TO BE PUBLISHED IN THE GAZETTE OF INDIA, EXTRAORDINARY,
PART III, SECTION 4
TELECOM REGULATORY AUTHORITY OF INDIA
NOTIFICATION

THE TELECOMMUNICATION (BROADCASTING AND CABLE) SERVICES INTERCONNECTION (ADDRESSABLE SYSTEMS) (FIFTH AMENDMENT) REGULATIONS, 2023
(4 of 2023)

New Delhi, 14/09/2023

F. No. C-1/2/(1)/2021-B AND CS(2) — In exercise of the powers conferred by section 36, read with sub-clauses (ii), (iii) and (iv) of clause (b) of sub-section (1) of section 11, of the Telecom Regulatory Authority of India Act, 1997 (24 of 1997), read with notification of the Central Government, in the Ministry of Communication and Information Technology (Department of Telecommunications), No. 39, —

(a) issued, in exercise of the powers conferred upon the Central Government under clause (d) of sub-section (1) of section 11 and proviso to clause (k) of sub-section (1) of section 2 of the said Act, and

(b) published under notification No. S.O.44 (E) and 45 (E) dated the 9th January, 2004 in the Gazette of India, Extraordinary, Part II, Section 3,—

the Telecom Regulatory Authority of India hereby makes the following regulations further to amend the Telecommunication (Broadcasting and Cable) Services Interconnection (Addressable Systems) Regulations, 2017 (1 of 2017), namely:-

1. Short title, extent, and commencement.—

(1) These regulations may be called the Telecommunication (Broadcasting and Cable) Services Interconnection (Addressable Systems) (Fifth Amendment) Regulations, 2023 (4 of 2023).

(2) These regulations shall apply throughout the territory of India.

(3) These regulations shall come into force from the date of their publication in the Official Gazette.

Provided that for the existing systems, the provisions of these regulations shall apply after three months from the date of their coming into force.

2. In regulation 10 of the Telecommunication (Broadcasting and Cable) Services Interconnection (Addressable Systems) Regulations, 2017 (hereinafter referred to as the "principal regulations"),—

(a) in sub-regulation (6), after the words "Schedule III", the words "or the Schedule X or both, as the case may be" shall be inserted;

(b) in sub-regulation (7), for the words "Schedule III", the words "Schedule III or the Schedule X or both, as the case may be" shall be substituted;

(c) in proviso to sub-regulation (7), after the words "Schedule III", the words "or the Schedule X or both, as the case may be" shall be inserted.

3. In regulation 15 of the principal regulations,—

(a) in sub-regulation (2), for the words "Schedule III", the words "Schedule III or the Schedule X or both, as the case may be" shall be substituted;

(b) in third proviso to sub-regulation (2), after the words "Schedule III", the words "or the Schedule X or both, as the case may be" shall be inserted.

4. In Schedule II of the principal regulations,—

(a) in item 17, for the words "Schedule III", the words "Schedule III or the Schedule X or both, as the case may be," shall be substituted;

(b) in declaration, for the words "Schedule III", the words "Schedule III or the Schedule X or both, as the case may be," shall be substituted.

5. After Schedule IX to the principal regulations, the following schedule shall be inserted, namely:-

"Schedule X

(Refer sub-regulation (6) of the regulation 10, sub-regulation (7) of the regulation 10 and sub-regulation (2) of the regulation 15)

Scope and Scheduling of Audit

(A) Scope: The annual Audit caused by distributor shall include the Audit to validate compliance with this Schedule and the Subscription Audit, as provided for in these regulations.

(B) Scheduling: The annual Audit as caused by distributor under regulation 15(1) shall be scheduled in such a manner that there is a gap of at-least six months between the audits of two consecutive calendar years. Further, there should not be a gap of more than 18 months between audits of two consecutive calendar years.

Digital Rights Management (DRM) System Requirements

The term DRM, herein, refers to the management of the encryption systems for, *inter-alia*, providing the functionality of CAS for the Internet Protocol Television (IPTV) service provider under these regulations.

(C) DRM Requirements in so far as they relate to subscriber management systems (SMS) for IPTV services:

Table 1

Sl. No.	Proposed DRM requirements for SMS
1.	There shall not be any data mismatch between DRM and SMS. Maximum mismatch based on subscription base may be allowed as mentioned below:

	(1) Must be less than 0.20% for subscriber base up to 100000 subs (0 to 200 for subscriber base of up to 100000) (2) Must be less than 0.04% for subscriber base up to 1000000 subscribers (0 to 400 for subscriber base of up to 1000000) (3) Must be less than 0.01% for subscriber base above 10000000 subscribers (0 to 1000 for subscriber base of up to 10000000) The data between both the systems shall be reconciled on a monthly basis. The reconciliation report shall be stored along with the system data for a minimum of three (3) years or at least three audit cycles, or as per Schedule III whichever is later.
2.	**Password Policy Creation for Users**: SMS shall have a defined password policy, with minimum length criteria and composition (upper and lower-case characters, numeric, alphabets or special characters), forced password changes or any other appropriate mechanisms or combinations thereof or alternatively user account has to be locked/paired to the Mac Id of the set top box (STB) /unique consumer subscription or the customer premises equipment (CPE)/device.
3.	**After-Sales Service Support**: The required software and hardware support should be available to the distributor of the television channels' installations from the SMS vendor's support teams located in India. The support should be such as to ensure the SMS system with 99.99% uptime and availability. The systems should have sufficient provisions for backup systems to ensure quality of service and uptime
4.	All activation and deactivation of STBs/unique consumer subscription shall be done in such a way that SMS and DRM are always integrated and synchronised on real time basis.
5.	Necessary and sufficient methods shall be put in place so that each activation and deactivation of STBs/unique consumer subscription is reflected in the reports generated from the SMS integrated with the DRM and *vice versa*
6.	DRM and SMS should be able to activate or deactivate services and/or STBs/unique consumer subscription of the subscriber base of the distributor within 24 hours.
7.	The SMS shall be independently capable of generating, recording, and maintaining logs, for the period of at least immediately preceding three (3) consecutive years, corresponding to each command executed in the SMS including but not limited to activation and deactivation commands.
8.	The SMS should be computerized and capable of recording all logs including information and data concerning the subscribers such as: (a) Unique customer identification (ID) (b) Subscription contract number (c) Name of the subscriber (d) Billing address (e) Installation address (f) Landline telephone number (g) Mobile telephone number (h) E-mail address (i) Channels, bouquets and services subscribed (j) Unique STB number/unique consumer subscription ID attached to a specific unique MAC ID. (k) Unique VC number or MAC ID.
9.	The SMS should be capable of: (a) Viewing and printing of historical data in terms of the activations and the deactivations of STBs/unique consumer subscription.

	(b) Locating each and every STB/unique consumer subscription and VC/MAC ID installed at city and state level. (c) Generating historical data of changes in the subscriptions for each subscriber and the corresponding source of requests made by the subscriber.
10.	The SMS should be capable of generating reports, at any desired time including about: (a) The total number of registered subscribers. (b) The total number of active subscribers. (c) The total number of temporary suspended subscribers. (d) The total number of deactivated subscribers. (e) List of blacklisted STBs/unique consumer subscription in the system. (f) Channel and bouquet wise monthly subscription report in the prescribed format. (g) The names of the channels forming part of each bouquet. (h) The total number of active subscribers subscribing to a particular channel or bouquet at a given time. (i) The name of a-la carte channel and bouquet subscribed by a subscriber. (j) The ageing report for subscription of a particular channel or bouquet.
11.	The distributor shall ensure that the SMS vendor has the technical capability in India to maintain the systems on 24×7 basis throughout the year.
12.	DPO shall declare the details of the DRM and the SMS deployed for distribution of channels. In case of deployment of any additional DRM/SMS, the same shall be notified prior to commissioning of the system, to the broadcasters by the distributor.
13.	If there is active infrastructure sharing (as and when permitted by MIB) then, DPO shall declare the sharing of the DRM and the SMS deployed for distribution of channels. In case of deployment of any additional DRM/SMS, the same should be notified to the broadcasters by the distributor.
14.	SMS shall have a provision to generate synchronization report, with date and time, with the minimum fields as listed below: (a) STB/unique consumer subscription Number (or in case of card-less system, chip ID or MAC ID number of the STB) (b) Product Code pertaining to à-la-carte channels and bouquets available on the platform (c) Start Date of entitlement (d) End Date of entitlement (e) Status of STB/unique consumer subscription (active/Inactive)
15.	The file output of DRM shall be processed by SMS system to compare and generate a 100% match or mismatch error report.
16.	**Channel/Bouquet management**: SMS shall, in synchronisation with DRM on real time basis, support the following essential requirements: (a) Create and manage relevant product ID for all channels and bouquets along with the relevant details such as name, tariff, broadcaster, or DPO bouquet, etc. (b) Manage changes in the channel/bouquet, as may be required, from time to time. (c) Link the Products IDs for à-la-carte channels and bouquets (Single and Bulk) created in DRM with the product information being managed in SMS, for smooth working of SMS and DRM integration. (d) Management of historical Data of Product name, i.e., Broadcasters (name), maximum retail price (MRP), distributor retail price (DRP).
17.	**Network Capacity Fee (NCF) Policy Creation**: SMS shall support all NCF related requirements mandated by the applicable tariff order.

18.	**Bill/Invoice Generation**: SMS shall be capable of generating proper subscriber bill/invoice with explicit details of NCF charges, pay channels charges (with clear itemized details of à-la-carte channel cost and bouquet costs), rental charges for STB/unique consumer subscription (if any), other applicable charges, including Goods and Services Tax (GST).
19.	**Management of Logs**: (a) SMS shall have the facility to provide user detail logs with the ID of users on each login event. (b) SMS shall have the provision of generating the user activity log report to enable tracking users' work history. It shall not be allowed to delete the records from the log. (c) All logs shall be stamped with date and time and the system shall not allow altering or modifying any logs. (d) The logs shall be maintained for a period as specified in Schedule III or at least three audit cycles, whichever is later. (e) Channel subscription report: SMS shall be able to provide broadcaster wise total counts of monthly subscribers of channels including both à la carte and bouquet subscriptions as per format that may be prescribed by TRAI. (f) DRM and SMS should be running on separate and independent servers.
20.	**SMS Database and tables**: (a) There shall not be any active unique subscriber outside the database tables declared by the Vendor (b) SMS shall not provide an option to split SMS database or for creation of more than one instance. (c) SMS shall have the provision to enable or disable channel (à-la-carte channel or bouquet of channels) selection by subscribers either through website or an application through interface provided by the distributor platform operator. (d) SMS shall be capable of capturing the following information required for audit or otherwise: i. Bouquet à la carte status change history ii. Bouquet composition change history iii. Change in status of connection (primary to secondary and vice versa)
21.	SMS shall be accessed through a Firewall
22.	STB/unique consumer subscription and MAC ID shall be paired from the SMS to ensure security of channel (applicable for DRM with pairing facility).
23.	The SMS shall be capable of individually addressing subscribers, for the purpose of generating the reports, on channel by channel and STB/unique consumer subscription by STB/unique consumer subscription basis.
24.	SMS should have a facility to carry out monthly reconciliations of channels/a-la-carte and bouquet (with their respective ID created in SMS with DRM) and the variance report should be available from the DRM and SMS logs and made available during audits.
25.	SMS should have a provision of generating the following reports pertaining to STB/unique consumer subscription/MAC ID.: (a) White list of STB/unique consumer subscription /MAC ID along with active/inactive status (b) Faulty STB/unique consumer subscription/MAC ID – repairable and beyond repairable

	(c) Warehouse fresh stock (d) In stock at local cable operator (LCO) end (e) Blacklist (f) Deployed with activation status (g) Testing/demonstration STB/unique consumer subscription /MAC ID with location
26.	**Audit-related requirements**: SMS should have the capability to capture below-mentioned information that may be required for audit and otherwise: (a) Subscriber related: (i) Subscriber contact details change history (ii) Connection count history (iii) Transition of connection between Disconnected/Active/Temporary Disconnected (iv) Subscription change history (b) Product (Bouquet/à-la-carte channel) related: (i) Broadcaster à-la-carte relation (ii) Bouquet name change history (iii) À la carte name change history (iv) Bouquet/à-la-carte channel rate change history (c) STB/unique consumer subscription related: (i) Change in location history (ii) Change in status (Active/Damaged/Repaired/Replaced)
27.	**User Authentication**: SMS should have the capability to authenticate its subscribers through registered mobile number (RMN) through one-time password (OTP) system
28.	SMS should have the provision to support the following additional requirements: (a) List of à-la-carte channels and bouquets, digital headend (DHE): Provision to support/ Sub-Headend-wise list of à-la-carte channels and bouquets, in sync with the list available in DRM. (b) Product (à-la-carte channels and bouquets)-wise Renewal and Reversal setting for the Subscriber Account: Provision to allow renewal of a product to a subscriber after the expiry date of a product, and provision to auto-calculate and refund the amount to a subscriber if he discontinues a product midterm. These requirements may be configurable on selective products, as required by the DPOs as per their business plans. (c) Product (à-la-carte channels and bouquets)-wise Reversal setting for LCO Account: Provision to calculate and refund the amount due to LCO, if he or the subscriber discontinues a product midterm. Product (à-la-carte channels and bouquets) Tenure-wise LCO and Subscriber Discount Scheme/Free Days Scheme: Provision to create Discount Scheme and Free-day scheme for LCO and Subscriber, based on the duration (Tenure) of the product subscription. (d) Calendar/Activity Scheduling: Provision to auto-schedule activities like STB/unique consumer subscription activation/deactivation, à-la-carte channels and bouquets addition/removal, channel/bouquet composition modification, etc. (e) Bulk Channel/Bouquet Management: Provision to perform bulk activity of à-la-carte channels and bouquets addition and removal on all or a designated group of STBs/unique consumer subscription. (f) Token-number-based reports: Provision to download multiple generated reports with the help of token number, such as audit reports with different intervals. (g) Third-Party Integration: Provision to support integration with relevant third-party systems, such as, payment gateway integrations, interactive voice response (IVR) Integrations, SMS Gateway Integrations, etc. (h) Bill payment and reconciliation feature: Provision for bill payment and reconciliation (in case a DPO is running service in post-paid mode).

