TV18 Broadcast Limited's ("TV18") preliminary response to TRAI's Consultation Paper on Framework for Technical Compliance of Conditional Access System (CAS) and Subscriber Management Systems (SMS) for Broadcasting & Cable Services dated 22-April-2020

We thank Telecom Regulatory Authority of India ("TRAI") for providing the opportunity to participate on this consultation process regarding Framework for Technical Compliance of Conditional Access System ("CAS") and Subscriber Management Systems ("SMS") for Broadcasting & Cable Services. We hope that the inputs given by us will help and assist TRAI in resolving issues pertaining to CAS and SMS (including their transactional capacity), fingerprinting and watermarking. We appreciate TRAI's efforts to ensure elimination of rampant piracy and under declaration existent on the ground even as on date. Please see below our response on the said consultation paper.

Q1. List all the important features of CAS & SMS to adequately cover all the requirements for Digital Addressable Systems with a focus on the content protection and the factual reporting of subscriptions. Please provide exhaustive list, including the features specified in Schedule III of Telecommunication (Broadcasting and Cable) Services Interconnection (Addressable Systems) Regulations, 2017?

Response: In addition to the mandatory requirements mentioned in Schedule III of the Telecommunication (Broadcasting and Cable) Services Interconnection (Addressable Systems) Regulations, 2017 (as amended) ("Interconnection Regulations"), following features should also be mandated to be available in CAS and SMS with a focus on the content protection and the factual reporting of extent of availability of channels as well as subscriber numbers:

(a) **CAS Requirements:**

(i) Only chipset-based advance embedded CAS should be allowed to be installed by DPOs which is not vulnerable to hacking.

(ii) CAS vendors need to have an original equipment manufacturer (OEM) certification. The certification will help in identifying the OEM and ensure that CAS has been approved pursuant to device verification tests prior to CAS implementation. DPOs should mandatorily insist on successful device verification tests and should get the confirmations of the same directly from OEM of CAS. Such tests / certification should be made available as a part of documentation to Broadcasters, Industry Body, TRAI and Empanelled Auditors, as and when called upon to do so.

(iii) For any new deployment, it should no longer be allowed to use CSA1. All new systems and STBs being deployed must support CSA3 so that over time a migration to CSA3 can be made.

(iv) Over the air ("OTA") upgrading capability.

(v) Next to facilitating OTA firmware upgrades, the CAS system should only be able to install firmware upgrades that have been rolled-out by the CAS vendor. The client devices shall only be able to upgrade to new firmware if the OTA firmware has been signed/certified correctly. Similarly, it should be permissible for DPOs to have upgrades from any entity unless the same has been approved by the CAS vendor.

The CAS system should have a mechanism in place to enforce mandatory installation of firmware upgrades on client devices. This will help in curbing any mischief and in this way, if firmware upgrades somehow are blocked at the subscriber end, then client device ought to lose the possibility to decrypt any channel unless and until the client device has been upgraded to the latest firmware.

The same applies for Viewing Cards in use i.e., it should be possible to securely renew the software on the Viewing Cards and to block working of Viewing Cards for those in respect of which software upgrades have been blocked.

(vi) CAS should detect and record clone / duplicate STBs running in the network of the distributor of television channels and record such instances in non-editable format. Each STB / VC / UA number deployed by distributor of television channels in viewer homes must be unique.

(vii) CAS should maintain ECM logs of communication between CAS and scrambler. ECM logs should contain the historical information regarding creation, modification and deletion of access criteria and information regarding which access criteria is been used for which service in scrambler.

(viii) CAS should maintain EMM logs of communication between CAS and scrambler. EMM logs should contain the historical information regarding creation, modification and deletion of EMM's and historical information regarding its connection and de-connection with different scrambler.

(ix) CAS should record information of source of commands coming into it for each line item of its logs and should have provision to provide all types of logs.

(x) One unique access criteria for each service/channel should be created in CAS. CAS should not allow multiple ECM connection with scrambler using one access criteria. One access criteria should not be get used by the scrambler to scramble multiple services. The above should be implemented since, during audits it has been seen that few DPOs were using the same access criteria that has been created for a Free to Air (FTA) channel to activate multiple pay channels. The authorisation of these multiple channels do not get reflected in the SMS systems which leads to under-declaration of subscriber number to broadcasters.

