Telecom Regulatory Authority of India

Recommendations

on

Review of Terms and Conditions for registration of

Other Service Providers (OSPs)

21st October, 2019

Mahanagar Door Sanchar Bhawan
Jawahar Lal Nehru Marg,
New Delhi- 110 002
Website: www.trai.gov.in

CONTENTS

Chapter –I
Introduction

A- Background

1.1 The Other Service Providers (OSP) Category was introduced for the first time under the New Telecom Policy, 1999 (NTP-1999) framework. The OSPs, such as tele-banking, tele-trading, e-commerce etc were allowed to operate non-telecom services by using infrastructure provided by various authorized access providers. The OSPs are not permitted to infringe on the jurisdiction of authorized Telecom Service Providers (TSPs) and are not authorized to provide switched telephony. No licence fee is charged from OSPs but registration for specific services being offered is required. Department of Telecommunications (DoT) issued detailed terms and conditions for registration under OSP category vide letter dated 05.08.2008. Thereafter, amendments to these terms and conditions have been issued by DoT from time to time.

1.2 In the Unified License Agreement, different annexures (for Access Services, Internet Service and National Long distance service etc.) have been provided wherein the terms and conditions of authorization for specific services have been provided. Specific clauses of these authorizations provide nature of use of certain type of telecom resources which are part of OSP network. These conditions are part of the agreement signed by the Telecom Service Providers who are authorized to provide telecom resources to the OSPs. The Authorised TSPs are permitted to provide resources to the OSP only after examining the network diagram proposed to be setup by the OSP and after ensuring its bonafide use. Both the Authorised TSP and the OSP are responsible, as per the terms and conditions of their license/registration respectively towards any violation of the terms and conditions in the use of telecom resources.

B- DoT Reference

1.3 In view of the vast changes in technology and evolution of different networking architectures and solutions for setting up of OSP network and evolution of new user applications and service delivery scenarios, a need has been felt by DoT to review the terms and conditions for registration of OSPs. DoT vide its letter dated 10th September 2018 has sought the recommendations of TRAI on the terms and conditions for registration of Other Service Providers (OSPs) under Section 11(1)(a) of the TRAI Act, 1997. (Annexure-I). DoT has requested TRAI to review the technical, financial and regulatory requirements, scope of operations and the terms and conditions of registrations of OSPs in a comprehensive and holistic manner. DoT has desired that a technology neutral framework is required to be devised to promote innovations for setting up the OSP service delivery platform in the most cost-efficient manner for faster promotion of OSPs in the country. At the same time, DoT has requested that it is essential to ensure that the security aspects are guarded in national interest and there is no infringement of the scope of the licenses of the TSPs.

1.4 Initially, DoT provided a list of important issues for consultation as annexure to the letter dated 10.09.2018. However, no background information on any of the issues was provided. Subsequently, DoT, vide its letter dated 7th January 2019, provided background information on a few of the issues in response to TRAI letter dated 13.12.2018.

C- Consultation Process

1.5 A Consultation Paper (CP) on 'Review of terms and conditions for registration of Other Service Providers (OSP)' was issued on 29.03.2019 seeking comments from the stakeholders by 29.04.2019 and Counter-comments, if any, by 13.05.2019. On request of some stakeholders, the dates were extended for submission of comments

and counter comments till 20.05.2019 and 03.06.2019 respectively. A total of 34 comments and 4 counter comments were received from stakeholders in response to the Consultation Paper. An Open House Discussion (OHD) was conducted with the stakeholders on 15.07.2019 in New Delhi. Some of the stakeholders have also submitted comments on the CP post OHD.

1.6 After considering all the written submissions of the stakeholders, discussion in the OHD and examining the issues in depth, the Authority has finalized these recommendations.

1.7 A detailed analysis of the issues raised in the consultation paper, along with the response given by the stakeholders, is contained in the second chapter. The responses were widely divergent, the Authority has taken a holistic view of the different facets to arrive at the recommendations. The summary of the recommendations has been provided in the third Chapter.

Chapter II

Analysis of Issues and Recommendations

I. Definition and Registration of Other Service Providers (OSP)

2.1 The guidelines issued by DoT define the Other Service Providers (OSP) as a Company / Limited Liability Partnership (LLP) providing Application Service wherein "Applications Services" means providing services like tele-banking, tele-medicine, tele-education, tele-trading, e-commerce, call centre, network operation center, vehicle tracking systems and other IT Enabled Services by using Telecom Resources provided by authorized telecom service providers.

2.2 It has been noted that while forwarding the reference to TRAI for review of terms and conditions for registration of OSPs, DoT's concerns appear to be focused mainly on two aspects viz. to ensure that the security aspects are guarded in national interest and there is no infringement of the scope of the licenses of the Telecom Service Providers (TSPs).

2.3 On the definition of Application Service and registration of OSPs, divergent views have been received from the stakeholders. Most of the stakeholders have mentioned that the term 'Application Service' and other 'IT enabled service' in the DoT's guidelines are too broad and vague. Some of the stakeholders were of the view that the reference to Application based services needs to be removed and instead be replaced with the word "Outsourcing Services". Few stakeholders opined that the term Application Service may be renamed as 'Business Communication Service' and OSP be named as 'Business Communication Service Provider'. Some of the stakeholders mentioned that the term 'application service' may also be interpreted to include OTT and needs to be clearly defined. One of the stakeholders opined that the OSPs are no different from ordinary

business customers of ISPs and TSPs and hence no need to have a special category for these.

2.4 A large number of stakeholders were of the view that Captive services (providing services to own company or group company) may be kept outside the domain of OSP registration requirement. Further, majority of the stakeholders were of the view that Application Services that are purely based on data/ internet (non-voice) should be specifically excluded from the scope of the OSP.

2.5 With regard to regulatory requirement for OSPs, most of the stakeholders were of the view that the OSP registration should be simplified or a light touch regulatory approach may be adopted. Some of the stakeholders were of the view that the OSP registration should be done away with, while few of the stakeholders were in favor of OSP registration continuation. Few stakeholders were of the view that there is no need for OSP registration and the compliance of DoT objectives could be met indirectly through the concerned TSPs.

2.6 One of the stakeholders was of the opinion that the OSPs may be regulated with licensing through authorisation for application services as defined by TRAI in recommendations on Guidelines for UL/ Class License dated 12th May 2012. Another stakeholder was of the view that entities providing digital services such as social media platforms, content oriented platforms /websites, search engines etc., should not be required to obtain OSP Registration.

Analysis

2.7 The views of stakeholders have been considered in light of the objectives set by DoT. It has been noted that in the present guidelines only the term 'Application Service' has been defined and the term 'OSP' is in a way being used in place of Application Service Provider. Also, the present definition of Application Services includes the term 'other

IT enabled services' which makes its scope wide and leads to subjective interpretation. The Authority is of the opinion that the terms which are too broad and vague in the definition of the existing regime need to be addressed and therefore, the terms 'Application Service' and 'other IT enabled service' may not be used for defining the OSP and scope of business/service under OSP.

2.8 Presently, the types of business activities covered in the user manual for OSP registration are Vehicle Tracking Centre, Billing Service Centre, e-Publishing Centre, Medical Transcript Service, Financial Service, KPO, Tele-Trading, Tele-Medicine, Tele-Education, Network Operating Centre, Others[1]. The Authority is of the opinion that the list of business appears to be adequate as on date, however, with change in technology or nature of services the list of businesses included in the definition may change. Therefore, DoT should update the list from time to time.

2.9 The Authority noted that OSPs have been granted special dispensation to transport the incoming PSTN calls from one location to the other with load sharing to enable them to provide the services in an efficient manner.

2.10 The authority has also noted the views of stakeholders where it has been highlighted that ILD/ NLD network bypass is only possible in case of voice calls and there is no such issue in cases where only data is being used. In addition, the security aspect of monitoring of calls is applicable in case of voice calls only. As far as data traffic/ internet is concerned, the traffic passes through internet gateway and there is appropriate monitoring mechanism to address the security concern.

[1] As per list provided by DoT in the User Manual for Online Registration of Other Service Providers https://www.saralsanchar.gov.in/osprep/user_manual_osp_applicant.pdf

2.11 It has been noted that there are captive OSP centres i.e inhouse service centres providing voice-based or/and data-based services like IT support, Technical Helpdesk, Payroll, Accounting Services etc. to own company, parent or group company, by using telecom resources from authorized TSP. Also, there are captive centres of an entity providing services to their own customers/ users only by using telecom resources from authorized TSP.

2.12 The Authority is of the view that the Other Service Providers should be those service providers who are providing the services on outsourced basis i.e. on behalf of another entity. The provision of services to customers or employees of own company/group company i.e. for captive purposes should be excluded from OSP. The centres providing captive services should be termed as Captive Contact Centres (CCC). The Authority is of the view that the CCC should only furnish intimation to DoT.

2.13 The Authority is of the view that based on the service being offered, the OSP could be categorised as:

(a) Voice based i.e providing voice based services

(b) non-voice based/ data or internet based i.e providing non-voice-based services only.

Further, based on geographical location of their clients/customers, the OSP could be divided into two different categories:

(a) Domestic OSP - providing the services within national boundaries.

(b) International OSP - providing the services beyond national boundaries.

2.14 The Authority is of the view that registration under OSP category may be continued. However, the type of business activities for which registration is required needs to be reviewed and addressed. It should be based on the voice/data as explained in para 2.13 above.

2.15 The OSPs providing voice-based services need to be registered so that necessary information is collected, and concerns could be addressed. As far as the data/ internet based OSPs are concerned, prima facie the concerns related to bypass of PSTN (NLD/ILD) are not there. Hence, registration for such OSP may be exempted. However, to check any possible non-compliance at any stage, intimation requirement could be prescribed.

2.16 In regard to registration of OSP, the Authority noted that in recent past DoT has made the process of registration of OSPs online on the Saral Sanchar portal of DoT (https://saralsanchar.gov.in). Also, the explanation of online application process has been provided in the user manual which explains the registration process with screenshots. It is noted that there are still certain aspects of OSP registration where offline activity is being followed and separate agreement is being signed and hard copies of documents are being obtained.

2.17 The Authority is of the view that to leverage full potential of the technology, the entire process of registration should be made online and all the documents should be uploaded on the website/portal only. Wherever authentication of documents is required, digital signature may be obtained. Further, the Authority is of the view that a time bound registration process may be adopted. For this purpose, one-month time may be fixed by DoT to scrutinise the applications and convey approval or any shortcomings. To ensure efficient disposal of registration cases, the web portal may be made with a provision of auto-generation of registration certificate at the end of one month if no shortcomings are noticed. In case of intimation for data/internet based OSPs the web portal should immediately generate the acknowledgement-cum-registration. Also, for captive contact centres, the intimation acknowledgement should be issued immediately. In case of any system related issues in generating the acknowledgement

immediately, the acknowledgement for intimation may be issued within 48 hours in any case.

2.18 The Authority recommends that the OSP may be defined as below:

Other Service Providers (OSP) is a Company or Limited Liability Partnership (LLP) providing services like Business Process Outsourcing (BPO), Billing Service Centre, e-Publishing Centre, Financial Service, Knowledge Process Outsourcing (KPO), Medical Transcript Service, Network Operating Centre, Tele-Medicine, Tele-Education, Tele-Trading, Vehicle Tracking Centre or Other similar services on outsourced basis i.e. on behalf of another entity using Telecom Resources provided by authorized Telecom Service Providers. The above list of services may be modified by DoT as and when required.

The provision of above-mentioned services by a company/LLP for captive purposes i.e. to their own customers or employees shall be excluded from the scope of OSP. Such entities may be termed as "Captive Contact Centres".

2.19 The Authority, recommends that for the purpose of registration, the OSPs are categorised in following categories:

a) Voice-based OSP

An OSP providing voice-based services (using voice call or voice-based application).

b) Data/Internet based OSP (without voice component)

An OSP providing services which are purely based on data/ internet and no voice connectivity is involved.

The above categorization of OSP will be applicable to both Domestic and International OSP.

2.20 The Authority further recommends that:

(i) The voice based OSPs (Category (a)) above shall be required to register under OSP category and registration certificate shall be issued by DoT after due scrutiny of the application.

(ii) For data/internet based OSP (Category (b)), the registration shall be in the form of intimation under OSP category, where the acknowledgement of intimation shall be treated as registration certificate for OSP. However, OSP shall ensure that their activities do not infringe upon the jurisdiction of authorised TSPs.

(iii) The Captive Contact Centre shall file for intimation on DoT portal. They shall also ensure that their activities do not infringe upon the jurisdiction of authorised TSPs.

(iv) In all above cases, DoT would have the right to inspect and check any violation of terms and conditions of the guidelines.

<u>Process of Registration/ Intimation</u>

(v) The entire process of registration and intimation (data/internet based OSP and captive contact centres) should be completely online and there should not be requirement of submitting any document offline.