	(i) Generation of Reports: Provision to generate the following reports for operational purpose: (i) All, selective and single boxes' current status with their first-time activation date. (ii) Total number of à-la-carte channels and bouquets and STB/unique consumer subscription expiring detail till given future date on the dashboard, according to the permission. (iii) Today's fresh activation count, de-activation count, re-activation count, à-la-carte channels and bouquets addition/ removal count on dashboard, according to the permission. (iv) Total active and inactive subscriber's details with multiple criteria (network-wise, à la-carte channels and bouquets-wise, state-city wise and broadcaster-wise).
29.	It shall be mandatory for SMS to have backup servers and logs of all activities carried out in main server shall be concurrently copied into the backup servers, in an automated manner without any manual intervention. Provided that a log of all such instances shall be maintained along with date and time stamp, where the backup server has been used as the main server: Provided further that the main and backup server shall always be in sync with regard all data, such as subscription data, STB/unique consumer subscription UA/MAC ID details, entitlement level information, etc.

(D) DRM Requirements for conditional access by subscribers and encryption for IPTV services

Table 2

Sl. No.	Proposed DRM Requirements for conditional access by subscribers and encryption
1.	DPO shall ensure that the current version of the DRM in use do not have any history of hacking. A written declaration from the DRM vendor shall be required to be furnished on an annual basis as compliance of this requirement.
2.	DRM shall ensure all logs are un-editable, stamped with date and time of all transactions (all activations, deactivation, channel authorization/assignment and un-authorization / de-assignments and change in MAC ID/STB/unique consumer subscription). The DRM shall not allow altering or modification of any logs. There shall be no facility for the distributor/users to purge logs.
3.	DRM deployed do not have facility to activate and deactivate a Set Top Box (STB) /unique consumer subscription directly from the Graphical User Interface (GUI) terminal of DRM. All activation and deactivation of STBs/unique consumer subscription shall be done with the commands of the SMS (provided that such feature may be available only for specific testing. The command or access for such feature may be available with the highest system administration password. In all such cases a separate log file of such commands has to be maintained) integrated with DRM. The DRM shall be integrated with the SMS in a manner that ensures security of the channel.
4.	The SMS and the DRM should be integrated in such manner that activation and deactivation of STB/unique consumer subscription happen simultaneously in both the systems. Explanation: Necessary and sufficient methods shall be put in place so that each activation and deactivation of STBs/unique consumer subscriptions is reflected in the reports generated from the DRM.
5.	DRM deployed should be able to support two-way networks only.

6.	The DRM deployed should be able to support both carded as well as card-less STBs/unique consumer subscription for any provisioning.
7.	The DRM deployed should be able to generate, record, maintain independent reports and logs for verification purpose during audits corresponding to each command executed in the DRM issued by the SMS integrated with the DRM for last three (3) years minimum. The reports must have date and time stamp. Proposed reports should include: (a) Unique active STB/unique consumer subscription count as well as MAC ID wise on any desirable date (b) Unique bouquet/channel active for a specific STB/unique consumer subscription on any desirable date (c) MAC ID/User ID wise activation-deactivation report for service requests (d) Any alteration in bouquet and/or channels configured in DRM (e) Blacklist STB/unique consumer subscription report (desirable not mandatory feature) (f) Product code pertaining to channels/ bouquets available on the platform (g) Channel/bouquet authorization/assignment to STB/unique consumer subscription along with start date and end date of entitlement (h) STB/unique consumer subscription -VC pairing / de-pairing or User id- Mac-id Pairing / de-pairing (if applicable) in SMS/DRM (i) STB/unique consumer subscription activation / de-activation (j) Channels assignment to STB/unique consumer subscription (k) Report of the activations or the deactivations of a particular channel for a given period (l) The total number of registered subscribers (m) The total number of active subscribers (n) The total number of temporary suspended subscribers (o) The total number of deactivated subscribers (p) List of blacklisted STBs/unique consumer subscription in the DRM (desirable not mandatory feature) (q) Channel and bouquet wise monthly subscription report in the prescribed format. (r) The names of the channels forming part of each bouquet (s) The total number of active subscribers subscribing to a particular channel or bouquet at a given time (t) The name of a-la carte channel and bouquet subscribed by a subscriber (u) The ageing report for subscription of a particular channel or bouquet
8.	DRM deployed should be able to tag and blacklist the STB/unique consumer subscription in case of any piracy.
9.	DRM deployed should have the technical capability in India to maintain the systems on 24x7 basis throughout the year.
10.	The DRM and SMS should be integrated in such manner that upon deactivation of any subscriber from the SMS, all program/services shall be denied to that subscriber.
11.	The DRM should be capable of generating, recording and preserving unedited data / logs for at least three consecutive years for each command executed through the DRM, including logs of each command of the SMS integrated with the DRM.
12.	DRM deployed should be capable to support both software base as well as hardware base security.
13.	DRM shall be capable of adding/modifying channels/bouquets as may be required on real time basis in line with the activity performed in SMS.
14.	DRM should be so configured for specific type of STB/unique consumer subscription, that are procured and configured by the DPO. The DRM should not enable working/operation of any other type/brand/make of STB/unique consumer subscription, in the network.
15.	When infrastructure sharing (as and when permitted by MIB) is available, in such cases DRM shall be capable to support multiple DPOs.
16.	DRM should support content protection.
17.	DRM should support key rotation, i.e., periodic changing of security keys

18.	In case DPO has deployed hybrid STBs (hybrid STB for the purpose of this regulation means a STB that uses multiple methods of receiving transmission signals with video and audio content, however in a single instance such STB provides only one type of service), DRM shall ensure that the over-the-top (OTT) App and any browser does not get access to the linear television channels offered by the DPO from its own system, and similarly, DRM for IPTV service should not get access to channels delivered through OTT platform. Provided that, all the mandatory requirements for DRM shall be complied by hybrid STBs.
19.	There shall not be any active unique subscriber outside the database tables. Further, there shall not be an option to split DRM database for creation of more than one instance by a DPO or a vendor.
20.	It must support the following options with reference to uploading of unique access (UA)/MAC ID details in DRM database: (a) A secure un-editable file of MAC ID details, as purchased by the distributor, to be uploaded by the DRM vendor on the DRM server directly, (b) If it is uploaded in any other form, UA/MAC ID in DRM database shall be captured in logs, (c) Further, DRM shall support an automated, application programming interface (API)-based mechanism to populate such UA/MAC ID details in the SMS, without any manual intervention.
21.	It shall be mandatory to have backup servers and logs of all activities carried out in main server shall be concurrently copied into the backup servers: Provided that a log of all such instances shall be maintained along with date and time stamp, where the backup server has been used as the main server: Provided further that the main and backup server shall always be in sync with regard all data, such as subscription data, STB/unique consumer subscription UA/MAC ID details, entitlement level information, etc
22.	DRM and SMS shall ensure that the access to database is available to authorized users only, and in "read only" mode only. Further, the database audit trail shall be permanently enabled. Explanation: Database here refers to the database where data and log of all activities related to STB/unique consumer subscription activation, deactivation, subscription data, STB/unique consumer subscription UA/MAC ID details, entitlement level information, etc., is being stored.
23.	**Provision of à-la-carte channels or bouquet**: (a) DRM (and SMS) shall be able to handle all the channels, made available on a platform, in à la carte mode. (b) DRM (and SMS) shall have the capability to handle such number of broadcaster/DPO bouquets, as required by the DPO.
24.	DRM and SMS applications, along with their respective databases, shall be stored in such a way that they can be separately identified.
25.	DRM shall have a provision to export the database/report for reconciliation with the SMS database. Further, there shall be a provision of reconciliation through secure APIs/secure scripts.
26.	There shall be unique license key required for viewing, the encryption period for a specific key should be configurable to change at periodic interval in DRM deployed by DPO.
27.	For every change in channels, fresh license keys should be issued by the DRM. License keys issued by DRM should be secure and encrypted. DRM must ensure that the authorization keys are not received by the STB/unique consumer subscription from any other source other than the one specified by the IPTV system.
28.	DRM servers should comply with extant Rules and Regulations including relevant clause under extant provisions (if any) relating to data localisation, data security and privacy. It should not be

	allowed to connect main DRM server to some other location (India or other country) with some proxy or another server to integrate with SMS and DPO system.
29.	IPTV service delivery may conform to multicast and/or unicast mode. The system configuration should ensure that every television channel is available to every customer on selection to view, irrespective of the mode of delivery or the number of viewers seeking such channel at any point of time. STBs/unique consumer subscription with facilities for recording programs shall have a copy protection system (i.e., a feature which prevents reproduction of content and/or unauthorized copying and distribution of content) and such recorded content should not be transferrable to any other device or delivered to any other network in any manner whatsoever.
30.	IPTV system should not be allowed to deliver linear content to any other device except STB/unique consumer subscription which has been whitelisted in DRM.
31.	The DRM should have following features: (a) It should restrict user to editing. (b) It should restrict user from sharing or forwarding or mirroring the content from the STB/unique consumer subscription. (c) It should disallow user to take screen shots or screen grabs or screen-recording, if technically feasible. (d) It should lock access to authorized STBs/unique consumer subscriptions only. (e) It should have Geo blocking feature. (f) It should be able to set expiry date to recorded content at STB/unique consumer subscription end based on various policies.
32.	The DRM should have the capability of being upgraded over-the-air (OTA) so that the connected STBs/unique consumer subscription always have the most upgraded version of the DRM.
33.	The DPO shall ensure that the DRM is up to date by installing necessary patches, error corrections, additions, version releases, etc. so as to ensure protection of channels and content at all times
34.	No such functionality should be added to or removed from the DRM which compromises security of channels. DPO shall be responsible for encryption of channels' signals before their delivery through its IPTV platform using DRM hybrid STBs/unique consumer subscription. All costs / expenses (by whatever name called) that are required to be incurred or become payable for such upgradation and for delivery/distribution of multi channel television programmes to subscribers shall be borne solely by such DPO. The DPO shall employ all reasonable security systems and procedures to prevent any loss, theft, piracy, un-authorized use, reception or copying of channels or any part thereof and shall notify broadcasters as soon as practicable after it becomes aware that such an event has occurred
35.	The DRM should not in any way interfere with / invalidate fingerprinting.
36.	DPO shall promptly, and at it sole cost and expense, correct any issues with the DRM (such as bugs, defects, omissions or the like) that prevents subscribers from accessing the DRM hybrid STBs/unique consumer subscription or channels through the DRM hybrid STBs/unique consumer subscription.
37.	DPO shall provide broadcasters with video and audio codecs supported by the DRM hybrid STBs/unique consumer subscription. The DPO shall ensure that no such changes/modifications are made to such codecs parameters that will require broadcasters to incur any expense for delivery of channels / content that are free from viewer discernible problems (including, without limitation, video with no audio, audio with no video or significant signal distortion
38.	DRM should ensure that the hybrid STBs/unique consumer subscription are verifiably located within India by reference to internet protocol address and service address. DRM must ensure and lock the viewership to single device by single STB/unique consumer subscription or any device by ensuring MAC ID based authentication. The DRM must use industry-standard means (including IP-address look-up technology with screening and blocking of proxies (including anonymizing and spoofed proxies)) to prevent delivery of channels to IP addresses outside of India or to proxies.
39.	DRM should ensure that television channels are accessible on STBs/unique consumer subscription of only such subscribers who are then-current, valid subscribers of the DPO, and such confirmation

	must take place prior to the DRM delivering (or authorizing the delivery of) television channel to the STBs/unique consumer subscription of such subscribers.
40.	Upon deactivation of any subscriber from the SMS, the DRM shall restrict delivery of all programme/services to that subscriber.
41.	The DRM should not have any feature to insert any content (including advertisement, banner on portion of screen, etc) by itself. However, ticker messages for consumer information as regards their services from DPO shall be permitted.
42.	The DRM should not mask/remove any copyright, trademark or any other proprietary information on the channels at the time of their delivery.

The service providers shall ensure that they seek provisioning of after sales services and support through a local entity so as to *inter-alia* provide quick resolution to any technical and piracy related issues, from DRM equipment supplier, while procuring DRM equipment.

(E) DRM Requirements in so far as they relate to fingerprinting for IPTV services

Table 3

Sl. No	Fingerprinting requirements under DRM
1.	The DPO shall ensure that it has systems, processes and controls in place to run fingerprinting at regular intervals
2.	The STB/unique consumer subscription should support both visible and covert types of finger printing.
3.	The fingerprinting should not get invalidated by use of any device or software.
4.	The fingerprinting should not be removable by pressing any key on the remote of STB/unique consumer subscription.
5.	The finger printing should be on the topmost layer of the video.
6.	The finger printing should be such that it can identify the unique STB/unique consumer subscription number or the unique VC number or the MAC ID.
7.	The finger printing should appear on the screens in all scenarios, such as menu, Electronic Programme Guide (EPG), settings, blank screen, and games etc.
8.	The location, font color and background color of fingerprint should be changeable from head end and should be random on the viewing device.
9.	The finger printing should be able to give the numbers of characters as to identify the unique STB/unique consumer subscription and/or the MAC ID.
10.	The finger printing should be possible on global as well as on the individual STB/unique consumer subscription basis.
11.	The overt fingerprinting/watermarking should be displayed by the DPO without any alteration with regard to the time, location, duration and frequency.
12.	The DRM deployed should be able to generate fingerprinting/watermarking both global fingerprinting as well as targeted channel fingerprinting/watermarking.
13.	The DRM shall support and enable forensic watermarking at STB/unique consumer subscription level.
14.	The DRM shall have the capability to run fingerprinting with at least one fingerprinting every ten (10) minutes on a 24x7x365 basis. DRM should have a feature to publish report of fingerprinting schedule for defined interval. The DPO shall make such report available to broadcaster on request.