(xi) In case the distributor of television channels deploys Digital Rights Management system ("DRM") in its IPTV based distribution platform, the DRM should meet all the CAS requirements as per Schedule III including those mentioned herein and those relating to maintaining of all transaction logs and anti-piracy features such as, overt and covert fingerprinting.

We believe that adaptation of above-highlighted important features will ensure integrity of systems, which coupled with requirement to maintain / recordal of all historical changes will ensure that there is no foul play and also ensure accurate determination of subscriber numbers.

(b) **Multiplexer ("MUX") and QAM (Headend Equipment):**

(i) Broadcasters and Auditors should be provided access of validating the MUX configuration during audit. This will enable to check on instances where common access criteria are used for FTA as well as pay channels.

(ii) Multiplexers installed at headend should be able to generate instantaneous logs for all the services configured at the headend including for the historical period.

(iii) MUX should be BIS approved to avoid sub-standard MUX to be used which are not compliant with regulatory requirements.

(iv) The logs of the Network Service Manager controlling the compression chain of all encoders and all MUX and the MUX logs must be maintained with details of audio video PID mapping, service IDs, service names, and all information related to the services and encryption. The DPOs shall provide recording of all the Transport Stream ("**TS**") being distributed from its headends on request by the broadcaster.

(v) Encryption of all channels distributed by DPOs must be implemented only by the CAS on the MUX and not on any other device of the Headend.

(vi) DPOs shall not retransmit any transport stream, or any blank LCN in the Transport Stream in an unencrypted manner. Further, all frequencies including those containing channels in the entire network should have end-to-end encryption i.e., they should originate from the headend and end at subscriber's STB, solely in encrypted form. DPOs should not permit any of its LCOs to add any channel or content in transport stream, or any blank LCN or any frequency.

(c) **Integration of SMS and CAS:** Package creation, deletion, modification / editing in CAS should be done through command of SMS only and not separately in SMS and CAS. Further, CAS and SMS should able to handle, in a-la-carte mode, all the channels distributed by DPOs. This will ensure that there is no mismatch of package composition between CAS and SMS. It is being observed that due to lack of clarity in this regard in the existing provisions of Schedule III unscrupulous DPOs use the same for camouflaging data. For example, DPOs may create a pack contain 110 channels in CAS, while in SMS the pack is created in such a manner that only 100 channels are shown, resultantly, in the reports generated from SMS only 100 channels get reflected in such pack thereby masking the 10 channels which are present in CAS and are otherwise being made available to subscribers. In is noteworthy that broadcasters are paid on the basis of reports generated from SMS, hence, such instances lead to underreporting of subscribers and extent of channel availability by DPOs. Further, CAS vendors ought to certify that no access / login IDs / user interface / application(s) have been provided to DPOs that may in any manner whatsoever compromise integrity of CAS inter-alia by providing ability to execute any commands including but not limited to activation / de-activation, package creation / modification / deletion, etc. directly from the CAS by bypassing the SMS.

The CAS and SMS should be able to tag and blacklist VC numbers and STB numbers that have been involved in piracy in the past to ensure that such VCs and STBs cannot be re-deployed.

We also submit that the prescribed format under the Interconnection Regulations for submitting monthly subscriber reports should be modified in such a manner that the reporting DPO is required to report number of subscribers from both CAS and SMS separately in every report. For example – active subscriber numbers as per CAS vis-à-vis active subscriber numbers as per SMS at the same point in time separately on a-la-carte as well as on bouquet basis, and on a consolidated / aggregate basis.

(d) **Reports from CAS and SMS:** The CAS and SMS shall be capable of generating the reports as mentioned herein below, in addition to the existing provision contained in Schedule III of Interconnection Regulations.

(i) All reports in SMS and CAS should be available from front end Graphic User Interface (GUI) as well as back end query (through script).

(ii) It is submitted that with an aim to discourage any attempt of DPOs to remove critical information, logs, data from their CAS & SMS ("Logs / Data") under one pretext or the other to avoid determination of actual subscriber numbers and to overcome issues relating to unavailability of data / records on grounds such as, technical glitches in systems / crashed of systems, etc.**)**, it is suggested that it should not be possible for any person (including DPOs) to alter Logs / Data in any manner whatsoever. In this regard, Logs / Data should be saved on a real-time basis using hashing or similar encryption mechanism to ensure its integrity. Further, Logs / Data along with their backup should be also be stored on live data servers of reputed third parties as may have been approved by Industry Body in consultation with prominent CAS and SMS vendors. Submissions regarding formation of Industry Body have been made subsequently in this document. Such online storing of Logs / Data on live data servers can also act as disaster recovery (DR) site for concerned stakeholders. The auditors conducting audits of DPOs can also be called upon to ascertain whether there are any discrepancies in online stored Logs / Data vis-à-vis those maintained by DPOs.