(vi) In case of registration of OSP (Category (a)) the DoT should scrutinize the application within one month. In case of any deficiency, the statement of deficiency along with the name of the document to be uploaded shall be generated on the Web portal for registration. Thereafter, the applicant shall take the necessary corrective action and upload the relevant document to the Web Portal. In case there is no deficiency, DoT will approve for generation of registration certificate at the Web portal as early as possible but not later than one month. The Web portal shall have the capability to auto generate the registration certificate at end of one month from the date of application if no deficiency is pointed out.

(vii) In case of intimation in respect of data/internet based OSP and Captive Contact Centres, the acknowledgment of intimation

shall be generated immediately, but in any case not later than 48 hours.

II. Period of validity of Registration

2.21 At present, the registration under OSP category is valid for a period of 20 years from the date of issue, unless otherwise mentioned in the registration letter. A one-time validity extension by 10 years is provisioned, if applied during the 19th year.

2.22 Most of the stakeholders have submitted their views for continuing the present period of validity of registration and extension. Some other stakeholders have stated that the period of extension should also be for 20 years. Some of the stakeholders have mentioned that there should not be any period of validity of registration similar to the registration under IP-1 Category issued by DoT. They have stated that the registration once issued should be valid till the time the OSP wants to continue the business activity.

Analysis

2.23 The Authority is of the opinion that the current provisions of validity of registration of OSP for a period of 20 years from the date of issue of registration may be continued unless a request is made by OSP to register it for a lesser period. Further, the registration period may be extended by 10 years at a time if the OSP applies for the same in the 19th year of the initial registration period or in the 9th year of extended registration period.

2.24 The Authority recommends that:

The registration of OSP shall be initially for a period of 20 years. The same may be extended by a period of 10 years at a time if applied in the 19th year of the initial registration period or in the 9th year of extended registration period.

III. Registration Fee, Documents required and registration of single/ multiple OSP centers

2.25 At present, a processing fee of Rs. 1000/- is charged for Registration of each OSP centre. While most of the stakeholders have agreed with the current fee for registration at Rs. 1000/-, few stakeholders have commented that the fee may be increased. One of the stakeholders has said that the fee may be increased to Rs. 5000/- for single all India entity and another stakeholder has said to increase it in the range of Rs. 10,000/- to 25,000/-.

2.26 Further, at present, each OSP centre is required to be registered separately. In case of multiple OSP centre registration belonging to same company/LLP, the registration for the first OSP centre is issued based on all the documents submitted for first OSP centre. Thereafter, the OSP has to submit only copy of OSP Registration obtained for first site and a copy of certificate of incorporation issued by registrar of companies if such request is made by OSP within one year and there is no change in the status of previously submitted documents. After one year, a complete set of documents are required to be submitted.

2.27 In regard to submission of documents for registration, a large number of stakeholders have stated that the current list of documents is adequate. One of the stakeholders has stated that list of Directors and Shareholding patterns should be removed from the list of the documents. Another stakeholder has said that network diagram and certificate of incorporation document should be sufficient. Some of the stakeholders have stated that DoT should take KYC documents from TSPs and company related compliance documents from Ministry of Corporate Affairs. Few stakeholders have also mentioned that DoT should have a digilocker of the documents and avoid asking same documents for multiple registration. One of the stakeholders has stated that MoA should be done away with. One of the stakeholders

has mentioned that Company incorporation/partnership deed, Network diagram, Legal Power of attorney for signatures officer/digital signatures – only should be asked. One stakeholder has stated that data of all companies are maintained at RoC and by simply asking for CIN, the rest of the data sans network diagram should be available. Another stakeholder has stated that OSPs should be treated like any other customer and no additional documents or Registration required. Some of the stakeholders have agreed with the existing process of registering each OSP centers separately.

2.28 Most of stakeholders have stated that single registration for multiple OSP centre of one company should be there. Some of the stakeholders have opined to have single registration for multiple OSP Centres of one company operating as one unit and for same application service. Few stakeholders have favoured single registration for multiple OSP Centres of one company for each LSA. One of the stakeholders has stated to have single registration for multiple OSP Centres of one company for each City. One stakeholder has opined that multiple OSP centres of same entity within the same campus should require single registration as long as type of their operations are identical. Domestic and international OSP in the same campus to be registered separately.

2.29 One of the stakeholders has stated that for larger players, a grant of registration for huge common clusters may be permitted following the model of the Unified Telecom License in which parties may apply for state wise and country wise license. Another stakeholder has stated that multiple centres for OSP should be restricted.

Analysis

2.30 The Authority is of the view that the list of mandatory documents in the current list appears to be appropriate and may be continued with. Also, in case the actual information is different from earlier submitted

information in the mandatory document, the documents under list B of the existing guideline i.e. list of present directors of company and present share holding pattern of the company, indicating equity details, may be continued to be submitted. Further, considering the present structure of licensed service area, the Authority is of the view that single registration of the multiple OSP centres, belonging to same company/LLP within a LSA, should be adopted. There should be flexibility with the OSP to add additional OSP centres, within LSA, with the existing registration. This could be done by uploading network diagram of the additional OSP centre. The OSP centre of domestic and international types having different telecom resources and client/ customer, needs to be registered separately. In case, multiple OSP centres of any company/LLP are in more than one LSA, separate registration certificate for each LSA may be issued. The mandatory documents should be required to be uploaded one-time in the LSA where the registration is applied first. After the registration certificate is issued in one LSA, only network diagram should be required to be uploaded for registration of OSP centres either in the same LSA or in other LSA(s). The requirement of additional document would only be there if there is change in information submitted earlier.

2.31 With regard to the registration processing fee, the Authority is of the view that the existing fee of Rs. 1000/- per OSP centre should be continued. In case of multiple OSP centres of one company/LLP in an LSA, the processing fee should be Rs. 1000/- per OSP centre.

2.32 The Authority is of the view that the requirement of documents for intimation in case of Captive Contact Centres should be same as OSP. The intimation may be filed separately for each centre with a fee of Rs. 1000/- per centre.

2.33 The Authority, therefore, recommends that:

(i) Multiple OSP centres of the same company/LLP should be registered as a single entity in an LSA. However, domestic and international OSPs shall not be grouped and shall be registered separately.

(ii) A processing fee of Rs. 1000/- be charged for registration of each OSP Centre.

(iii) The existing list of documents for registration may be continued. For registration of multiple OSP centres of same company, one set of documents with separate network diagrams of each centre should be submitted. In case of multiple OSP centres of same company/LLP in different LSAs, registration certificate may be issued separately in each LSA. However, mandatory documents (except network diagram) should be uploaded for initial registration only. The web portal of online registration should have provision to apply for registration of multiple OSP centres. Additionally, provision should be made to add OSP centres with existing registered OSP centre(s) of the same company. To ensure that the other OSP centres are belonging to the same company, the digital signature used should be same while applying for additional OSP centre. In case, the signatory gets changed, the intimation in this respect, duly signed by authorised signatory for this purpose, may be uploaded as additional document and the process of uploading the documents and information may be completed using digital signature of new authorised person.

(iv) The requirement of documents for intimation in case of Captive Contact Centres should be same as OSP. The intimation may be filed separately for each centre with a fee of Rs. 1000/- per centre.

IV. Annual Return

2.34 As per the existing guideline, OSPs are required to submit 'Annual return' to the registration authority in the prescribed Performa within six months of completion of the financial year, indicating the details of the activities of the previous financial year and the status of their continuing the OSP operation. The OSPs furnishing the annual return are put in the Active OSP list of DoT. Those OSPs, who are not submitting the annual return for consecutive three years, are put in the dormant list and their registration is cancelled after keeping them in the dormant list for two years. List of such OSPs is required to be made available on the DoT web site.

2.35 Most of the stakeholders have agreed to the existing provisions. One of the stakeholders has said that the date of submission of annual return should be extended to November from the existing September. Some of the stakeholders have stated that the OSP should not be required to disclose its revenue details as part of annual return. Few of the stakeholders have stated that due opportunity should be provided to OSP before cancelling the registration.

Analysis

2.36 The annual return is an indication of continuity of the active status of the OSP. As DoT does not charge any annual fee depending on the turnover or profit/loss of the OSP, these details do not serve any other specific purpose. Considering the views of the stakeholders, the Authority is of the view that the filing of annual return may be continued. However, the details of annual turnover and net profit/loss may be made optional data in the Performa for filing of the annual return. It would also be appropriate if an email intimation is sent to OSP, auto generated from the portal, before the filing of return is due, before the OSP is likely to be put under dormant list and before cancellation of the registration. These emails can serve as reminders

to the OSPs for filing of annual return or taking appropriate action to avoid from being declared as dormant OSP/ cancellation of registration. Further, auto generated emails may also be sent as acknowledgement to the filing of annual return by OSP. The software provisions for sending such auto generated emails can be incorporated in the web portal. Further, the Authority is of the view that the Captive Contact Centres should also furnish the annual return in the format prescribed for OSPs. However, other provisions of dormant declaration and cancellation of registration would not be applicable for CCC.

2.37 The Authority recommends that the existing provisions related to submission of annual return may be continued. The details of annual turnover and net profit/loss may be made optional data in the Performa for filing of the annual return. Auto generated email acknowledgement of annual return submitted by OSP may be sent to OSP. Auto-generated email should also be sent to OSPs as a reminder for submission of annual return, before putting them in dormant list or cancellation of registration.

Every Captive Contact Centre should also furnish the Annual Return.

V. Network Diagram

2.38 As per the present guidelines, the Authorised TSPs are required to provide resources to the OSP after examining the network diagram of the network proposed to be setup by the OSP and after ensuring its bonafide use. OSP is required to submit a copy of the network diagram approved by the TSP to DoT field units for records and verification.

2.39 The stakeholders have given divergent views regarding the requirements related to network diagram which is required to be submitted by the OSP at the time of registration. Many stakeholders

have agreed with the existing provisions while many have suggested that there should not be any requirement of network diagram. Many of the stakeholders have stated that the network diagram should not be approved by the TSP and should be either self-attested or approved by DoT. One of the stakeholders has stated that network diagram should be required to be submitted within three months of registration and should have information related to connectivity with TSP. Few of the stakeholders have stated that DoT should have no concern and network diagram should be a matter between TSP and OSP.

Analysis

2.40 It has been noted that the network diagram is one of the most critical requirements in the current regime and timely issue of registration certificate depends on the network diagram. It is noted that in the current regime, the depth of the details of the elements in the network diagram has not been outlined and this leads to subjective interpretation by all the stakeholders i.e. OSP, TSP and DoT. Therefore, there is need to define the components in the networks diagram.

2.41 The Authority is of the view that the network diagram should have complete details of connectivity of telecom resources showing the entry point of the telecom resources and the connectivity with different network elements (EPABX, Internet, Leased line, MPLS, VPN, Data centre/Server). Further, the Authority is of the view that the OSP should be free to choose any technical solution available for the connectivity which is being offered by the authorised TSPs provided that the terms and conditions of registration are met and there is no infringement to the scope of authorised TSPs. The proposed network diagram should have the details of:

(i) Name of Service provider proposed to provide telecom resources

(ii) Bandwidth and the type of connectivity (PRI, Internet, VoIP, MPLS, IPLC, etc.)

(iii) Details of EPBAX and its configuration (standalone/ distributed architecture/ cloud EPABX, location of EPABX).

(iv) Details of infrastructure shared if any, including CUG facility.

(v) Location of Data Centre of the client of OSP for whom the services are being provided by OSP

2.42 As far as the domestic OSP is concerned, the telecom resources obtained from authorised TSP has all its components within the Country. In case of International OSP, the telecom resources from authorised TSP will have International connectivity and therefore some of the components of OSP network will lie in foreign land. Further, as far as the provisions of the license condition regarding verifying the bonafide use of telecom resources provided, the TSPs and OSPs are equally responsible. Accordingly, the TSP should, at the time of providing the resources to the OSP, ensure that the proposed network does not infringe into the scope of authorised TSPs. To ensure the same, the TSP may inspect the OSP centre. The Authority is of the view that, for registration under Domestic OSP, self-attested network diagram should be required and for registration under International OSP, network diagram duly certified by TSP should be required. In case of any non-compliance noticed by DoT in the network diagram at the time of application for OSP registration, DoT should suggest necessary changes, wherever required, to the OSP to make the network compliant. CCC should also furnish self-attested network diagram at the time of intimation and any change in the network diagram may be intimated to DoT through the web portal immediately.

2.43 Therefore, the Authority recommends that:

(a) The proposed network diagram should have following details:

(i) Name of Service provider proposed to provide telecom resources

(ii) Bandwidth and the type of connectivity (PRI, Internet, VoIP, MPLS, IPLC, etc.)

(iii) Details of EPBAX and its configuration (standalone/ distributed architecture/ cloud EPABX, location of EPABX).

(iv) Details of infrastructure shared if any, including CUG facility.

(v) Location of Data Centre of the client of OSP for whom the services are being provided by OSP

(b) The OSP may choose any technical solution available for the connectivity from the authorised TSPs, provided that the terms and conditions of registration are met and there is no infringement on the scope of authorised TSPs. The network diagram should be self-attested in case of domestic OSP and counter signed by the TSP in case of International OSP.

(c) Captive Contact Centre should furnish self-attested network diagram at the time of intimation and any change in the network diagram may be intimated to DoT through the web portal immediately.

