keep statistical information about such companies;

(ii) ensuring that activities of OSPs do not infringe upon the jurisdiction of others access providers and

(iii) providing special dispensation to boost the BPO sector.

(iv) To prevent grey ILD connectivity by call centres and other entities that purchase telecom resources

(a) . Any extension of the OSP definition to include other services based on data/internet is irrelevant to the original objective. Also, the inability to define application services unambiguously- which the CP recognises - will hamper effective compliance. This will curtail innovation and efficiencies that will ultimately hurt consumers and the economy.

(b) The reference to the word "Application" is itself misplaced. OSPs do not provide any so called 'Application' service. Instead, the OSP guidelines were conceived to cater to the companies into the outsourcing business (primarily voice calling – inbound and outbound). **There is no concept of any application being provided**. The definition of OSP under the guidelines dated August 5, 2008 of "Application Service" which itself is indicative and not exhaustive also does not mention any service which is an application. **So mere reference to application itself needs to be removed and replaced with the word outsourcing.** **Services which are purely based on data / internet/VPN/IPLC should not be covered under OSP activities.** Also captive in house centralized services provided by a company to its parent, group, affiliate should also be excluded.

The current definition is not exhaustive and is indicative. Further, in its current form, the definition is too broad-based – by use of the words like IT/ITES would imply any IT enabled service to be part of OSP which should not be the intent.. For example it includes IT/ITES services which means everything in the IT domain has the potential to become an OSP which is not serving any purpose. **Therefore first the word application needs to be replaced with outsourcing, secondly only voice based calling services should be included in the definition, voice calling can be through PSTN and / or emerging collaboration tools like skype, lync, etc. Captive centres providing such services internal to a company or a group company should be exempted from OSP registration.**

(c) The CP seeks to address the issue of a broad and subjective definition of "Application Services" for the purpose of OSP registration. As presently understood under the Department of Telecommunication's "Revised Terms and Conditions – Other Services Providers" dated 5 August 2008 ("**OSP T&C**"), Application Services include those entities that provide services like tele-banking, tele-medicine, tele-education, tele-trading, e-commerce, call centre, network operation centre and "*other IT Enabled Services*" by using Telecom Resources provided by Authorised Telecom Service Providers. Telecom Resources, in turn, include telecom facilities used by OSPs such as PSTN, PLMN, ISDN, telecom bandwidth etc.

(d) The scope of Application Services is broad and needs to be specific in terms of which activities require an OSP and which do not. The CP itself acknowledges that technology is advancing at a rapid pace and the scope of terms such as "other IT enabled services" has widened to the point where such a definition no longer makes it clear who the target entities would be from the perspective of OSP Registration. In fact, it is highly subjective, and "*prone to different interpretations in the current scenario*" as the CP states.

(e) **One of the questions sought to be addressed by the CP is whether Application Services purely based on data / internet should be considered as OSPs. We submit that it should not.** The objective of providing a separate category of OSPs was elaborated on in the New Telecom Policy, 1999, ("**NTP**") which seeks to protect the jurisdiction of TSPs and to provide dispensation to the BPO sector.[1]

[1] Department of Telecommunications, *New Telecom Policy, 1999* available at http://dot.gov.in/new-telecom-policy-1999.

(f) Our principal concern with the present definition of OSP is that it is overly broad – and as a result it is unclear who needs to be registered under it and for what purposes. Given that the stated aims of the registration requirements is threefold:

(v) statistical information;

(vi) ensuring that activities of OSPs do not infringe upon the jurisdiction of others access providers and

(vii) providing special dispensation to boost the BPO sector.

We recommend rewriting the definition within these parameters, and making it far more specific than it presently is.

(g) We further recommend that a narrowly defined category of services requiring registration under the proposed revised definition should specifically exclude any services that do not pose significant risks in regard to the jurisdiction of telecom service providers, for instance:

(i) Any service based on PC to PC Internet telephony (as defined in TRAI Recommendations on Regulatory framework for Internet Telephony, dated 24th October, 2017), should be excluded, where both parties on a call establish communication by connecting to the internet simultaneously, and the role of the ISP is limited to providing internet access.

The TRAI Recommendations on Application Service Providers dated 14 May 2012 (**"2012 Recommendations"**) considered the possibility of regulating such services (commonly referred to as OTT services) and arrived at the considered conclusion that they should be excluded from the ambit of Application Services, as such services are delivered "*directly by the content / application provider to the user…independently of the user's TSP without the need for carriage negotiations agreement*." At the same time, the definition was left wide enough that such services could be included under the ambit of Application Services in future, if the need arose, and the TRAI presently raises the question of whether services provided purely based on data may be included in the definition of Application Services.