(iii) The CAS and SMS should be capable of generating below reports, at any desired time about:

A. Package creation history and logs with date/time / user stamp. Logs should contain at least SMS Package ID, CAS Package ID, Package Name, Channels in package.

B. Package modification history and logs with changes and date / time / user stamp

(iv) Additionally, CAS should also be capable of generating reports, at any desired time about:

A. The total number of registered subscribers.

B. The total number of active subscribers with package / channel assigned.

C. The total number of temporary suspended subscribers.

D. The total number of deactivated subscribers with last package / channel deactivated.

E. List of blacklisted VCs / STBs in the system.

F. The names of the channels forming part of each bouquet.

G. The name of a-la-carte channels and bouquets subscribed by a subscriber.

(e) **Accurate subscriber information to be captured in SMS** : Although, it is mandated in Interconnection Regulations that SMS should capture all critical information about subscriber before activation, it is observed that some DPOs are not capturing complete/accurate information of subscribers in Consumer Application Form (CAF) and as a result, dummy details are captured in SMS.

In view of the above, it is proposed that DPOs should ensure that correct and complete information is updated in the system to identify the subscribers. It is also observed that at many instances activation / deactivations are done by MSOs on basis of request from LCOs, hence a strong and robust mechanism needs to be built so as to ensure that only those subscribes are activated, whose complete details are being captured in the SMS. In this regard, we also propose for KYC of consumers and verification of details by DPO. The validation process for activation of a DPO's STB at the premises of a subscribers, may include at least a three tier validation process wherein three different OTPs shall get generated and transmitted – one to the STB via b-mail (which can be viewed on television screen connected to the STB), one to the subscriber's registered mobile number, and one to the mobile number of DPO's engineer / technician who visits to install and activate the STB. The STB shall only be activated with combination of these three OTPs.

(f) **EPG:** DPO shall mandatorily provide program information on the EPG. The EPG banner should be designed in such a manner that it is able to display current date, time, LCN number, name of channel, name of DPO or logo of DPO as mandatory information at all times. It has been observed that at many instances, DPOs are not providing program information on EPG which deprives subscribers of upcoming program information. This feature is also required for identifying the source DPO during audits and anti-piracy actions.

(g) **Anti-Piracy provisions:**

(i) Fingerprint and network watermark compliance: The current provisions of Schedule III of Interconnection Regulations provide for system capability to provide fingerprinting and network watermark. However, it does not provide for implementational aspect of these features. Hence, we submit the following to ensure that fingerprinting and network watermark are effectively implemented at ground level by DPOs.

A. Strong compliance should be ensured for implementing fingerprint scheduled across all STBs / Channels with fix intervals. Ideally, it should not be beyond an interval of more than 5-7 minutes.

B. Scheduled fingerprint should be random on screen and font size should be easily readable.

C. Insertion of network watermark at headend level (video level) only should be mandated.

D. Provisioning for forensic watermarking / fingerprinting should also be mandated.

E. Forensic watermarking should be mandatory for IPTV Headends to trace back the pirated content to specific individuals who illegally redistribute the content and to take action against the individual (including switching off their account).

(ii) For STBs with Recording Facility (copy-protect and non-transferable):

A. Content of the channel should get recorded and should not playout if the particular channel has not been subscribed to or for that matter if such channel and/or STB is deactivated due to any reason.

B. Content should get recorded along with fingerprinting / watermarking / scroll messaging and recorded content should display live fingerprinting / scroll message during play out. This will help in identifying the STB if recorded content is used for piracy.

C. Recorded content should be encrypted and should only play in the STB on which it is recorded and should not be able to be played/viewed through any other device. This will ensure that recorded content is not misused for unauthorized distribution / piracy.

(iii) DPOs to provide STB and viewing card information in STB user settings menus on a mandatory basis with current date, time and DPO's name/logo as mandatory information at all times. This information is essential to assist effective subscription audits and anti-piracy ground action.