(F) DRM Requirements in so far as they relate to STBs/unique consumer subscription

Table 4

Sl. No.	**STB**/unique consumer subscription **Requirements for DRM for IPTV services**
1.	All STBs/unique consumer subscription should have a DRM content protection.
2.	The STB/unique consumer subscription deployed should be capable to support content decryption, decoding and DRM license evaluation.
3.	The STB/unique consumer subscription should be capable of displaying fingerprinting inserted from Headend through DRM/SMS. The STB/unique consumer subscription should support both targeted channel fingerprinting as well as all global fingerprinting.
4.	The STB/unique consumer subscription should be individually addressable from the Head-end.
5.	The STB/unique consumer subscription should be able to receive messages from the Head-end.
6.	The messaging character length should be minimal of upto120 characters.
7.	There should be provision for global messaging, group messaging and the individual STB/unique consumer subscription messaging.
8.	The STB/unique consumer subscription must be compliant to the applicable Bureau of Indian Standards
9.	The STBs/unique consumer subscription should be addressable over the air to facilitate OTA software upgrade.
10.	The STBs/unique consumer subscription with facilities for recording the programs shall have international standard copy protection system
11.	The STB/unique consumer subscription should have a provision that fingerprinting is never disabled.
12.	The watermarking network logo for all pay channels shall be inserted at encoder end only.
13.	DRM/SMS deployed should be able to send scroll messaging which should be only available in the lower part of the screen.
14.	DRM deployed should be able to geo tag STB/unique consumer subscription deployed in the network for security.
15.	STB/unique consumer subscription should take all commands directly from DRM not from any intermediate servers.
16.	STB/unique consumer subscription while using IPTV infrastructure should not have feature to download (direct or side download) any 3rd party App/APK and should not have access to any browser.
17.	STB/unique consumer subscription should not be able to access the authorization keys from any other source except from the IPTV system through the IPTV closed network. DRM must ensure that the authorization keys are not received by the STB/unique consumer subscription from any other source other than the one specified by the IPTV system
18.	No play store should be accessible for enabling download, etc. when STB/unique consumer subscription, is functioning in the IPTV network.
19.	STB/unique consumer subscription should have copy protection.
20.	DPO system should have capability to maintain un-editable logs of all activity and configurations including download or upgrade of IPTV services App (if any) at STB/unique consumer subscription end

21.	The DRM should not allow delivering linear TV channels on Internet. The delivery of multi channel television programmes should remain in a closed network within the device.
22.	The STB/unique consumer subscription should have forced messaging capability including forced finger printing display.
23.	The DRM hybrid STBs/unique consumer subscription should be tested for the following prior to their seeding in the subscribers' premises: (a) System down testing (b) Error messaging (c) Negative user journey testing (d) Device variance testing (e) Destructive testing (f) Application monitoring testing (g) In-app monitoring testing

(V. Raghunandan)
Secretary, TRAI

Note.1: The principal regulations were published in the Gazette of India, Extraordinary, Part III, Section 4, vide notification No. 21-4/2016-B&CS dated 3rd March 2017 (1 of 2017).

Note. 2: The principal regulations were amended vide notification No. 21-6/2019-B&CS dated 30th October 2019 (7 of 2019).

Note. 3: The principal regulations were further amended vide notification No. 21-5/2019-B&CS dated 1st January 2020 (1 of 2020).

Note. 4: The principal regulations were further amended vide notification No. RG-1/2/(3)/2021-B AND CS(2) dated 11th June 2021 (1 of 2021).

Note. 5: The principal regulations were further amended vide notification No. RG-1/2/(2)/2022-B AND CS (2) dated 22nd November 2022 (2 of 2022).

Note. 6: The Explanatory Memorandum explains the objects and reasons of the Telecommunication (Broadcasting and Cable) Services Interconnection (Addressable Systems) (Fifth Amendment) Regulations, 2023 (4 of 2023).

Explanatory Memorandum

Introduction and Background

1. TRAI notified the Telecommunication (Broadcasting & Cable) Services Interconnection (Addressable System) Regulation, 2017 on 03.03.2017 [hereinafter referred to as "Interconnection Regulations 2017"].

2. During the consultation undertaken to prepare the Audit Manual, certain comments and observations reflect some issues in the Schedule III of the Interconnection Regulations 2017.

3. Accordingly, Draft Telecommunication (Broadcasting and Cable) Services Interconnection (Addressable Systems) (Amendment) Regulations, 2019 [hereinafter referred to as the "Draft Regulations"] was issued on 27 August 2019. These Draft Regulations amended Schedule III of the Interconnection Regulations 2017, on the following issues: -
   i. Digital Rights Management Systems
   ii. Transactional capacity of CAS and SMS system
   iii. Fingerprinting – Support for Visible and Covert fingerprinting in STBs
   iv. Watermarking network logo for all pay channels.

4. DRM is a systematic approach to copyright protection for digital media. The purpose of DRM is to prevent unauthorized redistribution of digital media and restrict the ways consumers can copy content they've purchased. DRM products were developed in response to the rapid increase in online piracy of commercially marketed material, which proliferated through the widespread use of peer-to-peer file exchange programs. Typically, DRM is implemented by embedding code that prevents copying, specifies a time period in which the content can be accessed or limits the number of devices the media can be installed on. DRM technology focuses on making it impossible to steal content in the first place, a more efficient approach to the problem than the hit-and-miss strategies aimed at apprehending online poachers after the fact.

5. The Schedule III of the Interconnection Regulations 2017 does not provide for the requirements / specifications of DRM based systems. The Authority, during its consultations on Audit manual, received the feedback that owing to its benefits the IPTV based DPOs are switching to DRM technology. It is necessary that the Audit regime covers the DRM based networks and provides for enabling provisions for such operators. Accordingly, Draft Regulations included DRM specifications in Schedule III.

6. During the consultation process, the Authority received numerous comments and suggestions from various stakeholders on this issue. Numerous modification/additions were proposed by several stakeholders. Hence, the Authority was of the opinion that system requirements for DRM shall be dealt with in a separate consultation paper (refer para 34 of Explanatory Memorandum to the Interconnection (Amendment) Regulations, 2019 dated 30.10.2019).

7. The Authority was of the view that on the issue related to "System Requirements for Digital Rights Management System", extensive deliberations with industry stakeholders is required. Accordingly, the Authority constituted a committee comprising of industry stakeholders to prepare and submit draft 'System Requirement for Digital Right Management (DRM)' to the Authority. The committee had representatives from the following firms/organisations/associations:

   - Broadcast Engineering Consultants India Limited (BECIL)
   - Indian Broadcasting and Digital Foundation (IBDF)
   - News Broadcasters & Digital Association (NBDA)
   - All India Digital Cable Federation (AIDCF)
   - Dish TV

- Tata Sky
- Bharti Telemedia
- Sun Direct
- NXT Digital
- IIT Kanpur
- Andhra Pradesh State Fibernet Ltd
- Delinet Broadband

8. The Terms of Reference of the Committee, was to:

   (i) Study TRAI's Telecommunication (Broadcasting & cable) Services Interconnection (Addressable System) Regulation, 2017 and its amendments (hereinafter called *"Interconnection Regulation 2017"*).

   (ii) Provide a report to the Authority on the "System requirement for Digital Right Management (DRM)" to be included in Schedule III of the Interconnection Regulation 2017.

9. The committee held several meetings. These meetings were facilitated by the Authority. After extensive deliberations, the committee submitted a report on "System requirement for Digital Right Management (DRM)" to be included in Schedule III of the Interconnection Regulation 2017 to the Authority. The Authority conveys its appreciation for the extensive work done by the committee.

10. Accordingly, TRAI issued a Consultation Paper on 'System Requirement for Digital Right Management (DRM)' in the form of draft amendment in the Interconnection Regulation 2017 on 9th September 2022. The comments of the stakeholders were invited by 7th October 2022 and counter comments, by 21st October 2022. On request of the stakeholders, the deadline to submit the comments was extended till 18th November 2022 for comments and 2nd December 2022 for counter-comments. Comments on the said consultation paper were received from twenty one stakeholders and counter-comments were received from two stakeholders, which were uploaded on TRAI website. Subsequently, an Open House Discussion (OHD) was held on 24th February 2023. A few additional comments were also received after OHD.

11. After taking into consideration the comments received from the stakeholders and in-house analysis, the Authority has finalized the Telecommunication (Broadcasting and Cable) Services Interconnection (Addressable Systems) (Fifth Amendment) Regulations, 2023 (hereinafter referred to as the "Fifth Amendment Regulations"). The subsequent paragraphs explain the objects and reasons of the Fifth Amendment Regulations.

12. The DRM based IPTV systems are being deployed. As it is a developing ecosystem, the regulations may require review on the basis of feedback or future developments. Accordingly, the Authority may consider to review these regulations as and when considered necessary.

Date of implementation of these Regulations

13. In the consultation paper on "Draft Telecommunication (Broadcasting and Cable) Services Interconnection (Addressable Systems) (Fourth Amendment) Regulations, 2022" dated 9th September 2022 [hereinafter called CP], the following was mentioned:
   "(3) These regulations shall come into force from the date of their publication in the Official Gazette."

14. During discussions with a few stakeholders, the stakeholders suggested that some time may be given to the industry to comply with these Regulations. Accordingly, the Authority is of the view that these regulations shall come into force from the date of their publication in the Official Gazette provided that for the existing systems, the provisions of these regulations shall apply after three months from the date of their coming into force.

Digital Rights Management (DRM) System Requirements

15. In the CP, the following was mentioned:
"The term DRM, herein, refers to the management of the encryption systems for, inter-alia, providing the functionality of CAS and SMS for the Internet Protocol Television (IPTV) service provider under these regulations."

16. In response, an association proposed that DRM System requirements "for IPTV services" should be specifically mentioned in the introduction and background to the Draft Fourth Amendment as well as captioned in Draft Schedule-X of the Draft Fourth Amendment. They mentioned that the Draft Fourth Amendment should clearly specify that these requirements are in the context of DRM systems deployed by DPOs providing IPTV services. The words "DPOs providing IPTV services" be suitably incorporated in Draft Fourth Amendment and Draft Schedule-X. The association further opined that scope of Consultation Paper, Draft Fourth Amendment and Draft Schedule-X is to be restricted to IPTV services, which for clarity, must exclude any over-the-top (OTT) services inter-alia for jurisdictional issues.

17. A few stakeholders and an association opined that the term DRM should refer to the management of the encryption systems for, inter-alia, providing the functionality of only CAS for the IPTV service provider under these regulations.

Analysis:

18. DRM mainly provides management of the encryption systems for, inter-alia, providing the functionality of CAS for IPTV service. Further, the regulation already has separate section for 'DRM requirements in so far as they related to subscriber management systems (SMS) for IPTV services'. Therefore, the Authority is of the view that the word 'SMS' may be removed from explanation of DRM. Accordingly, modification has been carried out in the regulation.

(C) Overall architecture / system requirements and certification for IPTV service

19. In the CP, the following was mentioned:
"(a) Retransmission of channels shall be over a closed network owned and controlled by DPO for electronic delivery of audio video stream of linear channels using Internet Protocol through an encrypted, point-to-point system architecture to set top boxes located within a subscriber's premises. For the avoidance of doubt, IPTV shall not include any electronic delivery for receipt and viewing via (i.e., directly accessible via) the Internet/world wide web/OTT."

20. In response, one association and a few stakeholders proposed that retransmission of channels shall be over a closed network owned and/or controlled by DPO for electronic delivery of audio video stream of linear channels using Internet Protocol through an encrypted, point-to-point system architecture to set top boxes located within a subscriber's premises. For the avoidance of doubt, IPTV shall not include any electronic delivery for receipt and viewing via (i.e., directly accessible via) the Internet / world wide web/OTT.

21. A few stakeholders and an association suggested removal of last line of (C) (a). One stakeholder suggested IPTV shall not include any electronic delivery for receipt and viewing via (i.e., directly accessible via) the Internet / world wide web/OTT. They opined that it is practically not feasible for any DPO to own the complete network.

22. One association opined that retransmission of channels should be only over the closed network that is owned, controlled, and managed by the relevant DPO. IPTV Services should neither be accessible through nor touch public/open Internet. DPO should not be allowed to sub-license the DRM and/or any rights granted to such DPO by the broadcaster. They further mentioned that at present, there are no guidelines issued by MIB regarding infrastructure sharing between IPTV operators, and as such, there are inter-alia jurisdictional issues

concerning infrastructure sharing between IPTV operators. It is premature to include requirements relating to infrastructure sharing in the Draft Fourth Amendment / Draft Schedule-X since, the same appears to be a foregone conclusion of TRAI on these aspects. One stakeholder opined that an option should be considered for introduction of Soft STBs (App based) for running IPTV services.

Analysis:

23. The IPTV operators are enjoined to comply with extant MIB Guidelines and TRAI Regulations. Appropriate provisions already exist in guidelines/ regulations. Therefore, after due consideration this clause has been removed.

(D) DRM Requirements in so far as they relate to subscriber management systems (SMS) for IPTV services:

Table 1 (1.) of CP

24. In the CP, the following was mentioned:
"There shall not be any data mismatch between DRM and SMS. Maximum mismatch based on subscription base may be allowed as mentioned below:

(1) Must be less than 0.20% for subscriber base up to 100000 subs (0 to 200 for subscriber base of up to 100000)
(2) Must be less than 0.04% for subscriber base up to 1000000 subscribers (0 to 400 for subscriber base of up to 1000000)
(3) Must be less than 0.01% for subscriber base above 10000000 subscribers (0 to 1000 for subscriber base of up to 10000000)

The data between both the systems shall be reconciled on a monthly basis. The reconciliation report shall be stored along with the system data for a minimum of 2 years or at least two audit cycles, or as per Schedule III whichever is later."