VI. Internet Connectivity

2.44 An OSP is permitted to have internet connectivity from the authorized Internet Service Providers. For the purpose of Internet connectivity in India, the OSPs are permitted to use IP address that is registered in the name of an Indian Entity that shall be traceable to a physical address (location) in India. Internet connectivity and IP address pertaining to any location outside India is not permitted.

2.45 Few stakeholders have stated that the existing provision be continued. Many stakeholders have stated that internet connectivity obtained by the OSP at one location from authorized TSP should be permitted to be used at other OSP locations of the same company. The reasons behind this view is that at each location where internet connectivity is taken by any OSP from the ISP, necessary security provisions such as

Firewall, Proxy, Intrusion Detection/Prevention System etc. is required. If the company has multiple OSP locations, it finds it cost effective to have all the security apparatus at one place and share the internet bandwidth.

2.46 A few stakeholders have stated that the requirement of having internet connectivity from Indian ISP and IP address in name of Indian entity, should be done away with. One of the stakeholders has stated that the internet connection should be either from category-A ISP at a centralized location or at each location. Few of the stakeholders have stated that in case of disaster, OSP should be allowed to utilize internet connectivity using infrastructure of its parent/Group or Affiliates (including overseas) for temporary limited period/30 Days.

Analysis

2.47 The internet connectivity is one of the most vital telecom resource. It is also important from the security point of view. The provision of internet connection is dealt under ISP licence. At present, only ISP is authorized to carry the internet traffic from one location to another location.

2.48 The Authority noted the views of stakeholders where it has been highlighted that the centralized internet connectivity at one OSP centre, in case of multiple OSP centres of one company, may be allowed from the point of view of ease of doing business and also keeping in view the cost and security measures. There will be no infringement of scope of TSP if:

(i) The internet connection at the centralized location is taken from an ISP having geographical jurisdiction covering every OSP locations proposed to be covered and

(ii) The internet is logically separated with other telecom resources.

2.49 With regard to security concern, the provision is already available for ISP Licensee under clause 7 of Internet Service (Chapter-IX) of Unified License. In case, single internet connection is proposed for multiple OSP centres of one company, it should intimate the intent to the ISP clearly providing the physical location of each OSP centre. The ISP should, in such situation, assign static IP address to the OSP indicating the specific IP addresses to be used at each OSP location. In addition, the pool of IP addresses used by the OSP at each location may be regularly updated to the ISP. Also, the complete traceability details to track all the users, machines, equipment etc and their location should be maintained for one year by OSP and be provided as and when required by DoT or security agencies.

2.50 Therefore, the Authority recommends that:

(i) The OSP may obtain Internet connectivity from authorized Internet Service Provider. The OSP should be permitted to use IP address that is registered in the name of an Indian Entity that is traceable to a physical address (location) in India, Internet connectivity and IP address pertaining to any location outside India should not be permitted.

(ii) A company/ LLP having multiple OSP centers may obtain internet connection at a centralized location from authorised ISP with further distribution to all the OSP centers. However, the concerned ISP should have geographical jurisdiction covering all the OSP centers. The internet VPN so established, should be logically separated from other telecom resources. The ISP shall assign specific IP addresses to be used at each OSP location. Any change in the IP address for any specific location shall be done only after prior intimation to the ISP.

VII. Hot-site for disaster management

2.51 As per existing provisions, the domestic OSPs are permitted to connect to the dedicated servers provided at the registered 'Hot-Sites' only at the time of disaster, with due intimation to the DoT giving connectivity details. Similar arrangements are permitted to the International OSPs also. OSP Centres of the same Company / LLP (both domestic & International) are permitted to cross map the seats for use during disaster, with due intimation to the DoT. However, any interconnection between the 'Hot-Sites' of domestic OSP and International OSP is not permitted.

2.52 Most of the stakeholders have stated that the existing provisions may be continued. Some of the stakeholders have stated that Hot-site should be allowed to operate, without any intimation/ notification to DoT. Few stakeholders have stated that considering the prime purpose of a Hot-site is that of business continuity, the requirement to register it as an OSP centre is an unnecessary requirement. One of the stakeholders has opined that periodic reporting may cover information with regards to what date and period hot-site was used. Another stakeholder has opined that all operational details and the BCP (Business Continuity Plan) of the OSP be better left to OSP to handle. Another stakeholder has mentioned that the term 'Hot Sites' implies that these are always active and an OSP should be permitted to use a Hot Site during normal business activity to validate the integrity of the data and infrastructure.

2.53 Some of the stakeholders have stated that 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'. They have further stated that Hot sites 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 business continuity purposes. Few of the

stakeholders have stated that interconnection between hot sites of domestic OSP and international OSP may also be allowed.

Analysis

2.54 The Authority has noted that the Hot-sites of the OSPs are already being registered. The provisions for necessary connectivity are there and the hot site can be made operational at the time of disaster. Thus, the arrangement for the hot sites and their operation appears to be adequate. The Authority is, therefore, of the view that no change is required to be made in the terms and conditions related to Hot sites.

2.55 The Authority recommends that the current provisions related to Hot Site in Clause 2 (sub clause 1 to 3) of the Chapter III of existing terms and conditions may be retained.

VIII. Terms and conditions specific to be Domestic OSP

2.56 Domestic OSP is permitted to terminate PSTN/PLMN connection with outgoing facility on the same EPABX. However, it is required to be ensured that such PSTN/PLMN lines are used for making calls through normal NLD network only. There is requirement of a logical partitioning to ensure the separation of these facilities. Other connectivities e.g. Lease Circuit and Virtual Private Network (VPN) are permitted at the same centre. However, call flow between these PSTN lines and Leased lines are not permitted. Further, interconnectivity of two or more Domestic OSP Centres of the same Company / LLP or group of companies is permitted. Domestic OSP is permitted to use Integrated Services Digital Network (ISDN) connections only for the purpose of back up of domestic leased circuits.

2.57 While many stakeholders have agreed with the existing provision, some of the stakeholders have stated that the restriction related to

logical partitioning should be removed. A few stakeholders stated that logical partitioning may be continued till PSTN and IP integration is legally prohibited. A few stakeholders have stated that logical partition is no longer critical and it should be left to be negotiated between OSP and TSP.

Analysis

2.58 The Authority has noted that the current terms and conditions specific to domestic OSPs, as provided in the Clause 3 (sub clause 1 to 4) of Chapter III of the existing guidelines for registration of the OSPs, are suitable for facilitating the operation of domestic OSPs as well as preventing the infringement of any scope of the authorised TSPs. Also, the logical partitioning between various telecom resources ensure compliance to licences and security conditions. Therefore, the current provisions may be continued.

2.59 The Authority recommends that the terms and conditions specific to the domestic OSP in Chapter III Clause 3 (sub clause 1 to 4) of the existing guidelines for OSP registration may be continued.

IX. Terms and conditions specific to be International OSP

2.60 No PSTN connectivity is permitted to the International OSP at the Indian end. PSTN connectivity on foreign end is permitted having facility of both inbound and outbound calls. Further, interconnection of two or more International OSPs of the same Company / LLP or the group companies is permitted, with intimation to the registering authority within 15 days of such interconnection.

2.61 Most of the stakeholders have agreed with the existing provisions. However, some stakeholders have stated that PSTN connectivity may

be permitted at International OSP. A few stakeholders have also stated Logical separation of call flow between PSTN and VoIP should be discontinued.

Analysis

2.62 The Authority is of the view that the provision of no PSTN connectivity at international OSP to be continued. The Authority has also noted the concern of the OSPs that the absence of any PSTN connection at the OSP centre creates difficulty in carrying out activities related to maintenance etc. Therefore, the Authority is of the view that the OSP may obtain minimal PSTN connection for catering to their voice calls needs to address logistics or maintenance requirements for the OSP centre. However, it may be ensured that such PSTN connection is having physical separation from other telecom resources of OSP, to address security/ infringement of scope concern. Bulk PSTN connection such as PRI etc may not be permitted at International OSP.

2.63 The Authority recommends that the terms and conditions specific to the International OSP in Chapter III Clause 4 (sub clause 1 to 2) of the existing guidelines for OSP registration may be continued. Minimal PSTN telecom resources, physically separated with the resources of the OSP, may be permitted at International OSP to address logistics requirements at the OSP centre.

X. Provision for monitoring and security mechanism

2.64 The terms and conditions for OSP registration were formulated with the consideration that the EPABX and related resources would be placed at the OSP centre. This allowed easy access and monitoring of the utilization of resources, as and when required. However, with the advancement of technology and change in business need, OSPs prefer to keep minimum infrastructure required for running the services in

their premises. Generally, Data Centres are preferred outside OSP location for aggregation of such infrastructure / resources. There is a trend in shifting EPABX also to locations outside OSP premises. It is also seen that telecom resources like PRIs / Internet are availed at outside OSP location and then extended to the actual OSP location where agents are seated for operational requirement.

2.65 In such a situation, where the infrastructure for OSP (Data Centre/ PABX /telecom resources) are placed outside the OSP center, the inspection of such infrastructure to check for the compliance of terms and conditions of OSP registration would be difficult. In cases, where these infrastructures are shared with other OSPs, it becomes a complex scenario to check the compliance of terms and conditions.

2.66 A few of the stakeholders have agreed with the existing provision. Many Stakeholders have stated that with growing use of Servers/ softwares by the OSPs in the data centres, assessing compliance through physical inspection of Data Centre/ Centralised PBX may not be insisted. Compliance may be assessed through checking the routing table, logical partitioning, command logs etc. from OSP centre. The audit procedure would need to be modified accordingly. One of the stakeholders has stated that CDRs of hosted PBX can be accessed remotely from OSP locations. Log of configurations for users, extensions shall be available at Data centres hosting PBX applications. Call trace could be done with CDR available in hosted PBX and TSP network. Physical inspection of OSP centre and Data Centre where PBX is hosted could be done. One of the stakeholders has stated that there are sufficient tools that have capability to apply policies at individual, department, and site level in order to ensure that necessary conditions are being met. The same tools allow for investigations in the event of a breach. All Telecom Service Providers (TSPs) keep a log of all calls and their content for a year due to their licensing conditions.

2.67 One of the Stakeholders has stated that necessary inspection of the OSP traffic at the source by TSP or LEAs should be mandated on providing substantive evidence of violation. TSPs are already subject to security norms. To extend these norms to users of TSP resources adds little to enhance security. Requirement of providing call records to security agencies is vague, as the term 'security agencies' has not been defined, leaving it open to interpretation. 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.

2.68 One of the Stakeholders has stated that Centralized shared infrastructure should be allowed. It will be far easier for the enforcement agencies to monitor usage at a centralized location rather than at multiple satellite sites. It is also opined that connectivity between the satellite centers and centralized locations should be allowed over the public Internet.

2.69 One of the Stakeholders has stated that 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. Another stakeholder has stated that the DOT should not specify the implementation of infrastructure but instead the data for which they would require free and ready access and it should up to the OSP to ensure that data is available.

Analysis

2.70 The Authority noted that as far as the resources (such as EPABX, telecom resources, Data Centre) at different locations are owned by OSP, the existing compliance measures are adequate and may be continued. However, in case the various resources located at different locations are owned by different entities, the same need to be

addressed either by provisioning of such services by licensed service providers or by creating another category of regulated service providers. The Authority is of the view that to meet the monitoring requirement, the remote access of CDRs, log of configurations of EPABX, routing tables and logical partitioning should be made available by the OSP at the OSP center. Further, physical access to Data Centre hosting the centralized EPABX and applications may also be provided, if required.

2.71 In addition to above, the Authority is of the view that specific technical provisions for addressing security concerns related to OSPs, may be finalized by DoT in consultation with the TEC.

2.72 The Authority, therefore, recommends that in case the EPABX is installed at a different location, the remote access of CDRs, log of configurations of EPABX, routing tables and logical partitioning should be made available by the OSP at the OSP center. Further, physical access to Data Centre hosting the centralized EPABX and applications may also be provided to DoT/ Security Agencies, if required.

2.73 The Authority further recommends that specific technical provisions for addressing the security and monitoring concerns related to OSPs may be finalized by DoT in consultation with the TEC.

XI. Extended OSP

2.74 At present, the guidelines for registration of OSPs do not provide any categorisation such as extended OSP. The registration of OSP is done for the facilities/ resources of any OSP at a given location. In case, the same OSP is required to expand in different floor of same building or

in the same campus, it is required to register separately as a new OSP centre.

2.75 Many stakeholders have stated that there should not be any geographic limitation in allowing the extended OSP. Some stakeholders have stated that the extended OSP should be within the same LSA. Other stakeholders have stated that the extended OSP should be within same city. One of the stakeholders has stated that the extended OSP should be within the same building/campus.

Analysis

2.76 There already exists the provision of registration of multiple OSP centres. Further, at para 2.31 above, single registration of multiple OSP centres of the same company within LSA has been recommended. Also, if the extended OSP centre is at a considerable distance from the main OSP centre then there would be requirement of additional telecom resources. Therefore, extended OSP centre located outside a campus may not be termed as extended OSP centre. Extended OSP may be allowed within same campus without any additional resource. Further, all the security compliance needs would be integrated with the main OSP centre.