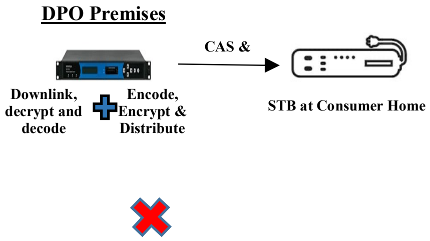
(iv) It should be mandatory for DPOs to share subscriber's verifiable details along with a copy of CAF in respect of those subscribers whose STBs have been found to have been used for piracy of signals. This is necessary so that detailed investigations can be made against erring persons / entities and appropriate legal action is initiated.

(v) Piracy is a big challenge, and pirated content appears online much faster than ever before due to easy availability of highspeed broadband connectivity. Worldwide loss of revenue for TV episodes & Movies due to piracy is being estimated to reach USD 52 billion by 2022[1]. We suggest TRAI should enable industry stakeholders to come together and form an industry body that includes trained investigators, legal and law enforcement representatives, cryptography analysists, network and system security auditors, representatives from major DPOs and broadcasters ("Industry Body"). In regard, kindly also refer to our suggestions regarding additional functions of the Industry Body including those in response to Question 5 (below). It is further submitted that depending on success of work and efforts of such Industry Body, decision by stakeholders can be taken regarding permanency of such industry body. The Industry Body can also be *inter-alia* tasked to generate awareness amongst small DPOs and LCOs on issues relating to piracy and content theft, put in concerted effort to detect and tackle piracy of content, and detect the breaches on the operator's network and suggest remedial action. Few types of piracy are being illustrated below for ease of reference, which can be brought within the purview of anti-piracy center:

[1] www.statista.com

A. **Unencrypted feed**:

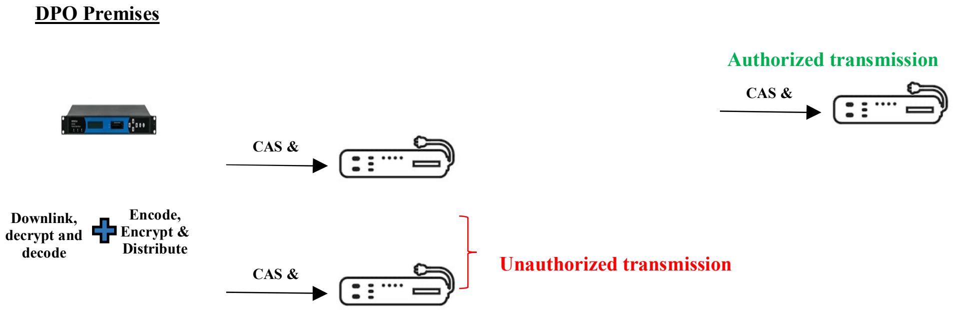
An authorized DPO distributes a broadcaster's channel to its subscribers in an unencrypted form thereby, violating Interconnection Regulations. As per, Interconnection Regulations, a cable operator is bound by law to distribute channels in encrypted form only which ensures correctness / transparency in number of subscribers viewing a channel.



When a channel is distributed in unencrypted form, the number of subscribers receiving such channel will not be reflected in the CAS and SMS system of the DPO. As a result, such subscribers will not be reported by the DPO to the broadcaster, amounting to under-declaration which cannot be identified through audits. The under-declaration not only impacts the broadcasters as it also causes losses to public exchequer in the form of lost taxes.

B. **Multiple SMS systems/ Undisclosed CAS**

In some cases, it has been observed that a DPO uses multiple CAS/SMS systems to activate channels on a subscriber's STB. However, the DPO does not declare the number of subscribers on all the said SMS/CAS.


DPO Premises
Authorized transmission
CAS &
CAS &
Downlink, decrypt and decode
Encode, Encrypt & Distribute
Unauthorized transmission
CAS &

This again amounts to under-declaration which cannot be identified through audits and results in tax evasion and non-payment to the broadcaster.