25. In response, a few stakeholders and an association opined that mismatch between DRM and SMS cannot be matched with low difference. Because number of users (LCO) and number of sessions used in SMS is very high and in 1st week of every month there will be huge commands travelling via API and SMS need to handle 2 or 3 DRM/CAS. In such scenario there is possible of mismatch, so making the mismatch 1% will be useful for DPO. An association opined that it is imperative that a period of three (3) years be prescribed by Authority for retention of data and records so as to inter-alia ensure that the broadcaster led audits can be meaningfully conducted.

26. On the other hand, a few stakeholders opined that the mismatch must be 0.5% as similar in cable TV. One stakeholder mentioned that the provided guidelines are really appreciated and the same should also be enforced to the other DPO platforms too.

Analysis:

27. Regarding mismatch percentage, some stakeholders have opined that the limits should be increased, however, the Authority is of the view that these percentages may not be modified at this stage and the case may be reviewed at a later stage.

28. With respect to retention period for data and records, it may be noted as per Schedule III of the Interconnection Regulations 2017 (as amended), the annual Audit as caused by Distributor under regulation 15 (1) shall be scheduled in such a manner that there is a gap of at-least six months between the audits of two consecutive calendar years. Further, there should not be a gap of more than 18 months between audits of two consecutive calendar years. In this regard, it has been brought to the notice of TRAI that many DPOs submit their DPO initiated audit reports (under clause 15(1) of TRAI's Interconnection Regulations) to the broadcasters six (6)

to eighteen (18) months after they receive the audit report from their respective auditors. By the time the broadcaster analyses the same, highlights relevant observations/discrepancies, and/or decides to conduct broadcaster caused audit in terms of Clause 15(2) of Interconnection Regulations, there is already a year's (or sometimes more) delay, which diminishes the relevance of audit report as well as allows DPOs to claim unavailability of data/records relying on TRAI's requirement to maintain data/records only for two (2) years. This, inter-alia, amplifies the problem and hinders detection of true and correct subscriber numbers. In this regard, the Authority is of the view that transparency is utmost important in the entire value chain and increasing the period of record retention from 2 to 3 years, will improve the overall transparency, assist in curbing the menace of under reporting subscribers and improve the effectiveness of broadcaster caused audit prescribed in 15(2) of Interconnection Regulation 2017. Same suggestion has been received for multiple places in the Regulation. Accordingly, modifications have been made in the regulation.

Table 1 (2.) of CP

29. In the CP, the following was mentioned:
*"**Password Policy Creation for Users**: SMS shall have a defined password policy, with minimum length criteria and composition (upper and lower-case characters, numeric, alphabets or special characters), forced password changes or any other appropriate mechanisms or combinations thereof."*

30. In response, one stakeholder suggested that above mentioned clause may be modified to read as follows: Password Policy Creation for Users: SMS shall have a defined password policy, with minimum length criteria and composition (upper and lowercase characters, numeric, alphabets or special characters), forced password changes or any other appropriate mechanisms or combinations thereof or alternatively user account has to be locked/paired to the Mac Id of the STB or the Customer Premises Equipment (CPE).

Analysis:

31. Since Mac id of the STB or the CPE are unique and if they are paired or locked with the user account, the support for the password validation and recovery for users may not be required. Therefore, the Authority is of the view that an alternate arrangement wherein user account has to be locked/paired to the Mac Id of the STB or the CPE, may also be permitted. Accordingly, modifications have been made in the regulation.

Table 1 (4.) of CP

32. In the CP, the following was mentioned:
"All activation and deactivation of STBs shall be done with the commands of the SMS integrated with the DRM."

33. In response, a few stakeholders and an association suggested that the word 'STB' should be replaced with 'STBs/APP'. They opined that IPTV can be provided as an application based with all security required under TRAI regulation.

Analysis:

34. With technological developments content can be viewed using application based services provided such arrangement meets extant licensing/regulatory framework. Therefore, the Authority is of the view that App based services, may also be permitted. Soft STBs (App based) may also be used for running IPTV services. In such cases, the unique id for each subscriber is required. In all such cases, STB or the CPE should have a unique Mac id that should be paired or locked with a user account. In view of above, the Authority is of the view that in place of 'STBs', the words 'STBs/unique consumer subscription' would be more appropriate to use. Similar/same suggestion has been received from a few stakeholders at multiple places in the Regulation. Accordingly, modifications have been made in the regulation.

Table 1(5.) of CP

35. In the CP, the following was mentioned:

"Necessary and sufficient methods shall be put in place so that each activation and deactivation of STBs is reflected in the reports generated from the SMS integrated with the DRM and vice versa."

36. In response, a few stakeholders and an association suggested that the word 'STB' should be replaced with 'STBs/APP'. Further, another stakeholder suggested the following 'Necessary and sufficient methods shall be put in place so that each activation and deactivation of STBs is reflected in the reports generated from the SMS integrated with the DRM and DRM Session logs should be able to validate the access of the channels between period of activation and deactivation of the STBs.'

Table 1(6.) of CP

37. In the CP, the following was mentioned:
"DRM and SMS should be able to activate or deactivate services and/or STBs of the subscriber base of the distributor within 24 hours."

38. In response, a few stakeholders and an association suggested that the word 'STB' should be replaced with 'STBs/APP'.

Table 1(7.) of CP

39. In the CP, the following was mentioned:
"The SMS shall be independently capable of generating, recording, and maintaining logs, for the period of at least immediately preceding two (2) consecutive years, corresponding to each command executed in the SMS including but not limited to activation and deactivation commands."

40. In response, an association suggested the period of at least immediately preceding three (3) consecutive years, instead of two (2) consecutive years. Further, they mentioned that the time period for record retention throughout the Draft Regulations 2022 has been prescribed as two (2) years instead of proposed three (3) years as was submitted in the DRM Committee Report. The three (3) years' time period was inter-alia suggested in order to ensure that the data for the preceding three (3) years is available for the purposes of broadcaster led audits prescribed under clause 15 (2) of the Interconnection Regulations. The Interconnection Regulations prescribe a period of two(2) years for data/record retention, which is insufficient and factors period of limitation contemplated under the provisions of the Consumer Protection Act. However, it completes overlooks the period of limitation contemplated under the Limitation Act, which is the only statute relevant from the perspective of broadcaster-DPO relationship. They further mentioned that by the time the broadcaster led audit is conducted, the prescribed period of two (2) years for data/ record retention is already over. Therefore, the period for retention of data in the Draft Fourth Amendment be prescribed for at least three (3) years.

Table 1 (8) (j) of CP

41. In the CP, the following was mentioned:
"The SMS should be computerized and capable of recording all logs including information and data concerning the subscribers such as:……..
(j) Unique STB number"

42. In response, a stakeholder suggested that the words 'STB number' should be replaced with 'STB number/user name'. They opined that DRM and Middleware systems work with usernames which are more user friendly than STB numbers.

Table 1 (9.) of CP

43. In the CP, the following was mentioned:
"The SMS should be capable of:
(a) Viewing and printing of historical data in terms of the activations and the deactivations of STBs.
(b) Locating each and every STB and VC/MAC ID installed at city and state level.

(c) Generating historical data of changes in the subscriptions for each subscriber and the corresponding source of requests made by the subscriber."

44. In response, a few stakeholders and an association suggested that the word 'STB' should be replaced with 'STBs/APP'.

Table 1 (10.) of CP

45. In the CP, the following was mentioned:

"The SMS should be capable of generating reports, at any desired time including about:
(a) The total number of registered subscribers.
(b) The total number of active subscribers.
(c) The total number of temporary suspended subscribers.
(d) The total number of deactivated subscribers.
(e) List of blacklisted STBs in the system.
(f) Channel and bouquet wise monthly subscription report in the prescribed format.
(g) The names of the channels forming part of each bouquet.
(h) The total number of active subscribers subscribing to a particular channel or bouquet at a given time.
(i) The name of a-la carte channel and bouquet subscribed by a subscriber.
(j) The ageing report for subscription of a particular channel or bouquet."

46. In response, a few MSOs and one association suggested that the word 'STB' should be replaced with 'STBs/APP'.

Table 1 (13.) of CP

47. In the CP, the following was mentioned:
"If there is active infrastructure sharing then, DPO shall declare the sharing of the DRM and the SMS deployed for distribution of channels. In case of deployment of any additional DRM/SMS, the same should be notified to the broadcasters by the distributor."

48. In response, one association opined that at present, there are no guidelines issued by MIB regarding infrastructure sharing between IPTV operators, and as such, there are inter-alia jurisdictional issues concerning infrastructure sharing between IPTV operators. It is premature to include requirements relating to infrastructure sharing in the Draft Fourth Amendment / Draft Schedule-X since, the same appears to be a foregone conclusion of TRAI on these aspects.

Analysis

49. Regarding infrastructure sharing amongst IPTV operators, it may be noted that Ministry of Information and Broadcasting (MIB) has not yet issued any guidelines in this regard. TRAI may forward its recommendations to MIB on this issue, after due consultation process. However, the Authority is of the view that Interconnection Regulation should have an enabling provision to promote infrastructure sharing amongst IPTV operators, which is subject to the MIB's 'Guidelines on infrastructure sharing for IPTV operators', as and when permitted by MIB. Same suggestion has been received for multiple places in the Regulation. Accordingly, modifications have been made in the regulation.

Table 1(14.) of CP

50. In the CP, the following was mentioned:
"*SMS shall have a provision to generate synchronization report, with date and time, with the minimum fields as listed below:*

(f) STB Number (or in case of card-less system, chip ID or MAC ID number of the STB)
(g) Product Code pertaining to à-la-carte channels and bouquets available on the platform

(h) Start Date of entitlement
(i) End Date of entitlement
(j) Status of STB (active/Inactive)"

51. In response, a few stakeholders and an association suggested that the word 'STB' should be replaced with 'STBs/APP'.

Table 1(15.) of CP

52. In the CP, the following was mentioned:
" The file output of DRM shall be processed by SMS system to compare and generate a 100% match or mismatch error report."

53. In response, one stakeholder opined that clarification is needed on File output formats required from DRM. The stakeholder has further mentioned that if not regulated, there may arise different versions of the clause mentioned.

Analysis:

54. TRAI has issued the Telecommunication (Broadcasting and Cable) Services Digital Addressable Systems Audit Manual [hereinafter called Audit Manual] on 8th November 2019. Similarly, TRAI may issue Audit Manual for audits of DRM systems. Therefore, the issue related to file output formats related to DRM systems may be dealt with at that stage.

Table 1 (16.) of CP

55. In the CP, the following was mentioned:
*"**Channel/Bouquet management:** SMS shall support the following essential requirements:*
(a) Create and manage all channels and bouquets along with the relevant details such as name, tariff, broadcaster, or DPO bouquet, etc.
(b) Manage changes in the channel/bouquet, as may be required, from time to time.
(c) Link the Products IDs for à-la-carte channels and bouquets (Single and Bulk) created in DRM with the product information being managed in SMS, for smooth working of SMS and DRM integration.
(d) Management of historical Data of Product name, i.e., Broadcasters (name), maximum retail price (MRP), distributor retail price (DRP)."

56. In response, one stakeholder suggested an amendment that SMS creates and manages packages based on Product ID and composition provided from DRM. They further mentioned that DRM API's cannot allow Packages to be directly be created/modified from SMS subject to DRM database security.

Analysis:

57. The Authority is of the view that SMS, in synchronisation with DRM on real time basis, should support the following essential requirements (amongst other essential requirements as specified in the regulation): Create and manage relevant product ID for all channels and bouquets along with the relevant details such as name, tariff, broadcaster, or DPO bouquet, etc.

Table 1 (17.) of CP

58. In the CP, the following was mentioned:
*"**Network Capacity Fee (NCF) Policy Creation:** SMS shall support all NCF related requirements mandated by the applicable tariff order."*

59. In response, one stakeholder opined that the Tariff orders need to be finalized and enforced by the authority, since there is a lot of ambiguity regarding this. The broadcasters are enforcing the tariff as per their convenience and some broadcasters are even seeking for minimum guarantee commitment to provide the IRD to the IPTV provider, which is against creating a playing field for the DPOs.

Analysis:

60. It is binding on the service providers to comply with TRAI's Regulation/tariff order/ directions/Order, etc.

Table 1 (19.) of CP

61. In the CP, the following was mentioned:
*"**Management of Logs**: ....*
(b) SMS shall have the provision of generating the user activity log report to enable tracking users' work history. It shall not be allowed to delete the records from the log."

62. In response, one stakeholder suggested that the word 'SMS' should be replaced with 'SMS/DRM'. They further opined that DRM maintains the session logs whenever a user views a channel including the time stamp. These logs facilitate the viewership analysis and provides validation for the channel access as per the user's subscription.

Analysis:

63. In the regulation there is already a provision related to DRM maintaining proper logs, accordingly no modification has been made in the Regulation.

Table 1 (22.) of CP

64. In the CP, the following was mentioned:
"STB and MAC ID shall be paired from the SMS to ensure security of channel (applicable for DRM with pairing facility)."

65. In response, one stakeholder suggested that STB/Username and MAC ID shall be paired from the SMS to ensure security of channel.

Table 1 (23.) of CP

66. In the CP, the following was mentioned:
"The SMS shall be capable of individually addressing subscribers, for the purpose of generating the reports, on channel by channel and STB by STB basis."

67. In response, a few stakeholders and an association suggested generating the reports, on channel by channel and STB/MAC ID by STB/MAC ID basis. They opined that for app, it can be identified with MAC ID or with its unique ID.

Table 1 (24.) of CP

68. In the CP, the following was mentioned:
"SMS should have a facility to carry out monthly reconciliations of channels/ala carte and bouquet (with their respective ID created in SMS with DRM) and the variance report should be available in both DRM and SMS logs and made available during audits."