2.77 Therefore, the Authority recommends that an OSP centre may be extended within the same campus/building under existing OSP registration. At the time of registration/extending the existing OSP, the information about the extended OSP may be uploaded on the DoT portal.

XII. Sharing of infrastructure between Domestic and International OSP centre.

2.78 At present, sharing of infrastructure between Domestic and International OSP centre of the same company is allowed. In addition, OSP should set up a call centre having at least 50 seats. The OSP is required to submit a bank guarantee of Rs. 50 lakh for Option – 1 and Rs. 1 Crore for Option – 2 (option 1 & 2 defined in technical conditions), in addition to signing an agreement in the prescribed format. The registration for sharing is valid for an initial period of 3 years from the effective date, unless revoked, extendable for a further period of maximum 3 years.

2.79 Under the existing option -1, separate & independent EPABX is permitted to be used for International & Domestic OSP Centres with sharing of same operator position. There is no interconnection between the EPABX used for domestic and international OSP and they are kept separate and independent. The OSP is required to ensure that one operator position is offered either incoming or outgoing call at a time, irrespective of domestic or international. No voice traffic flow between domestic and international OSP centers is permitted and the OSP is required to ensure that there is no bypass of the network of authorized TSPs in case of NLD / ILD calls. For audit purposes, OSP is required to ensure that the system logs are tamper proof and are preserved for at-least six months.

2.80 The existing option – 2 for infrastructure sharing is regarding sharing the EPABX of International Call Centre (ICC), Domestic OSP Centres and PSTN lines for office use with logical partitioning. For sharing of the EPABX of the International and domestic OSP, there should be complete logical separation between the activities of the domestic OSP, International OSP Centre and PSTN lines for office use. Logical separation should be such that no voice or data traffic shall flow among the Domestic / International OSP centers and PSTN lines for office use and no bypass of the network of the Authorized Telecom Service Providers shall be caused. OSP is required to certify before

using the EPABX sharing facility that the logical partitioning as per the OSP Registration has been implemented and shall remain implemented.

2.81 In this regard, the OSP is required to submit a certificate from the Vendors of the equipment that the software is capable of logically bifurcating the common infrastructure into two / three (as applicable) separate and independent environments for the Domestic OSP Centre, International OSP Centers and PSTN lines for office use. The certificate is required to be deposited with the concerned DoT LSA unit. Further, OSP is required to ensure that the system logs are tamper-proof and system logs are preserved at least for one Year. The usage records (Call Detail records and Usages Data Records) are required to be maintained for a period of one year. The OSP is also required to provide the CDRs and UDRs thus saved/stored to the Security agencies/DoT as and when demanded.

2.82 Many stakeholders have agreed with the existing provisions. Few stakeholders have stated that there should be seamless interconnection between International OSP and Domestic OSP network without any restriction and bank guarantee. Few stakeholders have stated that the condition of call centre having at least 50 seats for infrastructure shared should be removed. Many stakeholders have stated that the amount of bank guarantee may be reduced. One of the stakeholders has stated that the procedure for infra sharing permission is lengthy, needs to be simplified and should be made part of main OSP application. One of the stakeholders has stated that there should be no separate application process seeking prior permission of DoT for sharing of infrastructure and an intimation to DoT should suffice as long as OSP is complying the requirements/ principles notified by DoT in this regard.

2.83 Few stakeholders have stated that validity of permission for sharing infrastructure of 3 years and extension by another 3 years should be removed and made co-terminus with OSP registration validity. One of the stakeholders has stated that validity of infrastructure sharing may be extended to 5 years from current 3 years.

2.84 Some stakeholders have stated that the Option 1 and 2 should be reviewed, however, it must be ensured that there is no bypass of network of authorised TSP. Few stakeholders have stated that the Option 1 and 2 are not required and the logical partitioning can be implemented by the OSP. Few stakeholders have stated that OSP may be allowed to deploy the best available technology and without any regulatory deterrent. Some of the stakeholders have stated that Option 1 and 2 should be merged as single option.

Analysis

2.85 The Authority is of the view that there should be light touch regulatory framework for the OSPs, including for sharing of infrastructure between them. The process of permission for sharing of infrastructure should be simple and online. The current requirement of signing of agreement with DoT, including furnishing of bank guarantee, makes the process lengthy as it requires signing of agreement at DoT office and also bank guarantee is required to be arranged by the OSP. Since, the OSP is not directly liable to make any payment to DoT in regard to normal OSP, hence it is felt that there is no need of having separate agreement. Further, any terms and conditions, if felt so, can be made part of registration certificate which the OSP is bound to follow. Therefore, the Authority is of the view that no separate agreement is required for infrastructure sharing between domestic and International OSPs. The portal for registration should have the provision for infrastructure sharing also.

2.86 It is understood that the provision of a bank guarantee was kept only as a deterrent for misuse of sharing of infrastructure. The bank guarantee appears to act as a financial barrier in availing infrastructure sharing facility. The Authority is of the view that any barrier in availing the permitted facilities should be removed and the OSPs should be encouraged to use the infrastructure efficiently and effectively. In case of violation of terms and conditions the OSP should be subjected to penalty which could act as deterrent in violation of terms and conditions. Therefore, in case of violation of infrastructure sharing conditions, the OSP registration should be cancelled and the OSP company/LLP shall be debarred from taking registration for 3 years. In addition, a financial penalty equivalent to the BG amount in existing terms and conditions may be imposed (i.e. Rs. 50 Lakh in case of option 1 and Rs. 1 Crore in case of option 2). In case, the OSP fails to comply with the penalty order, penal action as provided in the Indian Telegraph Act may be initiated in addition to cancellation of Registration. These provisions may be mentioned in the registration certificate issued to the OSP.

2.87 The Authority recommends that the technical terms and conditions of infrastructure sharing between domestic and international OSP under option 1 and 2 mentioned in Clause 4, Chapter IV of existing terms and conditions for OSP registration may be continued. However, with regard to general conditions of the infrastructure sharing, the provisions related to signing of agreement, bank guarantee and certificate of manufacturer for logical partitioning capability should be removed. The sharing of infrastructure provisions therefore would become co-terminus with the period of registration. Provisions should be made in the portal to fill up the sharing requirement details at the time of applying for registration or at a later stage.

2.88 In case of violation of infrastructure sharing conditions, the OSP registration should be cancelled and the OSP company/LLP shall be debarred from taking registration for 3 years. In addition, a financial penalty of Rs. 50 Lakh in case of option 1 and Rs. 1 Crore in case of option 2 may be imposed. In case, the OSP fails to comply to the penalty order, penal action as provided in the Indian Telegraph Act may be initiated in addition to cancellation of registration. These provisions may be incorporated in the registration certificate issued to the OSP.

XIII. Open source EPABX or distributed architecture of EPABXs (main EPABX at a centralized location and media gateways at individual OSP centres)

2.89 The OSPs using distributed architecture of EPABX are required to implement call-restrictions, logical tenant-partitioning etc. from the central EPABX. The media gateway/ PBX at the remote ends are required to maintain a copy of configurations pertaining to logical separation and keep it updated at a predefined periodicity. The CDRs for all the Voice Traffic carried by EPABX is required to be segregated for each media gateway and preserved for at least one year. The time stamp in the CDR should be synchronized with Indian Standard Time and it should be possible to view the CDR data alongwith the details of the agent managing the position by remote login to CDR machine/ server.

2.90 The log of all command(s) relevant for implementation of partitioning / call-routing is required to be non-erasable & non-editable and be kept by the OSP in the EPABX Server/Media-Gateway for a minimum period of one year. List of commands (command-set) for the Central EPABX/ Server/ Media Gateway(s) along with their application and functional details are required to be submitted to the concerned DoT LSA unit. Any subsequent change later on in this command-set is also

required to be intimated within a week of its implementation to the concerned DoT LSA Unit. A schematic diagram depicting the authorisations and call-flow permitted at remote location and the partition/access table duly signed by the authorised signatory shall be submitted to the DoT LSA Unit. This shall include the details of barred access for remote location. Any subsequent change later on in the schematic is also required to be intimated to the DoT LSA Unit within one week of its implementation.

2.91 The distributed architecture in case of OSP can be categorised in two broad categories: Captive and out-sourced. The issues related to out-sourced model will be dealt in subsequent paras under hosted contact centre. In the captive distributed architecture, the entire infrastructure, except the telecom resources, is owned by the OSP itself. The telecom resources in all the cases shall be provided by the Authorised TSPs. As different network elements in a distributed architecture are located in different geographical locations, the verification/checking the compliance of terms and conditions of OSP registration becomes tedious.

2.92 Many stakeholders have stated that geographical limit should be within India while many have stated that geographical limit should be removed. Some of the stakeholders have stated that for domestic OSP, the limit should be LSA. One of the stakeholders has stated that geographical limit of city would suffice. One of the stakeholders has stated that in case of international OSP, multiple OSP centres of same entity should also be allowed to have distributed architecture with central PBX mandatorily deployed in India with its centres sharing central PBX, spread across country. One of the stakeholders has stated that the special dispensation provided under OSP registration, to transport the incoming PSTN calls from one location to the other should be extended to outgoing voice calls as well to enable the OSPs to provide IT enabled services in an effective and efficient manner. One

of the stakeholders has stated that as long as the OSP centre is able to provide mirror copy of the traffic exchanged on its network, no restriction is required to be put on the use of the EPABX from any part of the world.

2.93 Few stakeholders have agreed with the existing provisions on logical partitioning. Few stakeholders have stated that the restriction of logical partitioning should be removed. Some of the stakeholders have stated that the OSP should only have obligation for segregation of traffic for domestic and International OSP. One of the stakeholders has stated that OSP should have special dispensation to connect IP-PSTN traffic locally and should be allowed to use the unified communication beneficial for their business growth. One of the stakeholders has stated that in view of the modern 4G technologies, where voice is also a form of data and all network traffic will be necessarily data traffic only, the requirement to keep the voice and data paths separate can be done away with, while retaining the requirements of logical partitioning of resources between Domestic and international OSP centres.

2.94 One of the stakeholders has stated the concerns of toll-bypass are equally imminent in the case of other users of significant telecom resources as well. Therefore, there is no justifiable basis for only subjecting OSP to such requirements. In case the requirements to obtain an OSP registration is continued, there are means to prevent this in modern day EPABXs, where it is possible to introduce appropriate configurations to ensure that no unauthorised call flows are taking place. A few stakeholders have stated that the logical partitioning is only intended to accomplish the objective of preventing PSTN and IP integration. Once the NDCP 2018 recommendation gets implemented by removing this bar, then the PSTN and IP get integrated seamlessly. Then there is no need for these requirements.

2.95 Many stakeholders have agreed with the existing monitoring provision for distributed architecture of EPABX. Some stakeholders have also stated that the physical inspection of EPABX locations and server location may not be required and the necessary information may be accessed from OSP centre. One of the stakeholders has stated that instead of physical inspection at EPBAX locations and 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. A few stakeholders have stated that Regulatory monitoring of the operations of OSP may be required and this can be accomplished by having a node with regulator having real-time access to all Call Data Record details to ensure that the call data can be accessed any time.

Analysis

2.96 The Authority is of the view that the existing terms and conditions for distributed architecture of EPABX address the issues related to captive use of distributed EPABX by an OSP. With the distributed architecture of PABX, domestic OSP may connect OSP centres anywhere in India. In case of international OSP, multiple OSP centres of same entity should also be allowed to have distributed architecture with central EPABX sharing central EPABX, spread across country. Also, the provision for logical partitioning would ensure segregation of traffic of each type. The Authority is, therefore, of the view that the existing conditions for distributed architecture of EPABX should be continued for the EPABX owned by the domestic as well as International OSPs.

2.97 The Authority recommends that the provision for distributed architecture of EPABX, as provided in Clause 5 Chapter IV of the existing terms and conditions for registration of OSP, should be

continued for the distributed architecture of EPABX, where the EPABX is owned by the OSP.

XIV. Provision of Call Centre Facilities by Call/ Contact Centre Service Provider (CCSP)/ Hosted Contact Centre Service Providers (HCCSP)

2.98 There are Service Providers who have set up Data Centers/ Facilities for providing the infrastructure required for setting up of a Call Centre/ Contact Centre instantly. The service providers who offer these services directly from their Data Centres are termed as Contact Centre Service Providers (CCSP) and those service providers who have hosted their services over cloud and are providing these services using internet are termed as Hosted Contact Centre Service Provider (HCCSP). The existing terms and conditions for registration of OSPs does not have any provision governing the infrastructure provision or compliance requirements to be met by CCSP/HCCSP.

2.99 Many stakeholders have stated that there should be no registration or license to provide HCCSP/CCSP services. Some stakeholders have stated that HCCSP/CCSP should be brought under separate category of OSP registration. Many stakeholders have stated that provision of CCSP/HCCSP solutions to OSP should be permitted to authorized TSP (Access) /ISP/NLD/ILD licensees only. One of the stakeholders has stated that while providing CCSP/ HCCSP services all terms and conditions as stipulated in OSP guidelines need to be followed by the TSPs. One of the stakeholders has stated that this should be similar to OSP registration and CCSP/HCCSP should be required to submit architecture to TSP's while procuring telecom resources and they should be subjected to a bi-annual audit by TSP's. TSP's should be responsible for making sure that CCSP/HCCSP is not inter-mixing IP and PSTN traffic.