We believe that based on the rationale provided by the TRAI earlier, that such services should continue to be excluded – and further, that the definition should be narrowed so that there is no scope for ambiguities arising in this regard. **Instead of an overarching term "*IT enabled services*" – the definition should categorically include only those services which use telecom resources including managed IP networks involving a carriage negotiations agreement with network providers.**

(ii) There have been several possibly unintended consequences of the use of the term "*IT enabled services*". Numerous services seem to have sought OSP registration on account of the ambiguity in the definition. For example, even though data centers do not fall in the scope of OSP registration, companies which have data centres for captive data storage and processing often seek such registration despite the fact that they do not pose similar risks or give rise to concerns regarding TSP jurisdiction being infringed on. Such entities should also be expressly excluded from the ambit of Application Services. In the alternate, the entity which needs to obtain the registration should be clearly defined in the OSP T&Cs.

(h) **Therefore, we feel that the definition of Application Service needs to revised and narrowed. In particular, we are of the view that the term 'other IT Enabled Services' should be deleted from the definition. This is a broad and vague term that confuses the clear distinction between OSPs and data and internet based platforms that do not seek separate resources from TSPs.**

(i) We do not believe that data based services as distinguished from pure voice based services, should be brought under the purview of registration. Further, the scope of OSP registration should expressly exclude entities that should be treated differently as they do not give rise to similar concerns, such as data centres for captive use vis-a-vis third party use. Any new category/categories that may be created as such, should have the same dispensation as granted by DOT to OSPs which is ostensibly to help promote growth in the sector and not burden this sector with undue additional compliances.

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.**

BIF Response:

As mentioned in our response to Q1 above, we feel that the Registration based framework may kindly be permitted to continue, to help boost growth in this sector. However, as mentioned above, this requirement should be clarified to exclude other data/internet based services from its ambit.

While the OSP guidelines operate on a registration based framework. However, over the years and the level of enforcement and compliances like server localization, bank guarantees, inspection, agreement and more importantly different interpretations have made the guidelines look more onerous like that of a license.

Registration should follow a coding mechanism that refers to the reason or status of the application for registration. Subsequent registration should be made seamless wherein, all the relevant documents that are provided during the registration of the first OSP unless, there is any change to the documents submitted for the registration of the first

OSP. The department may insist on an undertaking which may reiterate that the existing documents are relevant for the current registration as well

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

BIF Response:

Validity should be for telecom licenses and not for registration. These should be perpetual in nature. Other registrations issued by DoT (eg.IP-1) do not come with any validity. Therefore, there should not be any validity for the authorization of OSPs either. They should be allowed to operate till the time they wish to till their registration is cancelled for any non-compliance.

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.**

BIF Response:

As stated above, that despite being categorized as a registration, due to amount of compliances and documents sought, the same has become a license. Given the 3 objectives specified by the Government as stated above, taking OSP registration should not be a liability as against a recognition for being an OSP. Therefore, the amount of documents should be culled down to bare minimum. Any company desirous of getting registered as OSP should simply provide the following documents:

1. Name of the Company
2. CIN Number along with a copy of Certificate of Incorporation
3. Registered office address
4. Address of proposed OSP centre(s)
5. Name of client for whom outsourcing services are proposed to be provided
6. Details of activities proposed to be provided
7. Types of telecom connectivity proposed to be used
8. Undertaking stating that all telecom connectivity will be taken from authorized Indian TSPs .
9. MoA & CoA
10. Certificate of Incorporation
11. List of Directors

The lengthy Form 1 should also be reduced in line with above.

We welcome the launch of saralsanchar.gov.in to streamline OSP registration process. However, the number of documents should be reduced. Data of all companies are maintained at RoC. So by simply asking for CIN, the rest of the data sans network diagram should be available. This will significantly reduce the documentation. Similar to how Aadhar linking with PAN and Bank accounts.

The current procedure is unnecessarily cumbersome and should be simplified. Documentation should be limited to minimum essential without undue financial burden on players. This is especially important, keeping in mind that most players are likely to be small and medium enterprises and should be incentivized to enter and compete in the market.

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

BIF Response:

As a one-time registration fee of Rs. 1000/, the same may be retained.

Currently for each location even within the same city requires separate OSP registration and an additional fee of Rs. 1000 thereof. It is requested that multiple OSP centres within the same city or LSA and belonging to the same organisation be treated as one single OSP .