69. In response, one stakeholder opined that SMS should have a facility to carry out monthly reconciliations of channels/ala carte and bouquet (with their respective ID created in SMS with DRM) and the variance report should be available from the DRM and SMS logs and made available during audits.

Analysis:

70. The Authority accepts the suggestion made by stakeholder.

Table 1 (26.) of CP

71. In the CP, the following was mentioned:
*"**Audit-related requirements**:*

SMS should have the capability to capture below-mentioned information that may be required for audit and otherwise: …..

(c) STB related:

(i) Change in location history

(ii) Change in status (Active/Damaged/Repaired/Replaced)"

72. In response, a few stakeholders and an association suggested that the word 'STB' should be replaced with 'STBs/APP'.

Table 1 (27.) of CP

73. In the CP, the following was mentioned:
*"**User Authentication:** SMS should have the capability to authenticate its subscribers through registered mobile number (RMN) through one-time password (OTP) system."*

74. In response, one stakeholder desired to know if the above clause is to enable logging in from other device to check subscription status or to use OTP to activate the box.

Analysis:

75. As mentioned above, one stakeholder has desired to know if the above clause is to enable logging in from other device to check subscription status or to use OTP to activate the box. In this regard, it is clarified that user authentication is required not only to activate any subscription but also to continue using it as per subscription terms and conditions.

Table 1 (28.) of CP

76. In the CP, the following was mentioned:
"SMS should have the provision to support the following additional requirements:
(a) List of à-la-carte channels and bouquets, digital headend (DHE) and Zone-wise: Provision to support/manage Zone/ Sub-Headend-wise list of à-la-carte channels and bouquets, in sync with the list available in DRM. ……"

77. In response, one stakeholder enquired the meaning of 'zone'.

Analysis:

78. Since the concept of zone does not find a mention in any Regulation/Tariff order, the words 'zone' or 'Zone-wise' has been removed from the regulation.

Additional clause

79. An association suggested insertion of the following additional clause,
"It shall be mandatory for SMS to have backup servers and logs of all activities carried out in main server shall be concurrently copied into the cloud-based backup servers, in an automated manner without any manual intervention, of reputed companies viz., AWS, Oracle, Microsoft Azure, Google cloud.

Provided that a log of all such instances shall be maintained along with date and time stamp, where the backup server has been used as the main server:

Provided further that the main and backup server shall always be in sync with regard all data, such as subscription data, STB UA/MAC ID details, entitlement level information, etc.

Provided further that it shall be permissible for vendors of servers to provide data / records to TRAI, MIB, relevant empaneled auditor and to relevant broadcasters."

Analysis

80. In order to avoid any loss of logs and activities, it is imperative that backup servers are there for SMS data. This will also facilitate the audit process. Accordingly, provisions have been made in the Regulation.

(E) DRM Requirements for conditional access by subscribers and encryption for IPTV services

Table 2 (2.) of CP

81. In the CP, the following was mentioned:
"DRM shall ensure all logs are un-editable, stamped with date and time of all transactions (all activations, deactivation, channel authorization/assignment and un-authorization / de-assignments and change in MAC ID/STB). The DRM shall not allow altering or modification of any logs. There shall be no facility for the distributor/users to purge logs."

82. In response, one stakeholder suggested to remove un-editable and not allowing altering the logs. They mentioned that this is possible in theory to generate fully protected logs using technologies like blockchain or ledger databases. However, this is a very expensive approach that the regulator shouldn't require. The DPO and DRM provider should enforce controlled access to the logs, so only authorized personnel can access the logs. Only the logging application should have the writer write the logs. All other users can only read the logs.

83. Another stakeholder opined that DRM shall ensure all logs are uneditable, stamped with date and time of all transactions (all session logs of the users, channel wise, date wise with user id or mac id should be available). The DRM shall not allow altering or modification of any logs. There shall be no facility for the distributor/users to purge logs. Provision for validation of session logs with subscription status should be available via middleware or an equivalent software.

Analysis:

84. The Authority is of the view that it is necessary to ensure that the logs are un-editable and stamped with date and time of all transactions. In case tempering of logs is permitted then it will defeat the whole purpose of maintaining logs. Accordingly, no modifications have been proposed in the regulation.

Table 2(3.) of CP

85. In the CP, the following was mentioned:
"DRM deployed do not have facility to activate and deactivate a Set Top Box (STB) directly from the Graphical User Interface (GUI) terminal of DRM. All activation and deactivation of STBs shall be done with the commands of the SMS integrated with DRM. The DRM shall be integrated with the SMS in a manner that ensures security of the channel."

86. In response, a few stakeholders and an association suggested that DRM deployed do not have facility to activate and deactivate a Set Top Box (STB)/MAC ID (APP) directly from the Graphical User Interface (GUI) terminal of DRM. All activation and deactivation of STBs/APP shall be done with the commands of the SMS integrated with DRM. The DRM shall be integrated with the SMS in a manner that ensures security of the channel. Another stakeholder opined that in some cases, like for testing purposes, the UI or other means should allow authorized personnel to manage the client devices.

Analysis:

87. All activation and deactivation of STBs/unique consumer subscription must be done with the commands of the SMS integrated with DRM. However, the Authority is of the view that some provisions may be kept for specific testing purposes. It is pertinent to ensure that such feature may be available only for specific testing. The command or access for such feature may be available with the highest system administration password. In all such cases a separate log file of such commands must be maintained. Accordingly, modifications have been made in the regulation.

Table 2 (4.) of CP

88. In the CP, the following was mentioned:

"The SMS and the DRM should be integrated in such manner that activation and deactivation of STB happen simultaneously in both the systems.
Explanation: Necessary and sufficient methods shall be put in place so that each activation and deactivation of STBs is reflected in the reports generated from the DRM."

89. In response, a few stakeholders and an association suggested that the SMS and the DRM should be integrated in such manner that activation and deactivation of STB/MAC ID happen simultaneously in both the systems. Explanation: Necessary and sufficient methods shall be put in place so that each activation and deactivation of STBs/APP is reflected in the reports generated from the DRM.

90. Another stakeholder suggested that the SMS and the DRM should be integrated in such manner that activation and deactivation of STB are synchronized in real time.

Analysis:

91. The Authority is of the view that SMS and the DRM should be integrated in such manner that activation and deactivation of STB happen simultaneously in both the systems and both the systems are synchronized in real time.

Table 2(6.) of CP

92. In the CP, the following was mentioned:
"The DRM deployed should be able to support both carded as well as card-less STBs for any provisioning."

93. In response, a few stakeholders and an association suggested that the word 'STBs' should be replaced with 'STBs and APP based'. Another stakeholder opined that it is irrelevant for DRM which is cardless by its nature. Another stakeholder suggested that the DRM deployed should be able to support both carded card-less STBs & Smart TV for any provisioning.

Table 2 (7.) of CP

94. In the CP, the following was mentioned:
"The DRM deployed should be able to generate, record, maintain independent reports and logs for verification purpose during audits corresponding to each command executed in the DRM issued by the SMS integrated with the DRM for last two (2) years minimum. The reports must have date and time stamp. Proposed reports should include:……"

95. In response, one stakeholder suggested that the clause may additionally mention that MSO can have these transactional logs exported to an external storage system ensuring that it is available in raw format without any change for the period of at least immediately preceding two (2) consecutive years, corresponding to each command executed in the SMS including but not limited to activation and deactivation commands. As mentioned earlier an association opined that it is imperative that a period of three (3) years be prescribed by Authority for retention of data and records so as to inter-alia ensure that the broadcaster led audits can be meaningfully conducted.

Table 2 {7(a)} of CP

96. In the CP, the following was mentioned:
"Unique active STB count as well as MAC ID wise on any desirable date"

97. In response, one stakeholder suggested Unique active STB count as well as Unique MAC ID/User ID/DRM ID wise on any desirable date.

Table 2 {7(b)} of CP

98. In the CP, the following was mentioned:

"Unique bouquet/channel active for a specific STB on any desirable date"

99. In response, one stakeholder suggested unique channel active for a specific STB/User on any desirable date.

Analysis:

100. It is understood that some DRM do not have provision to maintain bouquet information. In this regard, the Authority is of the view that bouquet information is required to be maintained in the DRM for verification and reconciliation of data. The Authority has already specified that these regulations should come in to force after three months from the date of publication of these regulations in the Official Gazette. Therefore, in case this facility does not exist in some of the existing DRM then the existing service providers should get this feature developed in the DRM within these 3 months. Same suggestion has been received for multiple places in the Regulation. Accordingly, modifications have been made in the regulation.

Table 2 {7(c)} of CP

101. In the CP, the following was mentioned:
"MAC ID wise activation-deactivation report for service requests"

102. In response, one stakeholder suggested MAC ID/User ID wise Channel viewership report for service requests.

Table 2{7(d)} of CP

103. In the CP, the following was mentioned:
"Any alteration in bouquet and/or channels configured in DRM."

104. In response, one stakeholder any alteration in bouquet and/or channels configured in DRM if the facility is available in DRM.

Table 2 {7(e)} of CP

105. In the CP, the following was mentioned:
"Blacklist STB report"

106. In response, one stakeholder opined that Blacklist STB should not have access/session log in the DRM. This clause can be removed also.

Analysis:

107. It is learnt that Blacklisting STB is done only in SMS. When it is blacklisted in SMS it will not send the request to DRM for viewer ship so no activity can be recorded in DRM. Therefore, the Authority is of the view that Blacklist STB/unique consumer subscription report may be made a desirable feature and it should not be mandated at this stage. Accordingly, modifications have been made to the regulation.

Table 2 {7(f)} of CP

108. In the CP, the following was mentioned:
"Product code pertaining to channels/ bouquets available on the platform."

109. In response, one stakeholder opined that product code pertaining to channels should be available in DRM.

Table 2 {7(g)} of CP

110. In the CP, the following was mentioned:
"Channel/bouquet authorization/assignment to STB along with start date and end date of entitlement".

111. In response one stakeholder suggested Channel Viewership Access by STB /User for a particular date / week / a period (from date to date). A few stakeholders and an association suggested that the word 'STB' should be replaced with 'STB/Mac ID'.

Table 2 {7(h)} of CP

112. In the CP, the following was mentioned:
"STB-VC pairing / de-pairing (if applicable)"

113. In response, one stakeholder suggested STB-VC pairing / de-pairing or User id- Mac-id Pairing / de-pairing (if applicable) in SMS/DRM.

Analysis:

114. The Authority accepts the suggestion made by stakeholder.

Table 2 {7(i)} of CP

115. In the CP, the following was mentioned:
"STB activation / de-activation"

116. In response, one stakeholder opined that Session Log validation should be possible for each active subscribed channel per user during subscription period of the user for any channel.

Table 2 {7(j)} of CP

117. In the CP, the following was mentioned:
"Channels assignment to STB"

118. In response, one stakeholder opined that DRM should not have facility for assignment of channel / bouquets to STB/User. If the facility is available, the corresponding logs should be available. A few stakeholders and an association suggested that the word 'STB' should be replaced with 'STB/Mac ID'.

Table 2 {7(k)} of CP

119. In the CP, the following was mentioned:
"Report of the activations or the deactivations of a particular channel for a given period."

120. In response, one stakeholder suggested that report of the activations or the deactivations of a particular channel for a given period available in SMS should be able to validate the session logs available in DRM.

Table 2 {7(l)} of CP

121. In the CP, the following was mentioned:
"The total number of registered subscribers."

122. In response, one stakeholder suggested that the clause should be the total number of registered subscribers if the DRM has the facility to register subscribers.

Analysis:

123. The same suggestion has been received for multiple places in the Regulation. The Authority does not agree with the stakeholder comment.

Table 2 {7(n)} of CP

124. In the CP, the following was mentioned:
"The total number of temporary suspended subscribers."

125. In response, one stakeholder suggested that the clause should be the total number of temporary suspended subscribers if the subscribers have registration facility in the DRM.

Table 2{7(o)} of CP

126. In the CP, the following was mentioned:
"The total number of deactivated subscribers."

127. In response, one stakeholder suggested that the clause should be the total number of deactivated subscribers if the registration of subscribers is available in DRM

Table 2{7(p)} of CP

128. In the consultation paper on "Draft Telecommunication (Broadcasting And Cable) Services Interconnection (Addressable Systems) (Fourth Amendment) Regulations, 2022" dated 9th September 2022, the following was mentioned:
"List of blacklisted STBs in the DRM."

129. In response, one stakeholder opined that the clause should be list of blacklisted STBs in the DRM if the registration of subscribers is available in DRM. Another stakeholder suggested that the word 'STBs' should be replaced with 'STBs/Mac ID (APP)'.

Table 2 {7(q)} of CP

130. In the CP, the following was mentioned:
"Channel and bouquet wise monthly subscription report in the prescribed format."

131. In response, one stakeholder suggested Channel and User wise monthly viewership report in the prescribed format.

Table 2{7(r)} of CP

132. In the CP, the following was mentioned:
"The names of the channels forming part of each bouquet."

133. In response, one stakeholder suggested that the clause should be the names of the channels in relation to their names registered in SMS.

Table 2{7(s)} of CP

134. In the CP, the following was mentioned:
"The total number of active subscribers subscribing to a particular channel or bouquet at a given time."

135. In response, one stakeholder suggested that the clause should be the total number of active subscribers subscribing to a particular channel at a given time.

Table 2 {7(t)} of CP

136. In the CP, the following was mentioned:
"The name of a-la carte channel and bouquet subscribed by a subscriber."

137. In response, one stakeholder suggested that the clause should be the name of the channels per user viewership records with respect to subscription status of a subscriber.

Table 2{7(u)} of CP

138. In the CP, the following was mentioned:
"The ageing report for subscription of a particular channel or bouquet."

139. In response, one stakeholder suggested that the clause should be the ageing viewership report of a particular channel for a particular time. Another stakeholder opined that much of this belongs to the Control Plane that drives the DRM and not the DRM per se.