2.100 A few stakeholders have stated that CCSP/HCCSP is the Telephony Application Service Provider. Their scope includes call conferencing/bridging of two call legs, one call leg to the calling associate and another to the far end customer. The Telecom resources of CCSP/HCCSP are always procured from Licensed BSOs/TSPs and CCSP/HCCSP are only Telephony Applications Services Providers operating in the domain of adding value to the services offered by BSO/TSP. Actually, it is but apt to redefine OSP as BCSP (Business Communications Service Provider) and CCSP/HCCSP as BCSTP (Business communications Services Technology Provider). Thus, there is no infringement whatsoever with the scope of licensed BSOs/Access Service Providers. One of the stakeholders has stated that all services under current OSP laws should be allowed under CCSP/HCCSP and should be able to share the infra similar to centralized architecture, EPABX sharing. OSP's can submit bank guarantee for the same, if required. One of the stakeholders has stated that they should be allowed to provide infrastructure and network services sans telecom connectivity as the latter is domain of licensed TSPs. One of the stakeholders has stated that allowing cloud providers to offer such services to end customers does not infringe or impact TSP or ISP revenues.

2.101 One of the stakeholders has stated that if the CCSP/HCCSP are non TSPs and the compliances are managed by the OSP centres such that the hosts are merely space and infrastructure providers without telecom connectivity, no further regulation is required. Another stakeholder has hoped minimal regulations in Licensing through Authorisation. To ensure national and global compliance, regulations, therefore should be light touch and there should be a level playing field between OSPs and CCSP/HCCSP as far as regulatory compliances are required. A few stakeholders have stated that in order to promote Skill India and start-up India, such services should also

be allowed by the non-telecom licensee (a company registered in India) to the extent they do not infringe upon the scope of authorised TSP.

Analysis

2.102 The CCSPs/HCCSPs provide platform as a service to the OSP to facilitate quick launch of services. Various models of service offering by CCSPs are providing a combination of services such as EPABX, IVR, call handling, call recording, contact centre data analytics, customer relationship management etc.. The technology used for Voice switching may be circuit switched or Packet switched. These facilities may be provided either on a system, installed in a single data centre, or emulated through software on servers having different components hosted in different data centres. In case the infrastructure of the OSP centre is fully owned by the OSP, they have full control on it and can take full responsibility for implementing the terms and conditions covering all components of the OSP Centre. In case the infrastructure is provided by CCSP/HCCSP, there is dual control in operation of call centre services, partly in the hands of CCSP/HCCSP and partly in hands of OSPs. CCSPs/HCCSPs actually control partition tables that are heart of all operations of such networks and only some part of data is administered by OSPs. This may lead to manipulation of networks by CCSPs/HCCSPs without the knowledge of OSPs. Even periodical inspection of OSPs cannot help in identifying activities related to violation of terms and conditions in such cases. Therefore, the Authority is of the view that the CCSP/HCCSP should be covered under regulatory framework.

2.103 It has been observed that there are two types of CCSPs/HCCSPs. Those who provide the platform as a service for contact centres including the components of EPABX, IVR, CRM, Call recording etc. but do not involve switching of voice calls or in resale of telecom services such as PRI etc. Therefore, the telecom resources are directly purchased either by the OSP or its customer. Such CCSPs are mere

extension of OSP networks. Therefore, the Authority is of the view that such CCSPs/HCCSPs may be registered with DoT on the lines of OSP registration. These CCSPs/HCCSPs should be Indian Company, having their data centre(s) in India for providing the contact centre platform to OSPs. As one CCSP/HCCSP would provide the service to more than one OSP, the CCSP/HCCSP should ensure that there is logical partitioning between the components of the platform handling telecom resources (such as EPABX) of different OSPs. The complete log and record of the logical partitioning should be maintained by the CCSP/HCCSP including the CDR. These records should be maintained, at least, for a period of one year. The CCSP/HCCSP should provide these records to DoT or security agencies designated by DoT, as and when required. Further, for checking the compliance or investigation related to violations, physical access to their data centre(s) should also be provided to DoT/ Security agencies as and when required. There should not be mixing of data and voice path and the CCSP/HCCSP should not infringe upon the scope of authorised TSPs. The CCSP/HCCSP should furnish the list of OSPs, served by them, to DoT annually.

2.104 For the purpose of registration of CCSP/HCCSP, a category similar to OSP registration may be created using the same online portal of DoT. The registration in this case may also be completed within a month. For any violation to these conditions, a penalty of Rs. 50 lakh per violation may be imposed on the CCSP/HCCSP.

2.105 The other category of CCSP/HCCSP are those who also offer resale of telecom resources to OSPs such as PRIs/toll free number etc. in addition to providing the necessary platform for OSPs explained in paras above. These activities infringe upon the scope of authorised TSPs. For such service providers who are involved in reselling telecom resources, licence under Virtual Network Operator (VNO) Category is issued by DoT. Therefore, the Authority is of the view that those CCSPs

who are reselling the telecom resources, after obtaining the necessary telecom resources from authorized TSPs, are required to obtain UL-VNO licence. Conversely, any authorised TSP who has necessary authorisation for access service, as per requirement, should be allowed to function as CCSP/HCCSP.

2.106 The existing CCSPs/HCCSPs should be given a reasonable time, say a period of 3 months from the date of issue of the policy for getting themselves registered or require license, as the case may be.

2.107 The Authority recommends that:

(i) The CCSPs/HCCSPs who provide only the platform as service including a combination of the components of EPABX, IVR, call handling/administration, call recording, contact centre data analytics, customer relationship management etc. for contact centres, should be required to get registered with DoT. These CCSPs/HCCSPs should be Indian Company, having their data centre(s) in India for providing the contact centre platform to OSPs. The CCSP/HCCSP should ensure that there is logical partitioning between the components of the platform handling telecom resources of different OSPs. A complete log and record of the logical partitioning including the CDR should be maintained by the CCSP/HCCSP. These records should be maintained at least for a period of one year. The CCSP/HCCSP should provide these records to DoT or security agencies designated by DoT, as and when required. Further, physical access to their data centre(s) should also be provided to DoT/ Security agencies as and when required. For the purpose of registration of CCSP/HCCSP, DoT should create a category similar to OSP registration and complete the registration activity online on the existing web portal. The document requirement should be similar to OSP registration. The CCSP/HCCSP should provide the location wise list of network elements. However, no network diagram should be required. The

registration process should be completed in a period of one month similar to OSP registration. There should not be mixing of data and voice path and the CCSP/HCCSP should not infringe upon the scope of authorised TSPs. For any violation to these conditions, a penalty of Rs. 50 lakh per violation may be imposed on the CCSP/HCCSP. The CCSP/HCCSP should furnish the list of OSPs, served by them, to DoT annually.

(ii) Those CCSPs/HCCSPs who provide the platform as service as mentioned in para (i) above and are also involved in reselling the telecom resources to OSPs, are required to obtain UL-VNO licence, as applicable, from DoT.

(iii) Any Licensed TSP / Unified Licensee having suitable Authorisation should be allowed to function as CCSP/HCCSP.

(iv) The existing CCSPs/HCCSPs may be provided a period of 3 months for getting registration/ suitable license from DoT.

XV. Interconnection of Data Path and Voice Path in Domestic Operations:

2.108 In case of Domestic OSP, a separation is required to be maintained between PSTN lines and leased circuits to ensure that there is no call flow between them. The domestic OSPs may require to have internet leased lines and NLD leased lines / VPN circuits terminated on the same network where PSTN is terminated and EPABX is connected. To comply with the separation of data and voice path requirement, the OSP may be willing to deploy logical partitioning. However, it is noted by DoT that monitoring of logical partitioning / separation of voice and data path is a challenging task. There may also be requirement of connectivity of EPABX with leased line for O&M of EPABX. In this case also the monitoring of usage of leased line with EPABX would be a challenge.

2.109 A few stakeholders have stated that interconnection of data and voice should be allowed while few stakeholders have stated that it must be permitted at the discretion of TSPs, while a few stakeholders have stated that interconnection of data and voice should not be allowed.

2.110 One of the stakeholders has stated that the compliance can be monitored with the help of call flow, call tests, CDR and system logs. A few stakeholders have stated that the compliance to these guidelines should be the responsibility of OSP and recommend the periodic check by LSA TERM Cells for ensuring the compliance of terms and conditions under OSP registration. The security compliance as well as penal clauses for OSP for noncompliance to guidelines may be incorporated suitably in OSP guidelines which acts as a deterrent and results in compliance by the OSPs. A few stakeholders have stated that monitoring of the underlying TSP network serves the purpose of security compliance and other monitoring may not be necessary.

2.111 Some stakeholders have stated that the primary concern of DoT is that there should not be any interconnection between public and private networks to protect against prohibited toll bypass. These concerns are equally applicable in the case of non-OSPs as well. This aspect can be verified by TSPs in the same manner that they do so currently, i.e. by conducting physical inspection of customer premises. One of the stakeholders has stated that all voice & data circuits are obtained from Licensed TSP/ISPs who 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.

2.112 One of the stakeholders has stated that ensuring a foolproof monitoring mechanism is a statistical impossibility especially when the Authority itself has noted that Grey route of ILD traffic still forms a sizable proportion of the traffic. Imposing any additional

requirements will only impact the ease of doing OSP business and defeat the very purpose of this exercise. Another stakeholder has stated that in the event the interconnection of data and voice path is allowed for domestic operations, adequate checks and balances need to be put in place to ensure monitoring of data and voice to make sure that there is no bypass of revenue for the Government. Logical partitioning must be insisted upon. It would be good to have periodic surprise checks.

2.113 One of the stakeholders has stated that interconnection between public and private networks should be avoided to prevent flow of voice traffic and data traffic as it is not a major concern or security concern for DoT. Moreover, without any practical way of monitoring such an obligation, it is rather impractical to have such compliance requirements in place. One of the stakeholders has stated that this can be done through regular audits by DOT. Few stakeholders have stated that if and when any call is received from any OSP that does not bear any 10 digit Directory Number (DN) provided by any Licensed BSO/TSP, then such OSP can be immediately investigated and basis any unscrupulous activity, be suspended and further action be taken. There must be clear KYC compliance for the DNs through which calls are put through for all auditability post facto. One of the stakeholders has stated that monitoring and compliance should be suggested by the Authority in conjunction with TSPs and OSPs.

Analysis

2.114 In case interconnection of data and voice path is allowed for domestic operations, main concern shall be regarding security and bypass of revenue for the TSP/ Government. At present, data and voice path interconnection is not allowed. This could be allowed only to meet those operational requirements which are critical for maintenance of the systems installed at OSP centres, such as remote login for EPABX. Therefore, the Authority is of the view that the interconnection of data

and voice path at OSP centre may be allowed in rare case of remote login for equipment maintenance. The complete details of the incident including the time duration for which the interconnection of voice and data path was resorted to should be recorded and shared with DoT immediately. Any unauthorised connectivity of data and voice path may be dealt with cancellation of the registration of the OSP.

2.115 The Authority recommends that:

The interconnection of data and voice path is not allowed. However, remote login for equipment maintenance by the OEM or its agent deputed for maintenance may be allowed. The complete details of the incident including the time duration for which the remote login was resorted should be recorded and shared with DoT immediately. Any unauthorised connectivity of data and voice path may be dealt with by cancellation of the registration of the OSP.

XVI. Use of Closed User Group (CUG) for internal communication of the OSP Company / LLP

2.116 The OSPs are permitted to use CUG facility for their Internal Communication needs subject to following conditions :-

a. PSTN/PLMN/Internet telephony network is not to be connected with CUG network. There should be no bypass of NLD/ILD while making PSTN/PLMN calls. The EPABX extensions are allowed to call any national or international number (without bypass of NLD/ILD) through the PSTN/PLMN lines terminated in the EPABX which has logical partitioning for CUG. [i.e CUG extension in City A shall use the PSTN/PLMN network connectivity only of the Licensed Service Area (LSA) encompassing the City 'A' and not of any other LSA for making or receiving calls to/from PSTN/PLMN].

b. For availing this facility, the necessary accessibility/tests as enumerated for distributed architecture of EPABX, mentioned in above section are also required to be extended to the DoT LSA units.
c. The OSPs not using the sharing of infrastructure (sharing of EPABX or sharing of operator or Centralised EPABX architecture) are also allowed to use the CUG facility.

2.117 Most of the stakeholders have agreed with the existing provision for use of CUG facility by the OSP and the provision related to monitoring of compliance. A few stakeholders have stated that the use of CUG may be permitted without the requirement of Bank Guarantee. Some of the stakeholders have stated that the terms and conditions for use of CUG for internal communication are not relevant, considering that non-OSPs are not subject to such restrictions. It is essential to create a level playing field and provide dispensation to OSPs, which was the original intent of introducing the OSP regime in the first place.