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

BIF Response:

Now the process of registration has become much more easier with saralsanchar.gov.in. We recommend streamlining the process to avoid duplication and multiple application requirements. Single/Multiple OSPs in a given city/LSA/ or as per the requirements of the OSP company, may be registered with one application. Due to online nature of application filing, once a complete set of requisite documents are filed for the first application. Further registrations should be automatic, if there is no change in status of the applicant, subject to submission of self declaration to that effect**.**

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.**

BIF Response:

If an OSP does not file Annual Return for 3 consecutive years, the OSP may be put in dormant list and the registration cancelled. The current procedure is ok. However, before cancellation due opportunity needs to be provided to the OSP company to justify the reason for default or possible non-compliance.

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.**

BIF Response:

There should not be a need to file network diagram with the concerned LSA. An OSP centre cannot operate without telecom connectivity from a TSP who themselves are mandated under their license to ensure KYC/customer bonafide including periodical inspections. OSPs are also bound by their registration requirements to ensure legitimate use of telecom resources. Since this matter is between TSP and OSP, the requirement of filing network diagram should be dispensed with. Both TSP and OSP need to work together to ensure there is no toll bypass and resources are used in accordance with the regulatory framework. OSPs are not TSPs and neither they can operate independently.

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.**

BIF Response

Current OSP guidelines are very restrictive in terms of permission as it states that Internet Connectivity & any IP addresses for locations outside India shall not be granted. With Mobility being a key requirement for Enterprises the world over, this clause is extremely restrictive and needs to be reviewed. If an IP address is available and fixed, any internet call/communication is possible to be traced these days. Hence there is a need to review and relax the clause accordingly. In any event connectivity even to proxies located outside India for internet at times (even in case of redundancy) will be done through the underlying connectivity provided to OSP by an Indian TSP. Therefore, the clause of having internet connectivity from Indian ISP – IP address should be in the name of Indian entity and address should be done away with.

Also the need to have separate Internet Connectivity for OSP needs to be reviewed, particularly if they are located within the same LSA as internet connection should not be location dependent. There should not be any mandate to have local internet breakout at each OSP location. A ISP having pan India authorization should be permitted to provide internet connectivity under its license from a centralized location to all the OSPs located in the country. Even the OSPs should have this flexibility as against procuring separate internet connectivity at each of its address. There are 34 LSAs – who should not insist on separate internet connectivity. So long as OSP takes internet connectivity from a licensed ISP who has the required authorization to serve in the concerned location, this should be accepted. No local internet gateway requirements are to be mandated for OSPs who take such connectivity from pan India ISPs (Category A).

Since the conditions of ISP license restricts to share the internet connectivity, ISP license should be modified in order to enable closed user group. One primary data connection procured by OSP should be allowed to aggregate to other sites. Aggregating internet bandwidth allows companies to improve their security monitoring and avoids multiple entry points through Internet.

Additionally, from a disaster recovery perspective, if need arises OSPs should be allowed to connect to infrastructure of its parent / group company / affiliate for a limited purpose from a BCP perspective.

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.**

BIF Response

These provisions/guidelines need to be reviewed in today’s context. During disaster management, there must be automatic & seamless switch over to hot sites without any delay of any kind. It is quite possible that a particular business entity may have a domestic OSP & International OSP running, in parallel, catering to different customers and market segments. In case of disaster, they should be allowed to be interconnected so that needlessly additional resources are not wasted for creating standalone hot sites. Also such hot site could be anywhere in the world so long as they belong to the OSP company / group company, this should be permitted to be connected for the purpose of business continuity. Lastly the current requirement of ensuring that a separate registration is required for Hot Sites which should be in ready mode always to take charge is cost prohibitive and needs to be removed. OSP will intimate the LSA as and when setup is switched over to hot sites for business continuity purposes.

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.**

BIF Response

Since, VPNs can be established on IP networks w/o intervention of the TSP, this physical/logical separation /partitioning has little relevance and hence needs to be reviewed.

Technology permits IP (VPN)-PSTN connectivity which has so far not been permitted despite NTP 2012 and now NDCP 2018 suggesting a favourable approach to do so.

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.**

BIF Response

No PSTN Connectivity at Indian end of International OSP is archaic in today's context and needs to be reviewed and liberalised.