C. **<u>Same Channel on multiple Logical Channel Number (LCN):</u>**

At the time of retransmission of channels, some DPOs resort to leaving certain LCNs blank so that the same may be used by LCOs for transmitting their local channels. However, at times, it has been observed that some LCOs, use those blank LCNs for retransmitting un-encrypted feeds of pay channels of broadcasters. Such un-encrypted retransmission of channel does not get captured in the SMS report generated at the MSOs' end, thereby leading to under-declaration of subscriber numbers to broadcaster even though the relevant pay channel may be available to complete subscriber base being catered through such LCO. This amounts to violation of provisions of TRAI's Interconnection Regulations for retransmission of a channel on more than one LCN and also for retransmission of a channel in an un-encrypted manner. It may further be noted that revenue loss for broadcasters also hurts the exchequer by way of loss of tax collection.

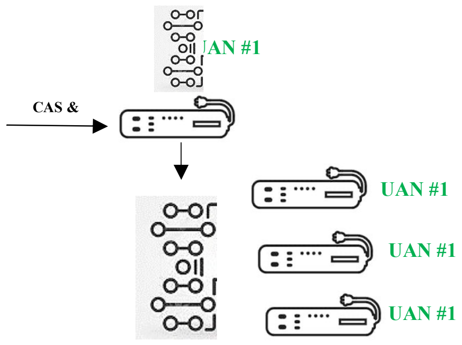
D. **<u>Illicit Set Top Box (STB):</u>**

As per Interconnection Regulations all the channels retransmitted by DPOs be it registered as Pay or FTA with the MIB, should be encrypted and received by the subscribers only through the DPO's STB.

However, it is observed that certain illicit FTA STBs are available for sale in the open market. These STBs allow decryption of encrypted channels of the DPO by extracting “decryption keys” from legitimate STBs of the DPOs. The keys are updated on servers and delivered through internet to the illicit FTA STBs. This amounts to misuse / hacking of an STB and thereby causing piracy of the broadcaster’s channels as extraction of decryption keys thereby compromising DPO’s CAS system or STBs. Currently, DPOs do not take any proactive action to prevent or resolve such illegitimate extraction of encryption keys. Example – “Pagaria 6060”, Pagaria being the brand name of a STB.

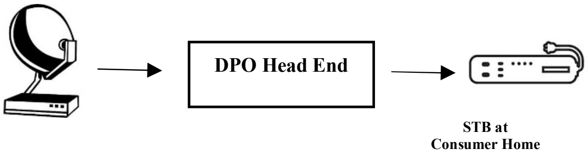
E. **<u>Cloning:</u>**

Every STB distributed by the DPO needs to have a Unique ID. A card-less STB’s Unique ID is its Unique Authorization Number (UAN). A UAN can represent only one STB /subscriber. Cable piracy through cloning occurs when one UAN representing one STB/subscriber is duplicated across multiple STBs/subscribers. This form of piracy results in activation of multiple STBs / subscribers, all tagged to a single subscriber /STB thus, leading to piracy and under-declaration.



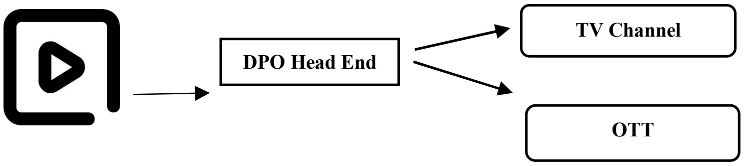
F. Use of DTH / IPTV STBs for Cable redistribution:

As per Interconnection Regulations, TV channels distributed by authorized DPOs cannot be redistributed by other unauthorized DPOs. However, due to lack of standardization on insertion of the DPOs Watermark, or compromise of the DPOs' STB, such instances of unauthorized redistribution of channels has been detected. This amounts to piracy of broadcaster's channels by the DPOs leading to undeclaration of subscriber number and revenue.



DPOs/LCOs use DTH STBs at times to retransmit Pay Broadcaster channels on their network, this generally occurs when a broadcaster shuts down signals of its channels to a DPO due to non-payment of dues. The defaulting DPO or its LCO, instead of paying the broadcaster pending dues arranges 10-15 DTH STBs and uses them to retransmit the signals of those services that are shut down.

G. Use of OTT streams for Cable redistribution:



As per Interconnection Regulations, DPOs are required to redistribute the broadcaster's channels which are authorized by the broadcaster. However, there are instances when the OTT streams are redistributed on the Platforms illegally. This amounts to piracy and under-declaration by the DPOs.

H. **Unauthorized sharing of broadcaster's signals:**

This generally occurs when a broadcaster shuts down signals of its channels to a DPO due to say, non-payment of dues. The defaulting 'DPO A', instead of paying the broadcaster pending dues colludes with another 'DPO B' to unauthorizedly transmit the signals of a channel.

