No.:131/TRAI/2017-18/ACTO
Dated: 3rd October, 2017

Shri S. T. Abbas
Advisor (NSL)
Telecom Regulatory Authority of India
Mahanagar Doorsanchar Bhawan
Jawahar Lal Nehru Marg
New Delhi - 110 002

Sub.: ACTO Response to TRAI's Draft Recommendations on Ease of Doing Telecom Business dated 19th September 2017

Ref.: TRAI Paper on Ease of Doing Business in Telecom Sector dated 14th March 2017 & ACTO response No. 127/TRAI/2017-18/ACTO dated 25th April 2017

Dear Sir,

We request reference to the captioned draft recommendations issued by Hon'ble Authority based on the inputs received to its paper dated 14th March 2017.

ACTO has also provided its detailed response by listing fifteen issues for consideration of Hon'ble Authority. However we would like to respectfully submit that none of the issues raised by ACTO were included in the draft recommendations.

We understand that the scope of this TRAI's consultation was to look more into process related issues than those requiring policy intervention. In this regard, we hereby submit three critical issues related to process which are attached as Annexure – I for the kind consideration of the Hon'ble Authority.

We trust that these issues will be duly considered as an important issue in the final recommendations for ease of doing telecom business in India.

Respectfully submitted,

Yours sincerely,

for Association of Competitive Telecom Operator

Tapan K. Patra
Director

Encl: As above

ANNEXURE-I

ACTO Comments on TRAI Draft Recommendations on Ease of Doing Telecom Business

1. **Website Blocking instructions:**

   a) **Technical difficulty in blocking secured "https" URLs:**

   Over the last few years, ISPs have been receiving blocking instructions from DoT regarding "https" (secured sites) & searching key words/contents on websites. Due to the highly encrypted nature of these URLs/websites, these websites cannot be blocked in the same manner as for "http" sites. The encrypted sites require specific decryption key or algorithm of it to be decrypted and then blocked which the ISPs do not possess. There are huge technical limitations for ISPs which include our members as they neither encrypt such sites nor are allowed to undertake deep packet inspection due to privacy issues as stated under the license. The technical complexity relating to "HTTPS" was also explained by industry participants present during the meeting held on August 21, 2012 convened by DoT under the Chairmanship of Former Member (T), Shri JK Roy and other Senior officers of DoT. In fact it was informed by DoT that suitable guidelines on blocking HTTPs websites / URLs will be intimated to the licensed ISPs. However, even after over 5 years now we are yet to receive any guidelines in this regard.

   We request if suitable recommendation on this be issued to ensure a meaningful compliance as of late the number of HTTPs URLs required to be blocked have increased.

   b) **Need For Suitable Guidelines For Retaining Urls On Blocking Tool:**

   - As per the instructions of DoT and other competent authorities, the websites/URLs etc continue to be blocked for unlimited period by ISPs including our members. These are blocked by appropriate tool having storage space limitation beyond a certain size. Currently there is no formal and default requirement under the license to un-block the

websites/ URLs after a certain time period except under a direction from DoT on a case to case basis.

- Over the years this continued blocking of URLs has resulted in the tool getting over burdened with the data generated. This has resulted in impacting the performance of the tool relating to the speed and the functional capacity. There are technical limitations in expanding the capacity beyond a certain limit.

- Unlike the other data retention requirements stated in the license either for commercial records or billing details or logs, there should also be a clear guideline to what period the blocked URLs have to be kept on the tool. From our experience of past couple of years, we have noted that not all URLs instructed to block relate to issue of national security and most of them relate to copyright infringement (movies, brand etc for which ISPs should not be directed for blocking as there are other legal recourses available to the applicant. Especially in case of blocking of movies, it has been observed that the said movie is available for viewing within months on DTH. This makes the applicability of blocking of the movies by and large irrelevant. These should be unblocked accordingly after a specific time period to reduce burden on the blocking tool.

We would therefore humbly request Hon'ble authority to include the following suggestions for your kind consideration and recommendation:

a) Each blocking instruction to have an expiry period. Beyond which the same can be unblocked owing to the technical limitations as stated above. Any further requirement to block can be in the form of a fresh instruction.
b) DoT to consider categorising the blocking instruction based on issues as stated under point 3 as above. The URLs in all the categories can be reviewed periodically and DoT may decide which ones are to be unblocked.
c) The expiry period to be based on achieving the intended objective. For example, if the objectionable post has been removed from the concerned website link, the URL for the same should be allowed to be unblocked. Similarly, if the matter relates to copy right infringement, the sites can be blocked for initial period of 2 -3 months. Once the movie or

content is widely publicized there is no merit in continuing to block the site if the content is freely available elsewhere.

d) As continued block beyond achieving the intended objective makes the purpose infructuous.