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.**

BIF Response

Since the entire traffic of OSP passes through the network of TSP/ISP and there is already an established regulation and practice of LI at TSP/ISP, there is no need for provisioning any additional monitoring of traffic at OSP premises. However, necessary inspection of the OSP traffic at the source by TSP or LEAs should be mandated on providing substantive evidence of violation.

(a) We appreciate concerns about security. However, it must be noted that TSPs who provide the underlying network resources are already subject to security norms. To extend these norms to users of TSP resources adds little to enhance security.

(b) The OSP T&Cs follow security conditions that are arguably archaic in the context of presentday realities governing the services that are registered under this provision. OSPs need to comply to the security as well as other terms and conditions forming part of its registration. It is however not recommended that stringent security conditions and liability thereof to the tune of physical inspection is extended to data centres in remote locations

(c) At the outset, it is our understanding that data centers fall outside the scope of OSP Registration. Presently, there is no clarity around the definition of "data centre" in India. Due to the lack of clarity in the OSP T&Cs, sometimes registration of OSPs for every data centre at every location is obtained, in particular as the Form for OSP Registration Application requires detailing out whether proposed OSP Centre will have data connectivity to any data centre of the client (a separate form is required for each OSP centre).

(d) We submit that the present regulatory framework framework is based on the assumption of physical proximity between the OSP centre and all other elements in the network such as data centres, PABX, etc. However, these services are being provided by the way of more efficient means such as the use of remote CCSPs, virtual call centres, etc. The 'physical' characteristic of OSPs is therefore becoming increasingly less critical.

(e) In light of this, the Security Conditions for OSPs in Clause 3 titled "Security Conditions" under Chapter V, bear reconsideration. These conditions are as follows:

    (i) The OSP shall make available on demand to the person authorized by the Authority, full access to their equipment for technical scrutiny and for inspection, which can be visual inspection or an operational inspection.

    (ii) OSP will ensure that their equipment installations should not become a safety hazard and is not in contravention of any statute, rule or regulation and public policy.

    (iii) The OSP shall be required to provide the call data records of all the specified calls handled by the system at specified periodicity, as and when required by the security agencies.

(f) There are several ambiguities in these conditions which become even more stark in the context of dealing with remote data centres. Physical inspection of all data centres may not be necessary as long as registration requirements contain an obligation of demonstrating the use of facilities as required. The opportunity of equipment becoming a safety hazard is increasingly limited in situations where premises are dispersed. Finally, the requirement of providing call records to security agencies is vague, as the term ‘security agencies’ has not been defined, leaving it open to interpretation. The chapter on “Security Conditions” further states that the OSP shall take necessary measures to prevent objectionable, obscene, unauthorized or any other content, messages or communications infringing copyright, intellectual property etc., in any form, from being carried on the network, consistent with the established laws of the country. It should be noted that TSPs are already subject to requirements under the IT Act in their role as intermediaries, and may be requested to terminate access to services of anyone who transmits certain kinds of unlawful content using their services. The license conditions also provide for lawful interception. In light of this, the additional obligation on OSPs appears to be unnecessary.

(g) The OSP sector regulations have been increasingly liberalised, including the recent “Work from Home” allowances in the regulatory regime. It is recommended that such liberalisation of the sector should continue – with fewer onerous obligations being imposed on critical services such as data centres.

(h) We further note that the security and monitoring obligations under the OSP T&C allow the inspection of OSP Centres upon receipt of any complaint or *suo moto* action by the designated authority. We recommend that provisions in the OSP T&C should not be such that leave the infrastructure facilities utilised in such data centres vulnerable to any unauthorized search and seizure by law enforcement agencies.

(i) India is looking towards rapid expansion of information technology infrastructure and is in need of more data centres in the country. The regulatory environment should incentivise the creation and operation of such facilities. Accordingly, it is our view that imposing additional security and monitoring measures upon data centres may increase the costs of regulatory compliance and discourage businesses from setting up data centres in India.

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?**

BIF Response

Regulation can promote efficiency by allowing flexibility of choice and quantum of resources.

As noted by TRAI in the CP, extended OSP centres are being set up where no new telecom resources are being deployed on account of (i) lack of adequate space at existing location; (ii) business exclusivity; and (iii) efficient utilisation of the existing resources. For the purposes of furthering these reasons and for giving a boost to the activities of OSPs and internet based platforms, we are of the view that extended OSP of existing registered OSP should be allowed, and the same should be governed by the business requirements of the company. Such flexibility will enable the sector to grow organically.