DPO A, thus continues to offer the broadcaster's channels through DPO B in an unauthorized manner to its subscribers in either of the following ways:

(i) DPO B distributes a broadcaster channel without authorization to DPO A's subscribers by replacing the broadcaster's IRD at DPO A's headend with its own set top box. Therefore, DPO A, despite defaulting on payments and signals being shut down by the broadcaster, can now distribute such broadcaster's channels to its subscribers; or

(ii) DPO B distributes a broadcaster channel without authorization to DPO A's subscribers by feeding the broadcaster's channels from the IRDs_installed at DPO B; or

(iii) Defaulting DPO A gives control of its CAS system to DPO B and DPO B simulcrypts both CAS systems (CASA and CAS B) at its Headend/network. Now the signal from DPO B will go into two different STBs that belong to DPO A and DPO B.

These are a few ways, the defaulting DPO continues to enjoy the signals without clearing dues to relevant broadcasters.

Q2. As per audit procedure (in compliance with Schedule III), a certificate from CAS / SMS vendor suffices to confirm the compliance. Do you think that all the CAS & SMS comply with the requisite features as enumerated in question 1 above? If not, what additional checks or compliance measures are required to improve the compliance of CAS/SMS?

Response: It is observed that, although SMS and CAS vendors are providing the certificate showing compliance as per the Interconnection Regulations, but at many instances it has been discovered that SMS/CAS are not in compliance with the regulatory stipulations or for that matter not even at par with industry standards. Hence, only certification from SMS and CAS vendor does not suffice to confirm the compliances. We submit that our response to Q1 should be referred for the additional checks required to ensure the compliance of CAS/SMS as per Interconnection Regulations.

Q3. Do you consider that there is a need to define a framework for CAS/ SMS systems to benchmark the minimum requirements of the system before these can be deployed by any DPO in India?

Response: Yes, a standardized framework is required for CAS/SMS systems to benchmark the minimum requirements of the systems before it can be deployed by any DPO in India. Unsecured CAS/SMS system may lead to theft of broadcaster's content and cause loss to public exchequer. Substandard CAS/SMS system also impacts the performance of STBs thereby leading to unnecessary harassment of end users.

Q4. What safeguards are necessary so that consumers as well as other stakeholders do not suffer for want of regular upgrade/ configuration by CAS/ SMS vendors?

Response:

(a) It should be obligatory for CAS and SMS vendors to ensure their systems are always in compliance with regulatory requirements. This can be ensured to make it mandatory to CAS and SMS vendors to regularly upgrade / configuration to ensure that the systems are in compliance.

(b) To ensure that vendors do not resort to charging exorbitant prices for pricing security updates, it should be mandatory that such updates should be provided without any additional fees to be payable by DPOs. Charges towards regular updates should be included in the original / annual costs payable by DPOs. Any exceptional situation / circumstance warranting payment of additional costs by DPOs, can be pre-approved by TRAI.

(c) To ensure that CAS and SMS vendors do not take their obligations lightly, it is suggested that punitive penalties (including blacklisting) is imposed on any vendor found to be flouting regulatory compliances. It is submitted that not fixing errors within prescribed or reasonable timelines should lead to imposition of penalties.

(d) All CAS companies should declare the CAS IDs with which they are operating in India. They should also update the IDs as and when they change it.

Q5. (a) Who should be entrusted with the task of defining the framework for CAS & SMS in India? Justify your choice with reasons thereof. Describe the structure and functioning procedure of such entrusted entity. (b) What should be the mechanism/ structure, so as to ensure that stakeholders engage actively in the decision-making process for making test specifications / procedures? Support your response with any existing model adapted in India or globally.