2. Simplification of the process on seeking Remote Access (RA) Permissions

The current process of obtaining prior approval for remote access from foreign locations to India locations has proved to be a time consuming matter. There have been continued / inordinate delays in securing approvals. This does not help in efficiently managing the networks, especially in case of disaster or failure of particular RA locations.

In order to continue to comply with the existing requirement of obtaining prior approvals for remote access for foreign locations, we would like to highlight that this has serious and adverse implications for efficient maintenance of telecom networks. In order to provide telecom services, it is imperative that the process be such which is agile and responsive and which enables the telecom service providers to efficiently manage and maintain their networks under all circumstances, especially in those situations where waiting for pre-approvals would hamper and defeat their ability to respond to critical outages and prohibit them to undertake necessary steps to revive their operations and deliver uninterrupted services.

For example, in the current era, cyber security threats have become a serious challenge and these need to be actively prevented and may require the telecom network service provider to leverage capabilities lying outside of its pre-approved RA locations. **The requested flexibility of "intimation" as opposed to "pre-approval" will help the telecom licensees to proactively and reactively mitigate the threats and prevent any such attacks on their network from a new location that may be best suited to undertake requisite preventive and counter measures**.

We recommend the current process of obtaining prior approval of locations be changed to a process of prior-intimation or post-intimation (within a specific time period). The telecom licensees have and will continue to comply with the requirements stated in RA guidelines issued by DoT. The telecom licensees will provide all the information as may be required pertaining to the RA locations. The licensees have made substantial investment in their networks and they should be allowed to legitimately operate it without any overbearing conditions which impair their ability to attend to issues

in a proactive manner. The change in the process requested will provide the much needed operational flexibility to telecom licensees to operate their network and also in. Alternatively a site should be deemed to be approved if there no update is received within 30 days from the date of application.

Remote Access (RA) is crucial part of enterprise data service network as the monitoring and maintenance activity is highly dependent on RA approval. The current process of obtaining prior approval for remote access from foreign locations is very time consuming. There have been continued inordinate delays in securing approvals and in most of the cases, approvals are pending before DoT. While TSP should comply to RA guidelines but current process of obtaining prior approval of locations be changed to a process of prior-intimation or post-intimation.

3. Security Testing of Telecommunication Equipment:

DoT vide its letter dated 31st May 2011 issued an amendment in which it was mandated to have the network elements tested as per Indian or global standard before deploying them in the telecom network. Since the labs were not set up in India the letter stated to get the network elements test in international agency/labs till 31st March 2013. Form 1st April 2013 the network elements need to be tested in the labs in India. Since the labs are not set in India as yet this deadline was kept on being extended till 31.03.2018. It looks current arrangement for having certification from global body is working fine and no major security breach has taken place in telecom sector just due to lack of testing of security element in Network Equipments.

We therefore request to continue with the present arrangement to consider and recognise various industry recognized baseline security practice references for security testing requirement for the induction of the network equipment into the Telecom network by Service providers.

Policies, Standards, Practices, and industry recognized security practice documents include, but are not limited to, the National Institute of Standards and Technology (NIST) Special Publication 800 series; ISO 27002 "Information Technology -- Security Techniques --Information Security

Management Systems"; the Generally Accepted Information Security Principles (GAISP), and the National Reliability and Interoperability Council (NRIC) Best Practices.

The procedural framework to allow industry recognised based line security that are equivalent to or better than security industry best practices, and are tailored to the specific security needs of enterprise network infrastructure.

4. Steps for increasing Foreign capital inflow:

The Finance Minister, in his budget presentation for the Financial Year 2017-18 had announced the closure of the Foreign Investments Promotion Board. We welcome this step taken as it attempts to remove another layer of approvals for the Telecom service License holders. However, though the FIPB stands closed, no transitional framework for replacing the FIPB has been announced by the government as of now. The FDI in Telecom is allowed upto 100 %. We would request the Hon'ble Authority that, for the benefit of the telecom sector, to either allow for automatic route for investments upto 100 %, instead of the present 49 %, in Telecom sector in a process under which the Licensor has only to inform the Nodal Ministry (Department of Telecom) the percentage of Foreign holdings or to have a single window, time bound clearance from the nodal ministry with minimal conditions attached. This will greatly help the Telecom sector to ramp up the foreign holdings and also to invite fresh induction of capital without having to go through long and circuitous processes thereby increasing the chances of boosting the inflow of foreign capital.

****