Table 2 (8) of CP

140. In the CP, the following was mentioned:
"DRM deployed should be able to tag and blacklist the STB independently in case of any piracy."

141. In response, one association suggested that the word 'STB' should be replaced with 'STB &VC'. A few stakeholders and an association suggested that the word 'STB' should be replaced with 'STBs/Mac ID (APP)'. Another stakeholder suggested that the clause should mention that DRM deployed should not have any facility to activate the blacklisted STB.

142. Another stakeholder enquired about the word 'independently'. They further opined that DRM by itself can't detect piracy, it should be notified by some other parts of the ecosystem about pirate devices that need to be blacked out.

Table 2 (11) of CP

143. In the CP, the following was mentioned:
"The DRM should be capable of generating, recording and preserving unedited data / logs for at least two consecutive years for each command executed through the DRM, including logs of each command of the SMS integrated with the DRM."

144. In response, one stakeholder opined that it's about the entire ecosystem and not DRM itself. Keeping not-editable logs for several years incurs very significant costs.

Table 2 (13) of CP

145. In the CP, the following was mentioned:
"DRM shall not support carriage of channel with same name or nomenclature in the distributor's network served by each headend under more than one LCN, and another channel descriptor. Further, each channel available in DRM shall be uniquely mapped with channels available in SMS."

146. In response, a stakeholder opined that DRM doesn't deliver channels and it is not aware of the channel names, LCN, etc. Another stakeholder suggested that the clause should mention that DRM shall not support carriage of channel with same name or nomenclature in the distributor's network served by each headend under more than one instance, and another channel descriptor. Further, each channel available in DRM shall be uniquely mapped with channels available in SMS.

Analysis:

147. As per sub regulation 2 of Regulation 18 of the Interconnection Regulation 2017 (as amended), it shall be mandatory for the distributor to place all the television channels available on its platform in the electronic programme guide, in such a manner that all the television channels of a particular language in a genre are displayed together consecutively and one television channel shall appear at one place only. Further as per sub regulation 3 of Regulation 18 of the Interconnection Regulation 2017, every distributor of television channels shall assign a unique channel number for each television channel available on the distribution network. Since above provisions already exist in the Interconnection Regulation 2017, the Authority is of the view that the above clause 13 of Table 2 proposed in the CP should be deleted.

Table 2(14) of CP

148. In the CP, the following was mentioned:
"DRM shall be capable of adding/modifying channels/bouquets as may be required on real time basis in line with the activity performed in SMS."

149. In response, one stakeholder suggested that DRM shall be integrated with SMS in such a way that addition/modification of channels/bouquets in SMS are automatically synced to the DRM on real-time. Another stakeholder opined that it probably doesn't belong to DRM. Another stakeholder suggested that DRM shall be capable of executing SMS requests for channels as may be required on real time basis in line with the activity performed in SMS.

Table 2(15) of CP

150. In the CP, the following was mentioned:
"DRM should support only agreed DPO's branded/proprietary and DPO's supplied business model for STBs."

151. In response, a few MSOs and an association opined that DPOs should not be restricted to use only STB. So, STBs/APP based should be permitted. Another stakeholder suggested that DPO should deploy and activate only the approved branded/proprietary STBs which are tested as per the technical Audit Manual and DPO's should include the STB models in their Annexure-3 declaration and should submit the updated Annexure-3 declaration if any new model STB is deployed for the viewership of pay channels.

Analysis:

152. In the view of the Authority, DRM should be so configured for specific type of STB/unique consumer subscription, that are procured and configured by the DPO. The DRM should not enable working/operation of any other type/brand/make of STB/unique consumer subscription, in the network.

Table 2 (16) of CP

153. In the CP, the following was mentioned:
"When infrastructure sharing is available, in such cases DRM shall be capable to support multiple DPOs."

154. In response, one association opined that at present, there are no guidelines issued by MIB regarding infrastructure sharing between IPTV operators, and as such, there are inter-alia jurisdictional issues concerning infrastructure sharing between IPTV operators. It is premature to include requirements relating to infrastructure sharing in the Draft Fourth Amendment / Draft Schedule-X since, the same appears to be a foregone conclusion of TRAI on these aspects.

Table 2 (17) of CP

155. In the CP, the following was mentioned:
"DRM should support content protection and usage rules enforcement for B2C model."

156. In response, one stakeholder suggested that DRM should support content protection and usage viewership data for B2C model. Another stakeholder enquired the meaning of "usage rules enforcement for B2C Model". Another organization also sought clarification regarding the usage rules.

Analysis:

157. The Authority is of the view that DRM should support content protection.

Table 2 (18) of CP

158. In the CP, the following was mentioned:
"DRM should be capable of handling at least 3 million license transactions per minute."

159. In response, one stakeholder suggested that DRM should be capable of handling at least 10000 license transactions per minute subject to the DPO subscriber base. Another stakeholder suggested that DRM should be capable of handling at least % of license transactions per minute. One stakeholder opined that

they are unsure whether regulator should state such requirement. They suggested that DPO should negotiate the numbers with the DRM vendor.

Analysis:

160. Enforcing this condition may increase the cost of investment especially for the small DPOs. Therefore, Authority is of the view that this decision should be left to the service provider. Accordingly, the clause Table 2 (18) has been deleted.

Table 2 (19) of CP

161. In the CP, the following was mentioned:
"DRM should support encryption of individual tracks of a content stream with individual keys, i.e., track level protection."

162. In response, one stakeholder suggested that DRM should support encryption of individual channels with individual keys and encrypt all the content available in the channel. Another stakeholder suggested that DRM should support encryption of individual services including all the pids comprising of that service with individual key for each service. A few stakeholders and an association opined that DRM would encrypt the complete URL. It's not same as scrambling to identify the video and audio track.

Analysis:

163. After due consideration, the Authority has made amendment to the Regulation.

Table 2 (21) of CP

164. In the CP, the following was mentioned:
"In case DPO has deployed hybrid STBs, DRM shall ensure that the over-the-top (OTT) App and any browser does not get access to the linear television channels offered by the DPO from its own system, and similarly, DRM for IPTV service should not get access to channels delivered through OTT platform. Provided that, all the mandatory requirements for DRM shall be complied by hybrid STBs."

165. In response, one association mentioned that the scope of the Draft Fourth Amendment and Draft Schedule-X should be limited to DRM requirements for IPTV service only. Another stakeholder opined that Hybrid STB should be defined. They further mentioned that every application should regulate access to its content independently, so the content decryption keys are only delivered in licenses of the system that delivers the content.

166. Another stakeholder suggested that in case DPO has deployed hybrid STBs, DPO Application integrated with the DRM shall ensure that the over-the-top (OTT) App and any browser does not get access to the linear television channels offered by the DPO from its own system, and similarly, DPO Application integrated with DRM for IPTV service should not get access to channels delivered through OTT platform. Provided that, all the mandatory requirements for DRM shall be complied by hybrid STBs.

167. One stakeholder suggested that Hybrid STB is an STB with access to internet as well as Linear services. DRM shall ensure that the over-the-top (OTT) App and any browser does not get access to the linear television channels offered by the DPO from its own system. DRM for IPTV service should not get access to channels delivered through OTT platform. Provided that, all the mandatory requirements for DRM shall be complied by hybrid STBs. DPO is free to integrate the OTT content on the UI along with linear content at his disposal. The OTT content has to be protected by OTT vendor by means of DRM and CPE certification.

168. Another organization suggested that in case DPO has deployed hybrid STBs, if the MSO is providing the linear television channel on IP delivery also either Unicast or Multicast, the DRM shall ensure that all the mandatory requirements are compiled by hybrid STBs. DRM shall also ensure that Any browser does not

get access to the linear television channels offered by the DPO. The IPTV channels should be accessible only in the specified STB and not in any other handheld device or computer.

Analysis:

169. ITU's Recommendation ITU-T J.298: Requirements and technical specifications of a cable TV hybrid set-top box compatible with terrestrial and satellite TV transport defines Hybrid STB as follows:
"*hybrid STB: A hybrid set-top box (STB) is a STB that uses multiple methods of receiving transmission signals with video and audio content.*
NOTE – For the purposes of this Recommendation, the dual streams will be IP based via the Internet protocols and cable, satellite and terrestrial television, based on the ITU-T J.83, DVB-S/S2, DVB-T/T2 or ISDB-T/Tb standards".

170. Though the hybrid STB may use multiple methods of receiving transmission signals with video and audio content, however for the purpose of this regulation, the Authority is of the view that it is pertinent to ensure that in a single instance such STB provides only one type of service. Accordingly, modifications have been made in the Regulation.

Table 2 (22) of CP

171. In the CP, the following was mentioned:
"There shall not be any active unique subscriber outside the database tables. Further, there shall not be an option to split DRM database for creation of more than one instance by a DPO or a vendor."

172. In response, one stakeholder mentioned that they are not sure if it's a relevant requirement.

Table 2 (24) of CP

173. In the CP, the following was mentioned:
"It shall be mandatory to have backup servers and logs of all activities carried out in main server shall be concurrently copied into the backup servers:
Provided that a log of all such instances shall be maintained along with date and time stamp, where the backup server has been used as the main server:
Provided further that the main and backup server shall always be in sync with regard all data, such as subscription data, STB UA/MAC ID details, entitlement level information, etc."

174. In response, one stakeholder mentioned that they appreciate the efforts to have better QoS for the users and it is in the right direction. However, this should be enforced on other types of DPO since majority of the subscribers are still under the legacy cable TV system or DTH.

Table 2(25) of CP

175. In the CP, the following was mentioned:
"DRM and SMS shall ensure that the access to database is available to authorized users only, and in "read only" mode only. Further, the database audit trail shall be permanently enabled.

Explanation: Database here refers to the database where data and log of all activities related to STB activation, deactivation, subscription data, STB UA/MAC ID details, entitlement level information, etc., is being stored."

176. In response, a few stakeholders and an association suggested that the word 'STB' should be replaced with 'STBs/Mac ID'.

Table 2 (26) of CP

177. In the CP, the following was mentioned:
*"**Provision of à-la-carte channels or bouquet**:*

(a) DRM (and SMS) shall be able to handle all the channels, made available on a platform, in à la carte mode.
(b) DRM (and SMS) shall have the capability to handle such number of broadcaster/DPO bouquets, as required by the DPO."

178. In response, one stakeholder opined that bouquet is irrelevant for DRM system.

Table 2 (28) of CP

179. In the CP, the following was mentioned:
"DRM shall have a provision to export the database/report for reconciliation with the SMS database. Further, there shall be a provision of reconciliation through secure APIs/secure scripts."

180. In response, one stakeholder opined that pure DRM may be just a slave of SMS and may not have any DB at all.

Table 2 (29) of CP

181. In the CP, the following was mentioned:
"DRM should have the following features:
(a) The entitlement end date in DRM shall be equal to the entitlement end date in SMS,
(b) The entitlement end date in DRM shall be open and SMS shall manage entitlements based on the billing cycles and payments."

182. In response, one stakeholder opined that DRM should have the following features: (a) The entitlement end date in DRM shall be equal to the entitlement end date in SMS. Another stakeholder opined that DRM should have the following features: (b) The entitlement end date in DRM shall be open and SMS shall manage entitlements based on the billing cycles and payments.

Analysis:

183. After due consideration, the Authority has made amendment to the Regulation.

Table 2(30) of CP

184. In the CP, the following was mentioned:
"There shall be unique license key required for viewing every 10 minutes in DRM deployed by DPO."

185. In response, one stakeholder suggested that there shall be unique license key required for viewing, the crypto period should be configurable to change at periodic interval in DRM deployed by DPO. Another stakeholder enquired if it is about the key rotation or license renewal period. They further opined that if it's the former, this is probably not feasible in the current systems in the industry. The latter is possible but in big deployments creates a lot of traffic between the clients and the HE.

Analysis:

186. The Authority is of the view that the unique license key should be a configurable parameter as per the DPO's business model. Accordingly, modifications have been made in the Regulation.

Table 2(31) of CP

187. In the CP, the following was mentioned:
"For every change in channels, fresh license keys should be issued by the DRM. License keys issued by DRM should be secure and encrypted. DRM must ensure that the authorization keys are not received by the STB from any other source other than the one specified by the IPTV system."

188. In response, a few stakeholders and an association suggested that the word 'STB' should be replaced with 'STB/APP'. Another stakeholder suggested that that for every change in channels, fresh license keys

should be issued by the DRM however the various packages can be created with bouquet of channels with same key. License keys issued by DRM should be secure and encrypted. DRM must ensure that the authorization keys are not received by the STB from any other source other than the one specified by the IPTV system.

Table 2 (33) of CP

189. In the CP, the following was mentioned:
"IPTV transmission has to be in multicast mode only just like cable TV transmission. There cannot be any such case where unicast is allowed. STBs with facilities for recording programs shall have a copy protection system (i.e., a feature which prevents reproduction of content and/or unauthorized copying and distribution of content) and such recorded content should not be transferrable to any other device."

190. In response, a few stakeholders and an association suggested that IPTV Transmission shall be agnostic to any network topology for both Multicast & Unicast methods provided it complies with all regulatory requirements. STBs with facilities for recording programs shall have a copy protection system (i.e., a feature which prevents reproduction of content and/or unauthorized copying and distribution of content) and such recorded content should not be transferrable to any other device.

191. Another stakeholder suggested that IPTV transmission should be in a closed network circuit just like cable TV transmission. STBs with facilities for recording programs shall have a copy protection system (i.e., a feature which prevents reproduction of content and/or unauthorized copying and distribution of content) and such recorded content should not be transferable to any other device.

192. A few stakeholders and an association suggested that IPTV transmission can be in both multicast and unicast encrypted way. STBs with facilities for recording programs shall have a copy protection system (i.e., a feature which prevents reproduction of content and/or unauthorized copying and distribution of content) and such recorded content should not be transferrable to any other device.