Same building, same campus and same city should be part of extended OSP., since the same come under same LSA and same TSPs. Since the area of TSPs and LSA are defined, any new location in the same LSA should be treated as extension. OSP can at best provide information about the same to LSA and TSP for record keeping.

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.**

BIF Response

We believe that extended OSP centres pose no additional security challenges. As set out in our response to Question No. 13, extended data and OSP centres should be allowed to run efficiently and the costs of regulatory compliance for running such facilities should not hinder their operations. In this connection, we also wish to underline the need to ensure protection of the data handled at such facilities. Please see our response to Q13 and 28 on streamlining of security provisions.

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.**

BIF Response

Sharing of Infrastructure should be permitted as it leads to more efficient & optimal utilisation of resources. However, as mentioned in our earlier response to Q1 above, we recommend that T & Cs should be further liberalized so that players are encouraged to enter the market and are able to operate in a predictable regulatory environment.

Even the duration of agreement should be commensurate with the validity of the OSP registration. The requirement of bank guarantees be reviewed for reduction. One of the key issue is location of the EPABX. This should be allowed to be located any where in the world so long as it is part of OSP network and belong to the same company/group company / affiliate.

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.

BIF Response

Sharing of infrastructure does not go against the objectives of the original OSP framework, as discussed in Q1. We believe that over-regulation is counterproductive. . We must permit optimal sharing of infrastructure in line with the Network architecture of the Contact Centre. This will promote efficiencies and help grow the market.

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.**

BIF Response

We believe that distributed network of OSPs should be left to the architecture proposed by the OSP. Given that most of the distributed processing & switching is happening in the cloud these days, hence imposing geographical restrictions serves no obvious purpose.

One of the main objectives of the OSP registration was to prevent any toll bypass of the TSPs. Nowadays, toll tariffs have come down drastically. Most of the TSPs are offering unlimited NLD calling plans. The restrictive clauses of the guidelines relating to logical partitioning etc flow from these concerns which are no more relevant. The guidelines should be suitably liberalized to encourage this important sector.

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.**

BIF Response

Please see Response to Q18 above.

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.**

BIF Response

Please refer to our Response to Q13 above and 28 below.

In order to enable physical inspection which is otherwise required from a compliance enforcement perspective for which, centralized server configuration can be monitored from OSP centers through console. Hence, physical inspection at the server locations may not be required instead, inspection at OSP centers should provide all the required information such as CDRs and other relevant information required for the inspection.

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.**

BIF Response

We believe that there should not be additional registration requirements imposed on CCSPs – as they have a critical role to play in improving the efficiency of this sector, and should therefore be encouraged. The registration requirements for data centres of OSPs are already onerous and we have recommended streamlining the same in Q. 13 above. To the extent that operational efficiencies are increased by certain cloud service providers, there is no regulatory rationale for increasing compliances on these service providers.

The CP notes that the reason for separately regulating CCSPs would be that they may manipulate underlying networks without the knowledge of OSPs. It is unclear how this can be done without the knowledge of OSP s. In any case, the CP does not appear to have relied on a cogent risk assessment or a case study of such issues arising. We do not believe that this untested hypothesis is sufficient reason to introduce any additional compliances. On the contrary, we recommend further liberalizing the regulatory regime to allow additional flexibilities in technology sought to be deployed. Since this is a form of distributed and shared network architecture which helps in reducing capex & TCO costs, improving network efficiencies etc, such models should be encouraged.

. Please note that authorized TSPs providing internet services already comply and are best placed to deal with specific security obligations. No regulation for such CCSP/HCCSPs is required if the services they offer do not infringe on the domain of

TSPs / do not lead to resale of telecom bandwidth. They should be allowed to provide infrastructure and network services sans telecom connectivity as the latter is domain of licensed TSPs under section 4 of ITA 1885 and highlighted specifically under the DoT's reference.

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

BIF Response

All voice & data circuits are obtained from Licensed TSP/ISPs which are fully compliant to the Lawful Interception Norms. There is no additional burden on this count which is required to be put on a CSP/CCSP/HCCSP if no telecom connectivity or activity is undertaken

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.**

BIF Response

Yes-we agree

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.**

BIF Response

Yes-we agree

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

BIF Response

Keeping in view the popularity of this provision in large cities , given the prevailing traffic situation and the odd hours at which activity is required to be carried out and to enable gender inclusivity, this feature/service should be encouraged.