2.118 Some of the stakeholders have opined that there should be no requirement for monitoring. One of the stakeholders has said that 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. One of the stakeholders has stated that there should be safeguard to ensure that there is no infringement into TSP jurisdiction. The responsibility of compliance should lie with the OSPs.

Analysis

2.119 The Authority is of the view that the current terms and conditions including those for monitoring of the use of CUG for internal communication by the OSPs are adequate and no change is required at this stage.

2.120 The Authority recommends that the terms and conditions for use of Closed User Group for internal communication of the OSP Company/LLP as mentioned in the Clause 6, Chapter IV of existing terms and conditions for registration of OSP should be continued.

XVII. Work from Home

2.121 In respect of Work From Home(WFH) facility for OSP, the agent at home is treated as Extended Agent Position of the call centre and interconnection is permitted through authorized service providers provisioned (secured) VPN (PPVPN) which have pre-defined locations i.e. home of the agent and the OSP centre as VPN end user sites. Over and above PPVPN, the OSP is allowed to use their own security mechanism like Authentication, Authorization and Accounting at the same call centre from which the connectivity has been extended to the home agent. A security deposit of Rs. 1 Crore for each registered location of OSP centre from which WFH is extended is required.

2.122 For obtaining the permission for WFH, the OSP is required to submit complete details for extended agent positions like name and complete address, connectivity alongwith the name of the service provider etc. as per the application form. All logs of the activities carried out by the extended agent should be maintained for 1 year. The IP address assigned on the VPN and the OSP centre in this regard should also be maintained for each extended agent position and should be produced whenever required by DoT. DoT has the right to carry out periodic/surprise inspection of such establishments. Registration for WFH is valid for a period of 3 years and can be extended for a further period of maximum 3 years after expiry.

2.123 Many stakeholders have agreed with the exiting provision for WFH facility. Most of the stakeholders have stated that the requirement of

PPVPN should be removed and the Bank Guarantee should be removed/reduced. One of the stakeholders has stated that the conditions of WFH should not be applicable to purely Data/ Internet Application Services provided by company for captive use.

2.124 It has been highlighted by the stakeholders that the WFH facility has been utilized in very limited way due to the requirements of PPVPN and Bank Guarantee. The use of PPVPN is costly and time consuming. Further, the Bank Guarantee of Rs. 1 Crore for each WFH connection makes the facility almost non-viable.

Analysis

2.125 The Authority is of the view that the primary purpose of the WFH facility is to provide flexibility to the agents of the OSP to connect to the OSP centres. There is a need to make the WFH facility flexible and at the same time addressing the monitoring requirements. In case the PPVPN requirements is removed and the agents are allowed to connect the OSP centre using VPN over internet, this will make the facility flexible. To ensure monitoring of the compliance and any possibility of misuse, the OSP may be mandated to intimate DoT the location (Complete Address, including IP Address) of the Home of the agents availing WFH facility in advance to DoT.

2.126 The other major limitation is the Bank Guarantee which is of Rs. 1 Crore for an OSP Centre. There could be situation where the company may prefer to change the agent than to have liability of Rs. 1 Crore in the form of Bank Guarantee. Therefore, the reduction/removal in the amount of Bank Guarantee appears to the justified. The purpose of the Bank Guarantee is just a deterrent for any misuse of WFH facility. The Authority is of the view that the provision of bank guarantee as pre-requisite to availing the WFH facility along with signing of the agreement, should be removed. As a deterrent to misuse of WFH facility, necessary penal provisions may be added to the terms and

conditions for registration of OSPs. In this regard, in case of violation of terms and conditions of WFH facility by any agent/employee or by the OSP, the OSP may be subjected to a penalty of Rs 10 lakh per WFH terminal subject to an upper limit of Rs. 1 crore. In case the penalty for violation of Rs. 1 crore is reached, the OSP may be declared as barred for using the WFH facility.

2.127 The Authority recommends that:

The Work-From-Home (WFH) is an extended agent position of the OSP centre. The requirement of PPVPN for WFH may be removed and the WFH may be connected to OSP centre using any commercially available VPN. However, the provision of prior intimation to DoT with complete address of the WFH location including static IP address for availing the facility should be continued. The requirement of agreement including the bank guarantee for availing the WHF facility may be removed.

In case of violation of terms and conditions of WFH facility by any agent/employee or by the OSP, the OSP may be subjected to a penalty of Rs 10 lakh per WFH terminal subject to an upper limit of Rs. 1 crore. In case the penalty for violation of Rs. 1 crore is reached, the OSP may be declared as barred for using the WFH facility.

XVIII. Domestic Operations by International OSP

2.128 Generally, Indian customers are served by domestic OSP centre while foreign customers are served by International OSP centres. An international OSP centre may also need to serve the customers in India. In such an arrangement, for in-bound calls, customers in India will be extended with service through an International Toll Free number. Calls will be taken to a foreign destination and from there these calls will come back through their foreign PoP. For out-bound

calls, the domestic customers receiving a service call from such OSPs will get CLI of an international number, even though the call is originated from India.

2.129 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. Else OSP will have to resort to sharing of resources with submission of Bank Guarantee, as applicable. These options may not be cost effective, if the volume of transactions for these two segments of clients separately is not adequate.

2.130 Most of the stakeholders have stated that domestic operations by International OSPs for serving their customers in India may be allowed while some of the stakeholders have stated that it should not be allowed. Few stakeholders have stated that no additional condition would be required. A few stakeholders have stated that from security point of view, all CDRs may be maintained and be made available to Law Enforcement Authority. One of the stakeholders has stated that the same should only be allowed if the volume of transactions for these two segments of clients separately is adequate. One of the stakeholders has stated that IT Act and data privacy act should be tightened to make sure that they sufficiently cover all the necessary T&C's to govern this industry. One of the stakeholders has stated that permitting VOIP and PSTN mixing will help facilitate this – Maintaining CDR's and appropriate audits can be prescribed. A few stakeholders have stated that 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. Another stakeholder has stated that operations by International OSPs serving their customers in India should be allowed unless it compromises national security or consumer safety.

Analysis

2.131 The present issue is applicable when the OSP centre is trying to serve the Indian customer of his client along with customers in other Countries. Therefore, the domestic operation by international OSP is applicable only when the client is same. To avoid any toll bypass the telecom resources for connecting with domestic customers may be separated from the telecom resources for international OSPs operations.

2.132 The Authority recommends that domestic operation by International OSP may be allowed subject to condition that it is serving the same client. Further, for making domestic calls separate resources may be taken having full separation for serving foreign customers of the client.

XIX. Use of Foreign EPABX for International Call Centre

2.133 The existing guidelines for registration of OSPs do not have any mention of the location of EPABX at foreign location.

2.134 Most of the stakeholders stated that EPABX at foreign location in case of International OSPs may be allowed provided that remote access to the system with access to CDR and other system logs is made available. Some stakeholders have stated that EPABX at foreign location in case of International OSPs may not be allowed. A few stakeholders have stated that provision for use of EPABX at foreign location should be kept in accordance with provision of national security. Some stakeholders have stated that for law enforcement purposes, a monitoring node with real time CDR details may be insisted. One of the stakeholders has stated that in case EPABX is located in foreign location, the agents should receive call from international numbers. The toll connect charges with local TSP will apply. In case the call connects over internet with the agent, the internet connectivity to local OSP centre is provided by the TSP.

2.135 One of the stakeholders has stated that as a Disaster Recovery (DR) or Server Failover measure use of EPABX at foreign location must be allowed not only for international OSP but also for Domestic OSP. Primary/Secondary servers would continue to be located in India, which as such is tuned to ensure that the scope of authorised TSP is not infringed, and security requirements are met. The DR Server at foreign location would also be controlled by the Primary /Secondary Server and would primarily be used only for signalling. One of the stakeholders has stated that IT enabled service providers should have the freedom to use global interconnected networks using the power of the Internet. VoIP calls between a foreign carrier and India are permissible under the ISP licensing as long as there is no interconnect with the PSTN within India. If the business wishes to interconnect within India then the regulation could provide for such calls being transported from overseas to India using an Indian TSP – this would protect all revenues of TSPs.

2.136 One of the stakeholders has stated that as long as the International OSP complies with the basic guidelines of Transparency and Lawful Interception and ties-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. One of the stakeholders has stated that in case of International OSP, the EPABX may be allowed at foreign end, provided that International OSP is not switching/ conferencing calls at India end.

Analysis

2.137 As long as the international OSP serves the customers of other country and there is no connectivity between the international OSP and PSTN/PLMN subscribers in India, there will not be any toll bypass issue. However, to meet the security requirement, either the EPABX

should be located in India or in case of EPABX located at foreign location, there should be undertaking from the owner of the EPABX and OSP to provide remote access of the EPABX and authenticated copy of CDR, System logs and message details as and when required.

2.138 Therefore, the Authority is of the view that EPABX at foreign location in case of international OSP may be allowed subject to conditions that the OSP provides remote access of the EPABX and authenticated copy of CDR, System logs and message details as and when required.

2.139 The Authority recommends that EPABX at foreign location in case of international OSP may be allowed subject to the condition that OSP provides remote access of the EPABX and authenticated copy of CDR, System logs and message details as and when required.

XX. Security Conditions:

2.140 The Chapter V of OSP registration provides the Security conditions applicable to the OSPs. In order to ensure their compliance, the Licensor reserves the right to inspect, as detailed in clause 1 of the Security conditions. The Security condition also provides prohibition of certain activities by the OSP under Clause 2. The Clause 3 of Chapter V provides security conditions regarding access to equipments, compliance to safety and other statue/ rule/ regulation including provision of CDR to security agencies.

2.141 Most of the stakeholders have agreed with the exiting provisions. A few stakeholders have stated that security conditions should be applicable to TSPs and not OSPs. A few stakeholders have stated that the requirement of providing call records to security agencies may be clarified and the "security agencies" to whom the call records are to be provided should be clearly identified and communicated. A few

stakeholders have stated that the security and monitoring obligations allow inspection of OSP Centres upon receipt of any complaint or Suo moto action by the designated authority. The provisions in the OSP T&C should not be such that leave the infrastructure facilities utilised in such data centres vulnerable to an unauthorized search and seizure by law enforcement agencies.

2.142 Some of the stakeholders have stated that 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 and hence may be reconsidered. One of the stakeholders has stated that as per the OSP T&Cs, DOT reserves the right to modify the terms and conditions of the registration, if required in public interest or in the interest of the security of the state or for the proper conduct of the telegraphs. This is a broad power which should be streamlined with adequate safeguards, and possibly linked to demonstrated non-compliance with registration requirements, or violation of any law, before being invoked.

2.143 A few stakeholders have stated that 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. A few stakeholders have stated that let the objectives of such regulations be crisply articulated and then examine if these are still relevant with the changed context of operations. Should regulator ensure security or the BPO should own its secure operations as the security SLA delivery always vests with BPO. A few stakeholders have stated that the security compliance as well as penal clauses for OSP for noncompliance to guidelines may

be incorporated suitably in OSP guidelines which acts as deterrence and result in compliance by the OSPs.

Analysis

2.144 The Authority is of the view that security conditions mentioned in Chapter V of the OSP guidelines are generic requirements related to security. Since the security conditions are mandatory requirements, no change in the security conditions mentioned in chapter V may be needed.

2.145 The Authority recommends that the security conditions mentioned in Chapter V of OSP registration guidelines may be continued.

XXI. Quantum and extent of penalties

2.146 The provision for penalty in case of violation of terms and conditions has been given in different chapters of the guidelines for OSP registration. The terms and conditions related to the OSP registration against which penalty has been prescribed in the current OSP registration guidelines are as below:

(i) Terms & Conditions specific to the Domestic OSP.

(ii) Sharing of infrastructure between international OSP and domestic OSP.

(iii) Penalty in case of violations for conditions related to Work From Home.

(iv) Penalty for violation of terms and conditions of Sharing of EPABX of ICC, DCC OSPs and / or PSTN lines with logical partitioning, Use of Centralized EPABX architecture, Deploying the CUG for internal communication of the OSP company with sharing of EPABX.

2.147 In most of the cases of violation it has been mentioned that punitive action including forfeiture of the security deposit and / or the cancellation of the registration held by OSP. Further, in case of sharing of infrastructure and Work From Home, in addition to the above penalty, it has also been provided that the company shall be debarred from taking OSP registration for 3 years from the date of cancellation of such registration. In all cases of the violations wherever Bank Guarantee have been prescribed, the same shall be forfeited.

2.148 Many stakeholders have stated that penalty should be specific/ graded and proportionate. Some of the stakeholder have agreed with the existing provision. Many stakeholders have stated that OSP should be given opportunity to explain before imposing penalty. A few stakeholders have stated that warning should first be issued. If no corrective action taken then penalty should be imposed. One of the stakeholders has stated that there should not be separate penal provisions for OSP, should be covered under existing provisions of License of TSPs. One of the stakeholders has stated that TSP should audit the OSP and levy penalty if there is violation based on architecture submitted at the time of registration.