193. Another stakeholder suggested that IPTV transmission has to be in Local Network only and the IPTV streams should use only Private IP Address space as per Internet Assigned Numbers Authority (IANA). STBs with facilities for recording programs shall have a copy protection system (i.e. the recorded content should be encrypted with the same DRM and decryption should be allowed only during the subscription period of the subscriber for that content) and such recorded content should not be transferrable to any other device.

194. One stakeholder suggested that IPTV transmission is to be restricted to the private network of the DPO/LCO in either multicast/unicast format, IPTV should not be available/transmitted over the Internet. In case of unicast delivery the DPO has to use HTTPS along with TLS for secure point to point delivery of the content stream. The DPO can engage with Telco's for long distance transmission over a dedicated leased line or through a TLS encrypted tunnel in case of shared infrastructure. STBs with facilities for recording programs shall have a copy protection system (i.e., a feature which prevents reproduction of content and/or unauthorized copying and distribution of content) and such recorded content should not be transferrable to any other device.

195. Two stakeholders opined that IPTV is an operator driven and controlled platform in which the consumer directly interacts with equipment installed by operator in closed user group. IPTV system delivers digital television service using Internet Protocol (IP) over various access technologies i.e., broadband connection based on copper loop, optical fibre, wireless technologies etc.

196. One stakeholder suggested that All broadband distribution networks are unicast only and if unicast is not allowed for IPTV we need to build an exclusive network for IPTV and there is no business case to

implement. Another stakeholder opined that a separate IPTV clause is required, it's not directly related to DRM.

197. Another stakeholder suggested that IPTV transmission has to be in a controlled network, the DPO can distribute either in Unicast or multicast mode. STBs with facilities for recording programs shall have a copy protection system (i.e., a feature which prevents reproduction of content and/or unauthorized copying and distribution of content) and such recorded content should not be transferrable to any other device,

198. An association opined that Unicast is the basic feature of IPTV technology. Any restriction of IPTV to provide only multicast will reduce the IPTV service to cable services. Further, both GoI and TRAI has always provided for an enabling and technology neutral regime, therefore, no artificial restriction should be imposed on IPTV services. Such restriction, if imposed, will disable the IPTV providers to provide the best of the class services to consumers. Unicast as a technology is fully compliant with the extant legal and regulatory framework and is in the larger interests of end consumers without compromising with the rights and privileges of any other stakeholder in the IPTV value chain. Legal and regulatory framework in India is technology agnostic.

199. Another stakeholder opined that Multicast is a better way for live streams to be transmitted through IPTV on wired line network. All across the world, Multicast on IPTV has been working from more than a decade especially for pay channels and that too with high usage channels. Unicast IPTV is better for small-scale deployments, while Multicast IPTV is better for large-scale deployments with a high number of viewers. However, implementing Multicast requires specialized network hardware and software, which can be expensive and complicated.

200. An association opined that since Unicast mode allows IPTV services to touch open internet, it cannot be introduced for the IPTV service DRM, as it will enable the DPO to easily shift the unicast stream from closed network to open network, which has different jurisdiction and further is the cause of rampant piracy. Retransmission of linear TV channels envisaged under TRAI regulations is by way of "broadcast" only. Retransmission of TV channels in Multi cast mode within closed network meets the requirement of a broadcast. Only technologies fulfilling this requirement should be permitted as mode of retransmission for IPTV services. The mode of retransmission used for provision of IPTV services is to be Multi cast only. Since IPTV is a Broadcast service it can be deployed by Multi cast only. If Unicast mode is used for provision of linear TV channels via IPTV, then it is technically impossible to differentiate between IPTV and OTT at subscriber's end as using Unicast mode may enable the DPO to easily shift the Unicast stream from closed network to open network. Regulations cannot permit a back door for the IPTV service to be equated to internet enabled services.

Analysis:

201. The Authority believes that a "technology neutral" approach is one of the best methods to foster technology growth. Accordingly, the mode of delivery of multi channel television programmes to be used may be left to the service providers to decide based on their business model. However, it is pertinent that the system configuration should ensure that every television channel is available to every customer on selection to view, irrespective of the mode of delivery of multi-channel television programmes or the number of viewers seeking such channel at any point of time. Accordingly, modifications have been made in the Regulation.

Table 2 (34) of CP

202. In the CP, the following was mentioned:

"IPTV transmission should not be allowed to configure any content delivery network (CDN) in their system to deliver linear content to STBs."

203. In response, a few stakeholders and an association opined that IPTV transmission should be allowed to configure any content delivery network (CDN) in their system to deliver linear content to STBs, provided it

complies with all regulatory requirements. Another stakeholder suggested that IPTV transmission may be allowed to use Content Delivery Network (CDN) only in private network and should not be allowed to use any public content delivery network (CDN) to deliver linear content to STBs. Another stakeholder suggested that IPTV transmission should be in encrypted format and only the STB/CPE should be allowed to decrypt as per the subscription status. If CDN/Stream Multiplexer/Stream Multiplier is involved, it should not have any facility to decrypt and encrypt and should distribute the stream in the same format of the source stream in real-time.

204. A stakeholder suggested that only private CDN's can be used by the DPO and no public CDN should be allowed. Private CDN nodes can only be accessed by the DPO customer base and should not be accessible from any other network. Another stakeholder opined that CDNs help in overcoming the bandwidth bottlenecks in the distribution trunk lines. One stakeholder was of the opinion that a separate IPTV clause is required as this is not directly related to DRM. Another stakeholder enquired that if CDN is not allowed how the catchup content can be accessed? Yet another stakeholder suggested that IPTV transmission can be delivered using any of the technologies (with or without CDN) based on the convenience of the operator.

205. On the contrary, an association opined that in Multi cast mode, delivery of linear TV channels through IPTV does not require Content Delivery Networks (CDNs) however in the event Unicast mode is being used the DPO needs to configure CDNs to deliver the IPTV services and to manage bandwidth and network traffic. IPTV transmission should not be allowed to configure any CDN.

Analysis:

206. The Authority is of the view that an enabling and light-touch regulatory regime, which facilitates growth and technological developments while protecting the consumer's interest needs to be promoted. In accordance with the policy of 'light-touch regulation' and 'technology neutral approach', the clause has been deleted in the Regulation. However, it remains incumbent upon IPTV operator to ensure that sufficient safeguards are built-in to ensure content security and avoidance of any possibility of delivery of content beyond the closed IPTV network. The delivery of IPTV services has to be limited to authorised IPTV STBs or authorised unique subscription identities within the IPTV network.

Table 2 (35) of CP

207. In the CP, the following was mentioned:

"IPTV should not be allowed to deliver linear content to any other device except STB which has been whitelisted in DRM."

208. In response, a few stakeholders and an association suggested that the word 'STB' should be replaced with 'STBs/Mac ID (APP)'. A stakeholder opined that IPTV should be allowed to deliver linear content to any large screen devices like smart TVs & STB which has been integrated and declared to be tested with the DRM security. Two stakeholders suggested that it should be allowed on Android TV to avoid unnecessary burden on subscribers. Another stakeholder opined that perhaps a separate IPTV clause is required as it is not directly related to DRM.

Table 2 (36) of CP

209. In the CP, the following was mentioned:

"IPTV should have capability to implement session based/token authentication with token authentication duration to be controllable to few minutes."

210. In response, one stakeholder opined that perhaps a separate IPTV clause is required as it is not directly related to DRM.

Analysis:

211. After due consideration, the Authority has made amendment to the Regulation.

Table 2 (37) of CP

212. In the CP, the following was mentioned:
"IPTV system should not allow recording of linear channel at headend/network level. It should be allowed to be recorded at STB/DVR level only, without there being any option available to transfer such recorded content to any other device."

213. In response, a few stakeholders and an association suggested that IPTV system should allow recording of linear channel at headend/network level provided Content is DRM protected and only authorized STB should be able to playback the same in line with broadcasters' agreements in this regard. It should also be allowed to record at STB/DVR level, without there being any option available to transfer such recorded content to any other device.

214. Another set of a few stakeholders and an association suggested that recording in server side need to be allowed to provide DVR functions of channels and catchup of channel content. They also suggested additional amendments that IPTV system can do server-side recording and the recorded content need to store in encrypted way. And the content will be accessible and decrypted only with the DPOs STBs/Hybrid STBs/Application (APP). Two stakeholders also opined that recording at head end level should be allowed to support catchup-tv & time shift, as it is good features to promote IPTV. One stakeholder opined that a separate IPTV clause is required as it is not directly related to DRM.

Analysis:
To align with extant Guidelines and Regulations, the above clause has been removed in the Regulation.

Table 2. (38) of CP:

215. In the CP, the following was mentioned:
"The DRM should have following policies implemented:
(a) It should restrict user to editing or saving content in part or full.
(b) It should restrict user from sharing or forwarding or mirroring the content from the STB
(c) It should disallow user to take screen shots or screen grabs or screen-recording……"

216. In response, one stakeholder opined that (a)-(c) are a mix of loosely bound requirements: a) second part prevents PVR b) limits implementation of a home gateway c) DRM can't prevent putting a camera in front of the TV screen and capture the video.

Analysis:

217. Since recording of linear channel is allowed at STB/unique consumer subscription /DVR level, the Authority is of the view that in Table 2. (38) (a), the following words may be deleted: *"or saving content in part or full"*

Table 2 {38(d)} of CP

218. In the CP, the following was mentioned:
"It should lock access to authorized STBs only."

219. In response, one stakeholder suggested that it should lock access to authorized STB and smart TV only. A few other stakeholders and an association suggested that the word 'STB' should be replaced with 'STBs/APP'.

Table 2 {38(e)} of CP

220. In the CP, the following was mentioned:
"It should have Geo blocking, that enables a broadcaster to determine and instruct the DPO/IPTV service provider to restrict the broadcast of TV channels in locations."

221. In response, one stakeholder suggested to remove the Geo Blocking clause. They opined that as per the DAS license provided by MIB, the DPO is free to provide the services as per the licensed territory. Hence this clause contradicts the provision.

Analysis:

222. The Authority is of the view that DRM system should have Geo blocking feature, accordingly modifications have been made in the Regulation.

Table 2. (39) of CP

223. In the CP, the following was mentioned:
"The DRM should have the capability of being upgraded over-the-air (OTA) so that the connected STBs always have the most upgraded version of the DRM."

224. In response, a few stakeholders and an association suggested that the word 'STBs' should be replaced with 'STBs/APP'.

Table 2 (40) of CP

225. In the CP, the following was mentioned:
"The DPO shall ensure that the DRM is updated/upgraded at regular intervals by installing necessary patches, error corrections, additions, version releases, etc. so as to ensure protection of channels and content at all times."

226. In response, one of the organizations suggested that the word 'regular intervals' should be replaced with 'whenever required'.

Analysis:

227. The Authority agrees with the view that in the above-mentioned clause the words 'regular intervals' needs to be appropriately amended to ensure that the DRM is kept up to date by the DPO by installing necessary patches, error corrections, additions, version releases, etc. for protection of channels and content at all times. Accordingly, modifications have been done in the regulation.

Table 2 (41) of CP

228. In the CP, the following was mentioned:
"No such functionality should be added to or removed from the DRM which compromises security of channels. DPO shall be responsible for encryption of channels' signals before their transmission through its IPTV platform using DRM integrated STBs. All costs / expenses (by whatever name called) that are required to be incurred or become payable for such upgradation and for retransmission and/or delivery/distribution of channels to subscribers shall be borne solely by such DPO. The DPO shall employ all reasonable security systems and procedures to prevent any loss, theft, piracy, un-authorized use, reception or copying of channels or any part thereof and shall notify broadcasters as soon as practicable after it becomes aware that such an event has occurred."

229. In response, a few stakeholders and an association suggested that the word 'STB' should be replaced with 'STBs/APP'. One stakeholder opined that this clause is for DPO not DRM.

Analysis:

230. Any piracy or content hacking causes market disruption and huge financial loss to the service providers. In addition, it causes loss of tax revenues for the government. The framework prescribed by the Authority is expected to reduce piracy and benefit the entire ecosystem. Further, in the Copyright Act appropriate remedies exists to address piracy related issues.

Table 2 (43) of CP

231. In the CP, the following was mentioned:
"DPO shall promptly, and at it sole cost and expense, correct any issues with the DRM (such as bugs, defects, omissions or the like) that prevents subscribers from accessing the DRM integrated STBs or channels through the DRM integrated STBs."

232. In response, a few stakeholders and an association suggested that the word 'STBs' should be replaced with 'STBs/APP'. One of the organizations stated that the clause was not clear at all.

Table 2 (44) of CP

233. In the CP, the following was mentioned:
"DPO shall provide broadcasters with video and audio codecs supported by the DRM integrated STBs. The DPO shall ensure that no such changes/modifications are made to such codecs parameters that will require broadcasters to incur any expense for delivery of channels / content that are free from viewer discernible problems (including, without limitation, video with no audio, audio with no video or significant signal distortion.)"

234. In response, one stakeholder opined that it is not related to DRM.

Table 2(45) of CP

235. In the CP, the following was mentioned:
"DRM should ensure that the integrated STBs are verifiably located within India by reference to internet protocol address and service address. Further, the DRM shall not permit delivery to an Internet/mobile device. The DRM must use industry-standard means (including IP-address look-up technology with screening and blocking of proxies (including anonymizing and spoofed proxies)) to prevent delivery of channels to IP addresses outside of India or to proxies."

236. In response, a few stakeholders and an association suggested that the word 'STBs' should be replaced with 'STBs/APP'. One stakeholder opined that this really limits the operator to deliver content only to STBs. Most of the operators in the world and in India want their DRM protected content to be delivered to mobile devices as well. Another stakeholder suggested that DRM should ensure that the integrated STBs are verifiably located within India by reference to internet protocol address and service address. The DRM must use industry standard means (including IP-address look-up technology with screening and blocking of proxies (including anonymizing and spoofed proxies)) to prevent delivery of channels to IP addresses outside of India or to proxies. One stakeholder suggested that DRM should ensure that the integrated STBs and Smart TVs are verifiably located within India by reference to internet protocol address and service address. The DRM must use industry standard means (including IP address look-up technology with screening and blocking of proxies (including anonymizing and spoofed proxies)) to prevent delivery of channels to IP addresses outside of India or to proxies.