The guidelines for work to home are very stringent and not practical. Each and every individual in a globally connected environment at times works from home by connecting to their office environment and perform the work. They don't need any work from home registration. Why is it mandatory for OSPs to apply and have separate connectivity for such locations. This is unwarranted and cost wise extremely prohibitive. Therefore OSPs should be permitted to allow their employees to work from home. Any use of office network through VPN client will be governed by internal IT policies including firewall. Having extra regulations on work from home seems to be overkill. That is one of the few reasons why work from home as a concept under OSPs have not progressed.

Keeping the above in perspective, the security deposit of Rs. 1 Cr/per location of the OSP should be reviewed and brought down to bare minimum of say Rs. 10,000. Besides, the Registration of such facility should be granted perpetually. TSPs are best placed to maintain call/activity logs of the extended agent. . Further, the provision of "surprise inspections" appear to be highly onerous and intrusive and should be reconsidered or specific procedural safeguards should be introduced in this regard. Further such centres should just be intimated and be connectivity neutral with no mandate of IP-VPN which is extremely cost prohibitive.

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.**

BIF Response

As correctly captured in the CP itself presently, such companies are advised to register for domestic OSP centres for serving their domestic customers. Domestic OSP registration for such operations necessitates having separate resources. This is expensive and inefficient.

We are of the opinion that domestic operations from International OSPs must be permitted. All inbound/outbound calls (including NLD & ILD calls if switched from local CSPs) should be logged & billed by the Local TSP/ISP.

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.**

BIF Response

In view of liberalisation, business flexibility should be permitted to do international business from anywhere. As long as the International OSP complies to the Basic Guidelines of Transparency and Lawful interception and tie-up with local Licensed TSP/ISP, the same should be permitted and the terms and conditions to be imposed should be monitored through the local TSP / ISP. without additional obligations on OSPs.

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.**

BIF Response:

We do not agree with some of the Security Conditions as we have highlighted in Q. 13. Key points of concern are as follows:

(a) The emphasis on physical inspection of premises and physical safety of equipment may be outdated and need to be revised – especially the provisions that permit arbitrary surprise checks in the context of Work From Home (in Chapter IV).

(b) OSP is required to take necessary measures to prevent objectionable, obscene, unauthorized or any other content, messages or communications infringing copyright, intellectual property etc., in any form, from being carried on the network, consistent with the established laws of the country. This is not an obligation that may be complied with very easily by OSPs as the OSP often has limited control over content transmitted by end users. Even in cases of tele-medicine, tele-entertainment etc. (where content may be in the control of Application Service Providers), much of the management of the services are performed by TSPs. It should be noted that TSPs are already subject to requirements under the IT Act in their role as intermediaries, and may be requested to terminate access to services of anyone who transmits certain kinds of unlawful content using their services. The license conditions also provide for lawful interception. In light of this, the additional obligation on OSPs appears to be unnecessary. It is also to be noted that the Supreme Court dealt with the use of ambiguous terms like “objectionable” etc in the case of Shreya Singhal vs Union of India, and held that such terms can be broadly interpreted go beyond reasonable restrictions to free expression in Article 19 of the Constitution.

(c) We further note that the security and monitoring obligations under the OSP T&C allow the inspection of OSP Centres upon receipt of any complaint or *suo moto* action by the designated authority. We recommend that provisions in the OSP T&C should not be such that leave the infrastructure facilities utilised in such data centres vulnerable to any unauthorized search and seizure by law enforcement agencies.

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

BIF Response:

We are in favour of liberalisation all around including on the penalties clauses as they seem to be too stringent.The penalty should be levied in a objective and proportionate manner.

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.**

BIF Response

Given the fact that there is a lot of infrastructure sharing, hosting of infrastructure in the cloud etc., OSP to OSP interconnectivity should be permitted. It is quite likely that backend infrastructure for the two OSPs which are either cloud hosted or shared may be the same.

Since cloud is seamless and borderless, hence it does not make sense to permit only between two domestic or two international as the same set of infrastructure could be serving multiple OSPs.

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

BIF Response

As long as the compliances are met for the underlying network service provider from whom the resources are being taken, we do not believe any additional onerous requirements should be imposed in this regard. We recommend that any security provisions should be minimally intrusive, decided in consultation with the industry, and further the recent spate of proliferation and growth in this sector. Please see Q. 13 above for streamlining security measures. .

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.**

BIF Response

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.**

BIF Response

It must be incumbent on the OSP to ensure that their platforms are not used to make any communication that falls under the category of UCC. We believe that the provision of registration of "telemarketers" under TCCCPR already adequately addresses this concern and no separate compliances are required.

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

BIF Response: No