2.149 One of the stakeholders has stated that in case of violation, Registration should be cancelled. Bank Guarantee should not be imposed on OSPs. Some of the stakeholders have stated that the provisions of penalty mentioned in the OSP guidelines should be made more stringent. One of the stakeholders has stated that the OSP Guidelines provide that DoT has rights to take punitive action against an OSP for violation of conditions. The word 'punitive' may have different interpretations under law and therefore, it is desirable that DoT clearly re-frames the exact nature of penalty or action that may be undertaken based on the degrees of breach committed by OSPs. One of the stakeholders has stated that OSPs be treated like any other business customer of TSPs and ISPs, and should be subject to the

same rules and regulations as for any other business user of telecom and Internet resources.

Analysis

2.150 The penalty provisions for violations related to sharing of infrastructure between domestic and international OSPs, interconnection of data and voice path in domestic operations and WFH have already been prescribed in the relevant paras above. With regard to violations of other terms and conditions of registration, the Authority is of the view that no change in the existing penal provisions is required.

2.151 Further, it has been observed that the term punitive action has not been defined in the provision of penalty. The Authority is of the view that term punitive action should be explained as per penal provisions in Indian Telegraph Act. Further, appellate provision at DoT HQ should be made to handle the differences in interpretation of guidelines and providing forum to OSPs/CCSPs/HCCSPs for appeal against decision of DoT field unit.

2.152 The Captive Contact Centre is also required to ensure that there is no infringement on jurisdiction of authorised TSPs. In case of violation, the telecom resources of the CCC may be disconnected and the concerned company/LLP may be debarred from having captive contact centre for three years. Further, DoT may take any punitive action in accordance with Indian Telegraph Act.

2.153 The penalty provisions for violations related to sharing of infrastructure between domestic and international OSPs, interconnection of data and voice path in domestic operations and WFH have already been prescribed in the relevant paras above. Further, the Authority recommends that, for violation of other terms and conditions of registration, penal provisions as

per existing terms and conditions for registration of OSP may be continued. The punitive action should be in accordance with the provisions of Indian Telegraph Act.

In case of violation by Captive Contact Centre, the telecom resources of the CCC may be disconnected and the concerned company/LLP may be debarred from having captive contact centre for three years. Further, DoT may take any punitive action in accordance with Indian Telegraph Act.

XXII. OSP to OSP interconnectivity providing similar services i.e. third party outsourcing and the safeguards

2.154 Interconnectivity of two or more Domestic OSP Centres of the same Company / LLP / or group of companies is permitted. Interconnection of two or more International OSP of the same Company / LLP or the group companies is permitted, with intimation to the registering authority within 15 days of such interconnection. Any interconnection between Domestic or International OSPs not belonging to same company or group of companies is not permitted.

2.155 Many stakeholders have stated that interconnectivity should be allowed in all cases. A few of the stakeholders have stated that interconnectivity should not be allowed. Some of the stakeholders have stated that interconnectivity should be allowed in case of same customer/client. A few of the stakeholders have stated that interconnectivity should be allowed subject to condition that Security conditions are met. Many stakeholders have stated that it should be allowed subject to condition that there is no bypass of network of authorized TSPs. One of the stakeholders has stated that should be allowed only between domestic entities. Another stakeholder has stated that it may be tried on trial basis.

2.156 A few of the stakeholders have stated that the OSPs can't infringe into licensed TSP scope. Some of the stakeholders have stated that this can be done through regular audits by DOT. A few of the stakeholders have stated TSPs and OSPs should be free to negotiate interconnectivity terms. A few of the stakeholders have agreed with the existing provisions. A few of the stakeholders have stated that TSPs should adopt reasonable measures to safeguard their interest.

2.157 One of the stakeholders has stated that the customer of the OSP(s) should get a master network diagram duly attested by respective TSPs along with individual OSP site network diagrams for all OSP sites. Such master and individual network diagrams should be submitted by respective OSPs with relevant TERM cells. Obligations in OSP guidelines for retention of data as per provisions to be complied by each OSP. One of the stakeholders has stated that electronic watch dogs should be installed to prevent any infringement of official secrets.

Analysis

2.158 In the existing guidelines for registration of OSP, multiple OSP centres of same company are allowed and also the interconnectivity between international and domestic OSP centres of the same company is allowed for efficient utilization of resources. However, if the same client has outsourced different segments of work to multiple OSPs (not belonging to same company) the client may require interconnectivity between such OSP centres for operational efficiency and efficient utilization of resources. In this scenario, in order to avoid any misuse or security issue, the client/customer of the OSPs should provide an overall network diagram, and the same should be available with each of the OSP centres, duly authenticated by respective TSPs.

2.159 The Authority is of the view that if multiple OSP centres are serving the same client, interconnectivity between them may be allowed even if the OSPs do not belong to same company. Such interconnectivity of

domestic OSP with other domestic OSP and international OSP with other international OSP only be permitted. Any interconnectivity between domestic and international OSPs not belonging to same company may not be permitted.

2.160 The Authority recommends that interconnectivity between OSP centres serving same client may be permitted with prior intimation to registering authority. However, interconnectivity between domestic and international OSPs not belonging to same company may not be permitted.

XXIII. Miscellaneous conditions

2.161 The Chapter VI of the existing OSP guidelines provides miscellaneous conditions to be complied by OSPs. It also includes conditions for Arbitration.

2.162 Many stakeholders have agreed to the existing provisions. One of the stakeholders has stated that the detailed registration process should be replaced with bare bones intimation based registration framework. Any actions on OSPs towards violation of rule/law will be applicable as law applicable to other companies registered with ROC including Indian Telegraph Act. One of the stakeholders has stated that 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. One of the stakeholders has stated that the provision of appointment of Arbitrator is arbitrary as the Arbitrator should be appointed by mutual consent of the parties and its seat should be the place of the LSA where OSP is registered. One of the stakeholders has stated that both the dispute parties, i.e. DoT and the OSP, can each nominate an arbitrator. Such arbitrators can then decide on appointment of presiding arbitrator.

Analysis

2.163 While the TSPs have TDSAT for redressal of disputes between them as well as with DoT. However, OSP being the subscribers of TSPs and the registered entity of DoT do not have any such redressal platform other than arbitration. They can only approach DoT against TSP as a normal subscriber. As far as the issue of the arbitrators is concerned, this is governed by Indian Arbitration and Conciliation Act, 1996. The Authority is of the view that DoT should offer a platform at headquarter level to the OSPs for considering the grievance/dispute raised during implementation of OSPs guideline at field units. Further, the rest of miscellaneous provision under Chapter VI may be continued.

2.164 The Authority recommends that the miscellaneous provisions in the Chapter VI of the existing guidelines for OSP registration may be continued.

Further, DoT should devise a platform at DoT Headquarter level to address the issues related to interpretation of guidelines to OSPs/CCSPs/HCCSPs/CCCs for appeal against decision of DoT field units.

XXIV. Issues related to Unsolicited Commercial Communications

2.165 Unsolicited Commercial Communications (UCC) are communications, made via voice calls or SMS, to subscribers without their consent or willingness. Revised regulations on UCC, "The Telecom Commercial Communications Customer Preference Regulations, 2018" (TCCCPR, 2018), were issued by TRAI on 19 07.2018.

2.166 The OSPs having out bound voice call facility may be involved in making calls for transactional, promotional and service purposes. They may be making calls as a sender or on behalf of some other

entity. Such calls are required to be complying with the provisions of TRAI's TCCCPR, 2018.

2.167 Many stakeholders have stated that OSPs engaged in outbound calling for transactional, promotional and service purposes should mandatorily register with the respective TSPs from which they have taken resources. It is also essential that they comply with the provisions of TCCCPR regulations. A few of the stakeholders have stated that compliance to TCCCPR 2018 should be incorporated in OSP guidelines. Many stakeholders have stated that the provisions under TCCCPR 2018 already covers this. There is no need for separate conditions in OSP guidelines. A few of the stakeholders have stated that the parent Telecom Companies providing signals to the OSPs must ensure that OSPs comply with provisions of TCCCPR. One of the stakeholders has stated Authorities must also make a condition for registration that if the OSPs do not adhere to the TCCCPR, it may amount to cancellation of license to do business as OSPs.

2.168 One of the stakeholders has stated that an amendment should be made to the terms and conditions of OSP registration w.r.t compliance to TCCCPR, 2018, which will inter-alia include telemarketer registration with TSP, registration of enders, headers, subscriber consent, content of communication, control over subscriber's preferences and submission of relevant undertakings to TSPs w.r.t declaration of use of auto-dialers in making commercial communication with appropriate controls to maintain silent or abandoned calls within prescribed limits.

Analysis

2.169 There is possibility of promotional communications from the OSPs utilizing outbound communication facilities. Therefore, the Authority is of the view that such OSPs should comply with TCCCPR 2018. A

provision mentioning this requirement may be made in the OSP guidelines.

2.170 The Authority recommends that OSPs having outbound communication facilities should comply with "The Telecom Commercial Communications Customer Preference Regulations, 2018".

Chapter III

Summary of Recommendations

3.1 BPO / ITeS Industry is one of the fastest growing segments under the Information Technology sector in the country. It has immense potential to grow at par with global standards and expand further because of strong foundation India has in IT sector and inherent cost advantage.

3.2 While framing the recommendations for review of terms and conditions for registration of OSPs, Authority has considered the present arrangement for Registration of OSPs, issues forwarded by DoT and the issues being faced by the industry. It has further been considered that the policy interventions should not act as a barrier for utilization of technological developments. Also, there should be efficient utilization of resources and at the same time suitable deterrent is provided to ensure any possible misuse or violation. It is expected that implementation of these recommendations will create better environment for growth of the sector making India as preferred BPO/ITeS destination.

3.3 The summary of recommendations are given in para below.

3.4 The Authority recommends that the OSP may be defined as below:

Other Service Providers (OSP) is a Company or Limited Liability Partnership (LLP) providing services like Business Process Outsourcing (BPO), Billing Service Centre, e-Publishing Centre, Financial Service, Knowledge Process Outsourcing (KPO), Medical Transcript Service, Network Operating Centre, Tele-Medicine, Tele-Education, Tele-Trading, Vehicle Tracking Centre or Other similar services on outsourced basis i.e. on behalf of another entity using Telecom Resources provided by authorized Telecom Service Providers. The above list of services may be modified by DoT as and when required.

The provision of above-mentioned services by a company/LLP for captive purposes i.e. to their own customers or employees shall be excluded from the scope of OSP. Such entities may be termed as "Captive Contact Centres".

(para 2.18)

3.5 The Authority, recommends that for the purpose of registration, the OSPs are categorised in following categories:

a) Voice-based OSP

An OSP providing voice-based services (using voice call or voice-based application).

b) Data/Internet based OSP (without voice component)

An OSP providing services which are purely based on data/ internet and no voice connectivity is involved.

The above categorization of OSP will be applicable to both Domestic and International OSP.

(para 2.19)

3.6 The Authority further recommends that:

(i) The voice based OSPs (Category (a)) above shall be required to register under OSP category and registration certificate shall be issued by DoT after due scrutiny of the application.

(ii) For data/internet based OSP (Category (b)), the registration shall be in the form of intimation under OSP category, where the acknowledgement of intimation shall be treated as registration certificate for OSP. However, OSP shall ensure that their activities do not infringe upon the jurisdiction of authorised TSPs.

(iii) The Captive Contact Centre shall file for intimation on DoT portal. They shall also ensure that their activities do not infringe upon the jurisdiction of authorised TSPs.

(iv) In all above cases, DoT would have the right to inspect and check any violation of terms and conditions of the guidelines.

<u>Process of Registration/ Intimation</u>

(v) The entire process of registration and intimation (data/internet based OSP and captive contact centres) should be completely online and there should not be requirement of submitting any document offline.

(vi) In case of registration of OSP (Category (a)) the DoT should scrutinize the application within one month. In case of any deficiency, the statement of deficiency along with the name of the document to be uploaded shall be generated on the Web portal for registration. Thereafter, the applicant shall take the necessary corrective action and upload the relevant document to the Web Portal. In case there is no deficiency, DoT will approve for generation of registration certificate at the Web portal as early as possible but not later than one month. The Web portal shall have the capability to auto generate the registration certificate at end of one month from the date of application if no deficiency is pointed out.

(vii) In case of intimation in respect of data/internet based OSP and Captive Contact Centres, the acknowledgment of intimation shall be generated immediately, but in any case not later than 48 hours.

(Para 2.20)

3.7 The registration of OSP shall be initially for a period of 20 years. The same may be extended by a period of 10 years at a time if applied in the 19th year of the initial registration period or in the 9th year of extended registration period.

(para 2.24)

3.8 The Authority recommends that:

(i) Multiple OSP centres of the same company/LLP should be registered as a single entity in an LSA. However, domestic and international OSPs shall not be grouped and shall be registered separately.

(ii) A processing fee of Rs. 1000/- be charged for registration of each OSP Centre.