Response: It is submitted and reiterated that Industry Body comprising of stakeholders from every level of the value chain (i.e., CAS Vendors, SMS Vendors, DPOs, Broadcasters, etc.) should be entrusted with the task of defining the framework for CAS and SMS in India and that an industry-led body is best suited solution that ought to be considered for the same. The Industry Body, thus, incorporated should take into consideration the framework adopted worldwide such as Movie Labs, IBCAP, DVB, etc. while defining the framework for India. However, it is necessary that DPOs as well as CAS and SMS vendors are made amenable to the Industry Body. In this regard, requirements such as, mandating CAS and SMS vendors to register as other service providers should be introduced. Further, registration of DPOs as well as CAS and SMS vendors ought to have mandatory pre-conditions such as:

(a) they will mandatorily register themselves with Industry Body and render all such assistances as may be necessary in furtherance of Industry Body's mandate or as may be prescribed by TRAI from time to time,

(b) they will ensure that systems supplied by them to DPOs are in continued compliance with provisions of TRAI's Interconnection Regulations and the Telecommunication (Broadcasting and Cable) Services Standards of Quality of Service and Consumer Protection (Addressable Systems) Regulations 2017 (as amended) ("QOS Regulations"),

(c) they will report agreements with DPOs to TRAI as well as Industry Body, and

(d) they will report all instances of detection of bugs, hacking attempts (successful or not), system breaches, etc. in the system, whether on account of actions / omissions of DPOs or otherwise, to TRAI as well as Industry Body without any undue delays.

Q6. Once the technical framework for CAS & SMS is developed, please suggest a suitable model for compliance mechanism. a) Should there be a designated agency to carry out the testing and certification to ensure compliance to such framework? Or alternatively should the work of testing and certification be entrusted with accredited testing labs empanelled by the standards making agency/ government? Please provide detailed suggestion including the benefits and limitations (if any) of the suggested model. (b) What precaution should be taken at the planning stage for smooth implementation of standardization and certification of CAS and SMS in Indian market? Do you foresee any challenges in implementation? (c) What should be the oversight mechanism to ensure continued compliance? Please provide your comments with reasoning sharing the national/ international best practices.

Response: Independent and accredited testing labs should be entrusted with the certification of the vendors. Companies like Cartesian have proven to be very capable of auditing CAS systems and might be interested to also run a certification scheme for the TRAI. Such testing labs can work exclusively with Industry Body.

Further, introducing standardization and certification into an existing business may be challenging therefore, a lead time may be considered depending on inputs from concerned stakeholders. Easiest and most efficient way of introducing is to make it obligatory for new to be deployed set top boxes and gradual phasing out existing set top boxes.

Q7. Once a new framework is established, what should be the mechanism to ensure that all CAS/ SMS comply with the specifications? Should existing and deployed CAS/ SMS systems be mandated to conform to the framework? If yes please suggest the timelines. If no, how will the level playing field and assurance of common minimum framework be achieved?

Response: Once new framework is established; it should be mandated that all DPOs as well as CAS and SMS vendors should ensure that all CAS and SMS deployed by them should conform to new guidelines and get certified through Industry Body. Existing deployed CAS and SMS should be mandated to upgrade to new framework in timely manner (between 6-12 months' time). An audit should be conducted to ensure and ascertain proper and complete implementation of all features and functionalities as per new guidelines and framework.

Q8. Do you think standardization and certification of CAS and SMS will bring economic efficiency, improve quality of service and improve end-consumer experience? Kindly provide detailed comments.

Response: We believe that standardisation and certification in CAS and SMS is critical for the industry. It will definitely help in developing transparency and trust between different stakeholders. It will also promote factual and correct reporting thereby, eliminating chances any disturbance to end-consumer experience. Standardization and certification of CAS and SMS will help in secured transmission of television signal that will benefit all the stakeholders in the value chain.

Q9. Any other issue relevant to the present consultation.

Response:

(a) DPO should mandatorily provide digital payment options by Subscribers towards monthly subscription and mode of payments should be widely published by DPO. It will bring more transparency in subscription process and reduce the loss to broadcasters as well as government for GST.

(b) We suggest provision for taking strict actions shall be specified, in case of systems are not robust, systems are unable to generate historical data, systems are not in compliance of Interconnection Regulations and QOS Regulations.

(c) A common portal should also be developed and maintained containing updates regarding history of all instances of detection of bugs, hacking attempts (successful or not), system breaches, etc. whether on account of actions / omissions of DPOs or otherwise. The portal should also enlist the corrective measures taken by CAS/SMS vendors to avoid the same in future.

(d) DPO should designate dedicated phone numbers and email ids inter-alia for reporting of piracy instances and other critical instances. This information should be shared with broadcasters to report the piracy and should also be published on the website of DPOs. This will ensure swift reporting of piracy and other critical instances and will also help in effectively curbing the same. Timely actions are important in minimizing the extent of losses due to piracy.