(iii) The existing list of documents for registration may be continued. For registration of multiple OSP centres of same company, one set of documents with separate network diagrams of each centre should be submitted. In case of

multiple OSP centres of same company/LLP in different LSAs, registration certificate may be issued separately in each LSA. However, mandatory documents (except network diagram) should be uploaded for initial registration only. The web portal of online registration should have provision to apply for registration of multiple OSP centres. Additionally, provision should be made to add OSP centres with existing registered OSP centre(s) of the same company. To ensure that the other OSP centres are belonging to the same company, the digital signature used should be same while applying for additional OSP centre. In case, the signatory gets changed, the intimation in this respect, duly signed by authorised signatory for this purpose, may be uploaded as additional document and the process of uploading the documents and information may be completed using digital signature of new authorised person.

(iv) The requirement of documents for intimation in case of Captive Contact Centres should be same as OSP. The intimation may be filed separately for each centre with a fee of Rs. 1000/- per centre.

(para 2.33)

3.9 The existing provisions related to submission of annual return may be continued. The details of annual turnover and net profit/loss may be made optional data in the Performa for filing of the annual return. Auto generated email acknowledgement of annual return submitted by OSP may be sent to OSP. Auto-generated email should also be sent to OSPs as a reminder for submission of annual return, before putting them in dormant list or cancellation of registration.

Every Captive Contact Centre should also furnish the Annual Return.

(para 2.37)

3.10 The proposed network diagram should have following details:

(a) The proposed network diagram should have following details:

(i) Name of Service provider proposed to provide telecom resources

(ii) Bandwidth and the type of connectivity (PRI, Internet, VoIP, MPLS, IPLC, etc.)

(iii) Details of EPBAX and its configuration (standalone/ distributed architecture/ cloud EPABX, location of EPABX).

(iv) Details of infrastructure shared if any, including CUG facility.

(v) Location of Data Centre of the client of OSP for whom the services are being provided by OSP

(b) The OSP may choose any technical solution available for the connectivity from the authorised TSPs, provided that the terms and conditions of registration are met and there is no infringement on the scope of authorised TSPs. The network diagram should be self-attested in case of domestic OSP and counter signed by the TSP in case of International OSP.

(c) Captive Contact Centre should furnish self-attested network diagram at the time of intimation and any change in the network diagram may be intimated to DoT through the web portal immediately.

(para 2.43)

3.11 The Authority recommends that:

(i) The OSP may obtain Internet connectivity from authorized Internet Service Provider. The OSP should be permitted to use IP address that is registered in the name of an Indian Entity that is traceable to a physical address (location) in India, Internet connectivity and IP address pertaining to any location outside India should not be permitted.

(ii) A company/ LLP having multiple OSP centers may obtain internet connection at a centralized location from

authorised ISP with further distribution to all the OSP centers. However, the concerned ISP should have geographical jurisdiction covering all the OSP centers. The internet VPN so established, should be logically separated from other telecom resources. The ISP shall assign specific IP addresses to be used at each OSP location. Any change in the IP address for any specific location shall be done only after prior intimation to the ISP.

(para 2.50)

3.12 The current provisions related to Hot Site in Clause 2 (sub clause 1 to 3) of the Chapter III of existing terms and conditions may be retained.

(para 2.55)

3.13 The terms and conditions specific to the domestic OSP in Chapter III Clause 3 (sub clause 1 to 4) of the existing guidelines for OSP registration may be continued.

(para 2.59)

3.14 The terms and conditions specific to the International OSP in Chapter III Clause 4 (sub clause 1 to 2) of the existing guidelines for OSP registration may be continued. Minimal PSTN telecom resources, physically separated with the resources of the OSP, may be permitted at International OSP to address logistics requirements at the OSP centre.

(para 2.63)

3.15 In case the EPABX is installed at a different location, the remote access of CDRs, log of configurations of EPABX, routing tables and logical partitioning should be made available by the OSP at the OSP center. Further, physical access to Data Centre hosting the centralized EPABX and applications may also be provided to DoT/ Security Agencies, if required.

(para 2.72)

3.16 Specific technical provisions for addressing the security and monitoring concerns related to OSPs may be finalized by DoT in consultation with the TEC.

(para 2.73)

3.17 An OSP centre may be extended within the same campus/building under existing OSP registration. At the time of registration/extending the existing OSP, the information about the extended OSP may be uploaded on the DoT portal.

(para 2.77)

3.18 The technical terms and conditions of infrastructure sharing between domestic and international OSP under option 1 and 2 mentioned in Clause 4, Chapter IV of existing terms and conditions for OSP registration may be continued. However, with regard to general conditions of the infrastructure sharing, the provisions related to signing of agreement, bank guarantee and certificate of manufacturer for logical partitioning capability should be removed. The sharing of infrastructure provisions therefore would become co-terminus with the period of registration. Provisions should be made in the portal to fill up the sharing requirement details at the time of applying for registration or at a later stage.

(para 2.87)

3.19 In case of violation of infrastructure sharing conditions, the OSP registration should be cancelled and the OSP company/LLP shall be debarred from taking registration for 3 years. In addition, a financial penalty of Rs. 50 Lakh in case of option 1 and Rs. 1 Crore in case of option 2 may be imposed. In case, the OSP fails to comply to the penalty order, penal action as provided in the Indian Telegraph Act may be initiated in addition to cancellation of registration. These provisions may be incorporated in the registration certificate issued to the OSP.

(para 2.88)

3.20 The provision for distributed architecture of EPABX, as provided in Clause 5 Chapter IV of the existing terms and conditions for registration of OSP, should be continued for the distributed architecture of EPABX, where the EPABX is owned by the OSP.

(para 2.97)

3.21 The Authority recommends that:

(i) The CCSPs/HCCSPs who provide only the platform as service including a combination of the components of EPABX, IVR, call handling/administration, call recording, contact centre data analytics, customer relationship management etc. for contact centres, should be required to get registered with DoT. These CCSPs/HCCSPs should be Indian Company, having their data centre(s) in India for providing the contact centre platform to OSPs. The CCSP/HCCSP should ensure that there is logical partitioning between the components of the platform handling telecom resources of different OSPs. A complete log and record of the logical partitioning including the CDR should be maintained by the CCSP/HCCSP. These records should be maintained at least for a period of one year. The CCSP/HCCSP should provide these records to DoT or security agencies designated by DoT, as and when required. Further, physical access to their data centre(s) should also be provided to DoT/ Security agencies as and when required. For the purpose of registration of CCSP/HCCSP, DoT should create a category similar to OSP registration and complete the registration activity online on the existing web portal. The document requirement should be similar to OSP registration. The CCSP/HCCSP should provide the location wise list of network elements. However, no network diagram should be required. The registration process should be completed in a period of one month similar to OSP registration. There should not be mixing of data and voice path and the CCSP/HCCSP should not infringe upon the scope of authorised TSPs. For any violation to these conditions, a penalty of Rs. 50 lakh per violation may be imposed on the

CCSP/HCCSP. The CCSP/HCCSP should furnish the list of OSPs, served by them, to DoT annually.

(ii) Those CCSPs/HCCSPs who provide the platform as service as mentioned in para (i) above and are also involved in reselling the telecom resources to OSPs, are required to obtain UL-VNO licence, as applicable, from DoT.

(iii) Any Licensed TSP / Unified Licensee having suitable Authorisation should be allowed to function as CCSP/HCCSP.

(iv) The existing CCSPs/HCCSPs may be provided a period of 3 months for getting registration/ suitable license from DoT.

(para 2.107)

3.22 The interconnection of data and voice path is not allowed. However, remote login for equipment maintenance by the OEM or its agent deputed for maintenance may be allowed. The complete details of the incident including the time duration for which the remote login was resorted should be recorded and shared with DoT immediately. Any unauthorised connectivity of data and voice path may be dealt with by cancellation of the registration of the OSP.

(para 2.115)

3.23 The terms and conditions for use of Closed User Group for internal communication of the OSP Company/LLP as mentioned in the Clause 6, Chapter IV of existing terms and conditions for registration of OSP should be continued.

(para 2.120)

3.24 The Work-From-Home (WFH) is an extended agent position of the OSP centre. The requirement of PPVPN for WFH may be removed and the WFH may be connected to OSP centre using any commercially available VPN. However, the provision of prior intimation to DoT with complete address of the WFH location

including static IP address for availing the facility should be continued. The requirement of agreement including the bank guarantee for availing the WHF facility may be removed.

In case of violation of terms and conditions of WFH facility by any agent/employee or by the OSP, the OSP may be subjected to a penalty of Rs 10 lakh per WFH terminal subject to an upper limit of Rs. 1 crore. In case the penalty for violation of Rs. 1 crore is reached, the OSP may be declared as barred for using the WFH facility.

(para 2.127)

3.25 Domestic operation by International OSP may be allowed subject to condition that it is serving the same client. Further, for making domestic calls separate resources may be taken having full separation for serving foreign customers of the client.

(para 2.132)

3.26 EPABX at foreign location in case of international OSP may be allowed subject to the condition that OSP provides remote access of the EPABX and authenticated copy of CDR, System logs and message details as and when required.

(para 2.139)

3.27 The security conditions mentioned in Chapter V of OSP registration guidelines may be continued.

(para 2.145)

3.28 The penalty provisions for violations related to sharing of infrastructure between domestic and international OSPs, interconnection of data and voice path in domestic operations and WFH have already been prescribed in the relevant paras above. Further, the Authority recommends that, for violation of other terms and conditions of registration, penal provisions as per existing terms and conditions for registration of OSP may be continued. The punitive action should be in accordance with the provisions of Indian Telegraph Act.

In case of violation by Captive Contact Centre, the telecom resources of the CCC may be disconnected and the concerned company/LLP may be debarred from having captive contact centre for three years. Further, DoT may take any punitive action in accordance with Indian Telegraph Act.

(para 2.153)

3.29 Interconnectivity between OSP centres serving same client may be permitted with prior intimation to registering authority. However, interconnectivity between domestic and international OSPs not belonging to same company may not be permitted.

(para 2.160)

3.30 The Authority recommends that the miscellaneous provisions in the Chapter VI of the existing guidelines for OSP registration may be continued.

Further, DoT should devise a platform at DoT Headquarter level to address the issues related to interpretation of guidelines to OSPs/CCSPs/HCCSPs/CCCs for appeal against decision of DoT field units.

(para 2.164)

3.31 OSPs having outbound communication facilities should comply with "The Telecom Commercial Communications Customer Preference Regulations, 2018".

(para 2.170)

List of Acronyms

Sl. No.	Abbreviation	Full Form
1.	4G	Fourth Generation
2.	BCP	Business Continuity Planning
3.	BCSP	Business Communications Service Provider
4.	BG	Bank Guarantee
5.	BPO	Business Process Outsourcing
6.	BSO	Basic Service Operator
7.	CCC	Captive Contact Centre
8.	CCSP	Contact Centre Service Providers
9.	CDR	Call Detail Records
10.	CIN	Corporate Identity Number
11.	CLI	Calling Line Identity or Calling Line Identification
12.	CP	Consultation Paper
13.	CRM	Customer Relationship Management
14.	CSP	Communications Service Provider
15.	CUG	Closed User Group
16.	DCC	Domestic Call Centre
17.	DoT	Department of Telecommunications
18.	DR	Disaster Recovery
19.	EPABX	Electronic Private Automatic Branch Exchange
20.	GICS	Global Industry Classification Standard
21.	GMPCS	Global Mobile Personal Communications by Satellite
22.	HCCSP	Hosted Contact Centre Service Providers
23.	ICC	International Call Centre
24.	ILD	International Long Distance
25.	ILL	Internet Leased Line
26.	IP	Internet Protocol
27.	IPLC	International Private Leased Circuit
28.	ISDN	Integrated Services Digital Network
29.	ISP	Internet Service Provider
30.	IVR	Interactive Voice Response
31.	KPO	Knowledge Process Outsourcing
32.	KYC	Know Your Customer
33.	LEA	Lawful Enforcement Agency
34.	LLP	Limited Liability Partnership
35.	LSA	Licensed Service Area
36.	MPLS	Multiprotocol Label Switching
37.	NLD	National Long Distance
38.	NLDO	National Long Distance Operator
39.	NTP99	New Telecom Policy, 1999

40.	O&M	Operation and Maintenance
41.	OEM	Original Equipment Manufacturer
42.	OHD	Open House Discussion
43.	OSP	Other Service Provider
44.	OTT	Over-the-Top
45.	PABX	Private Automatic Branch Exchange
46.	PLMN	Public Land Mobile Network
47.	PoP	Point-of-Presence
48.	PPVPN	Provider Provision Virtual Private Network
49.	PRI	Primary Rate Interface
50.	PSTN	Public Switched Telephone Network
51.	RoC	Registrar of Companies
52.	SEZ	Special Economic Zone
53.	T&C	Terms and Condition
54.	TCCCPR	The Telecom Commercial Communications Customer Preference Regulations
55.	TEC	Telecommunication Engineering Center
56.	TERM	Telecom Enforcement Resource and Monitoring
57.	TRAI	Telecom Regulatory Authority of India
58.	TSP	Telecom Service Provider
59.	UDR	User Data Records
60.	UL	Unified License
61.	VNO	Virtual Network Operator
62.	VoIP	Voice Over Internet Protocol
63.	VPN	Virtual Private Network
64.	WFH	Work From Home
65.	UCC	Unsolicited Commercial Communications