237. An association opined that they do not support the deletion of the underlined words, "Delivery to an Internet/mobile device cannot be permitted" from the above-mentioned clause.

Analysis:

238. With technological developments content can be viewed using application based services provided such arrangement meets extant licensing/regulatory framework. Therefore, the Authority is of the view that app based services, may also be permitted. Soft STBs (App based) may also be used for running IPTV services. In such cases, the unique id for each subscriber is required. In all such cases, STB or the CPE should have a unique Mac id that should be paired or locked with a user account. The Authority is of the view that DRM must ensure and lock the viewership to single device by single STB/unique consumer subscription or any device by ensuring MAC ID based authentication. Accordingly, modifications have been made in the Regulation.

Table 2 (46) of CP

239. In the CP, the following was mentioned:
"DRM should ensure that channels are accessible on integrated STBs of only such subscribers who are then-current, valid subscribers of the distributor of channels, and such confirmation must take place prior to the DRM actually delivering (or authorizing the delivery of) channel to the integrated STBs of such subscribers."

240. In response, a few stakeholders and an association suggested that the word 'STBs' should be replaced with 'STBs/APP'. One stakeholder suggested that DRM should ensure that channels are accessible on DRM certified STB and Smart TV of only such subscribers who are then-current, valid subscribers of the distributor of channels. Authorization to the content access should be implemented at both middleware and DRM levels.

Table 2 (48) of CP

241. In the CP, the following was mentioned:
"The DRM shall not allow insertion of any self-promotion and/or any third party and/or paid for advertisements (including banners and aston bands) before, during or after transmission of linear channels.

242. In response, a few stakeholders and an association suggested that the DRM may allow insertion of any self-promotion and/or any third party and/or paid advertisements (including banners and Aston bands) before, during or after transmission of linear channels subject to requisite agreement with the concerned Broadcasters in this regard. Another stakeholder suggested that the DRM may be allowed to insert any promotion, advertisement and/or notifications in a manner that it is not interfering with the playback of the linear channels and the content is played with covering any portion of it.

243. Two stakeholders suggested that it should be allowed if there is no objection by channel provider and the operator takes formal approvals for the same. Advertisement banners or Asto bands should be allowed at some place holders in such a manner that will not interrupt or block the content. One stakeholder opined that DRM can't distinguish between Operator's (DPO's) ads and the ones coming from third party.

Analysis:

244. The Authority is of the view that the broadcaster's feed should not be tampered/altered by the Distribution Platform Operators in any manner. The Distribution Platform Operators are bound under agreements executed with the broadcasters as per the provisions of Interconnection Regulations 2017 (as amended). The DRM should not have any feature to insert any content (including advertisement, portion, etc) by itself. Accordingly, modifications have been made in the Regulation.

Table 2 (49) of CP

245. In the CP, the following was mentioned:
"The DRM shall not permit subscribers to record and/or store channels/content from channels."

246. In response, a few stakeholders and an association suggested that the DRM may permit subscribers to record and/or store channels/content from channels subject to requisite agreement with the concerned broadcasters in this regard. Another set of a few stakeholders and an association suggested to remove the clause. They argued that already they have recording facility in Cable TV STBs. Recording functionality is allowed.

247. One stakeholder suggested that IPTV system should not allow recording of linear channel at headend/network level. It should be allowed to be recorded at STB/DVR level only, without there being any option available to transfer such recorded content to any other device.

Analysis:

248. The clause at Table 2 (49) was a repetition of earlier clause, therefore it has been removed in the Regulation.

Table 2 (51) of CP

249. In the CP, the following was mentioned:
"The DPO shall not sub-license the DRM and/or any rights granted to the DPO by the broadcaster to any entity for re-transmission of channels to subscribers."

250. In response, a few stakeholders and an association suggested that the DPO may sub-license the DRM and/or any rights granted to the DPO by the broadcaster to any entity for re-transmission of channels to subscribers subject to requisite agreement with the concerned broadcasters in this regard. Another stakeholder suggested that the DPO shall not sub-license the DRM and/or any rights granted to the DPO by the broadcaster to any entity for retransmission of channels to subscribers, However the DPO can appoint the Distributors and LCOs to deliver the channels to the subscribers. One stakeholder commented that this is how the content distribution works in many cases.

Analysis:

251. After due consideration, the Authority has made amendment to the Regulation.

Additional Clause

252. One stakeholder suggested two additional clauses: 1) DRM System to be deployed on secured server and 2) OTT Apps currently transmitting Linear Channels to be verified their mode of transmission. As HLS or Dash is not allowed.

Additional Clause

253. A few stakeholders and an association suggested an additional clause that for all the mandatory requirements of DRM to be suited for STBs/Hybrid STBs/Application (APP). They further opined that in growing technology, DPO can provide IPTV in app based with all security needs and without violating any security norms of TRAI.

(F) DRM Requirements in so far as they relate to fingerprinting for IPTV services

Table 3 (1) of CP

254. In the CP, the following was mentioned:
"The DPO shall ensure that it has systems, processes and controls in place to run fingerprinting at regular intervals."

255. In response, one stakeholder opined that it is not related to DRM, rather to the STB app.

Table 3 (2) of CP

256. In the CP, the following was mentioned:
"The STB should support both visible and covert types of finger printing."

257. In response, a few stakeholders and an association suggested that the word 'STB' should be replaced with 'STB/APP'. One stakeholder opined that it is not related to DRM, rather to the STB app.

Table 3 (3) of CP

258. In the CP, the following was mentioned:
"The fingerprinting should not get invalidated by use of any device or software."

259. In response, one of the organizations opined that it is not related to DRM, rather to the STB app.

Table 3 (4) of CP

260. In the CP, the following was mentioned:

"The fingerprinting should not be removable by pressing any key on the remote of STB."

261. In response, a few stakeholders and an association suggested that the word 'STB' should be replaced with 'STB/APP'.

Table 3 (6) of CP

262. In the CP, the following was mentioned:
"The finger printing should be such that it can identify the unique STB number or the unique VC number or the MAC ID."

263. In response, a few MSOs and an association suggested that the finger printing should be able to give the numbers of characters as to identify the unique STB and/or the MAC ID of STB/APP. One stakeholder opined that there is no VC in DRM.

Table 3 (7) of CP

264. In the CP, the following was mentioned:
"The finger printing should appear on the screens in all scenarios, such as menu, Electronic Programme Guide (EPG), settings, blank screen, and games etc."

265. In response, one stakeholder suggested that fingerprinting should appear on the screens in all scenarios, such as menu, Electronic Programme Guide (EPG), settings, blank screen and in all screens of the Linear channel Interface in the case of Hybrid STB.

Table 3 (8) of CP

266. In the CP, the following was mentioned:
"The location, font color and background color of fingerprint should be changeable from head end and should be random on the viewing device."

267. In response, one stakeholder suggested that it is for application not DRM.

Table 3 (9) of CP

268. In the CP, the following was mentioned:
"The finger printing should be able to give the numbers of characters as to identify the unique STB and/or the MAC ID."

269. In response, a few MSOs and an association suggested adding 'of STB/APP' at the end of above clause.

Table 3 (10) of CP

270. In the CP, the following was mentioned:
"The finger printing should be possible on global as well as on the individual STB basis."

271. In response, a few stakeholders and an association suggested that the word 'STB' should be replaced with 'STB/APP'.

Table 3 (13) of CP

272. In the CP, the following was mentioned:
"The DRM shall support and enable forensic watermarking at STB level."

273. In response, a few stakeholders and an association suggested that the word 'STB' should be replaced with 'STB/APP'. Another stakeholder opined that similar security features should also be implemented for other types of DPOs.

Table 3 (14) of CP

274. In the CP, the following was mentioned:
"The DRM shall have the capability to run fingerprinting at regular intervals of at least one fingerprinting every ten (10) minutes on a 24x7x365 basis) and provide broadcasters with the fingerprint schedule on request."

275. In response, one stakeholder opined that for anti-piracy, the client may randomize the times of the fingerprinting on each device, therefore the schedule can't be provided.

Analysis:

276. The Authority is of the view that the DRM should have the capability to run fingerprinting with at least one fingerprinting every ten (10) minutes on a 24x7x365 basis. DRM should have a feature to publish report of fingerprinting schedule for defined interval. The DPO shall make such report available to broadcaster on request.

Table 3 (15) of CP

277. In the CP, the following was mentioned:
"The DRM shall have the capability to run customized fingerprinting at such intervals as may be requested by broadcasters. Further, DPOs shall mandatorily run fingerprinting at regular intervals with a minimum of 2 fingerprints per hour on a 24x7x365 basis and provide broadcasters with the fingerprint schedule on request."

278. In response, one stakeholder opined that the clause is for application not DRM.

Analysis:

279. The clause of Table 3 (15) was a repletion of earlier clause, therefore it has been removed in the Regulation.

(G) DRM Requirements in so far as they relate to STBs

280. In response, a few stakeholders and an association suggested that the word 'STBs' should be replaced with 'STBs/APP'.

Table 4 (1) of CP

281. In the CP, the following was mentioned:
"All STBs should have a DRM content protection."

282. In response, a few stakeholders and an association suggested that the word 'STBs' should be replaced with 'STBs/APP'. One stakeholder enquired on which STBs was the above clause applicable.

Table 4 (2) of CP

283. In the CP, the following was mentioned:
"The STB deployed should be capable to support content decryption, decoding and DRM license evaluation."

284. In response, a few stakeholders and an association suggested that the word 'STB' should be replaced with 'STB/APP'.

Table 4 (3) of CP

285. In the CP, the following was mentioned:
"The STB should be capable of displaying fingerprinting inserted from Headend through DRM/SMS. The STB should support both targeted channel fingerprinting as well as all global fingerprinting."

286. In response, a few stakeholders and an association suggested that the word 'STB' should be replaced with 'STB/APP'.

Table 4 (4) of CP

287. In the CP, the following was mentioned:
"The STB should be individually addressable from the Head-end."

288. In response, a few stakeholders and an association suggested that the word 'STB' should be replaced with 'STB/APP'.

Table 4 (5) of CP

289. In the CP, the following was mentioned:
"The STB should be able to receive messages from the Head-end."

290. In response, a few stakeholders and an association suggested that the word 'STB' should be replaced with 'STB/APP'. One stakeholder opined that it is unrelated to DRM.

Table 4 (6) of CP

291. In the CP, the following was mentioned:
"The messaging character length should be minimal 120 characters."

292. In response, one stakeholder suggested that messages of length of 1 to 120 or more characters shall be supported.

Analysis:

293. The Authority agrees with the suggestion of the stakeholder that the messaging character length should be minimal of up to 120 characters. Accordingly, modifications have been made in the Regulation.

Table 4 (7) of CP

294. In the CP, the following was mentioned:
"There should be provision for global messaging, group messaging and the individual STB messaging."

295. In response, a few stakeholders and an association suggested that the word 'STB' should be replaced with 'STB/APP'.

Table 4 (9) of CP

296. In the CP, the following was mentioned:
"The STBs should be addressable over the air to facilitate OTA software upgrade."

297. In response, a few stakeholders and an association suggested that the word 'STBs' should be replaced with 'STBs/APP'.

Table 4 (10) of CP

298. In the CP, the following was mentioned:
"The STBs with facilities for recording the programs shall have international standard copy protection system."

299. In response, a few stakeholders and an association suggested that the word 'STBs' should be replaced with 'STBs/APP'.

Table 4 (11) of CP

300. In the CP, the following was mentioned:
"The STB should have a provision that fingerprinting is never disabled."

301. In response, a few stakeholders and an association suggested that the word 'STBs' should be replaced with 'STBs/APP'.

Table 4 (12) of CP

302. In the CP, the following was mentioned:
"The watermarking network logo for all pay channels shall be inserted at encoder end only. In case of infrastructure sharing, it shall be as per terms and conditions of infrastructure sharing."

303. In response, one association suggested that the words 'In case of infrastructure sharing, it shall be as per terms and conditions of infrastructure sharing' should be deleted. In support of their argument, they opined that at present, there are no guidelines issued by MIB regarding infrastructure sharing between IPTV operators, and as such, there are inter-alia jurisdictional issues concerning infrastructure sharing between IPTV operators. Another stakeholder suggested that the first line of the clause should read as follows: The watermarking network logo for all channels should be inserted at encoder/Transcoder end only.

Table 4 (13) of CP

304. In the CP, the following was mentioned:
"DRM deployed should be able to send scroll messaging which should be only available in the lower part of the screen."

305. One stakeholder suggested that the word 'DRM' should be replaced with 'DRM/SMS'. One stakeholder opined that it is not related to DRM.

Analysis:

306. It is learnt that SMS can execute the required function without DRM involvement. Accordingly, modifications have been made in the Regulation.

Table 4 (14) of CP

307. In the CP, the following was mentioned:
"DRM deployed should be able to geo tag STB deployed in the network for security."

308. In response, a few stakeholders and an association suggested that the word 'STB' should be replaced with 'STB/APP'. One stakeholder opined that the clause is probably for the application, not DRM.

Table 4 (15) of CP

309. In the CP, the following was mentioned:
"STB should take all commands directly from DRM not from any intermediate servers."

310. In response, a few MSOs and an association suggested that the word 'STB' should be replaced with 'STB/APP'. Another stakeholder suggested that STB should take all commands directly from SMS/DRM not from any intermediate servers. One stakeholder opined that there are many commands not related to security/DRM that STB can fetch from other sources.

Table 4 (16) of CP

311. In the CP, the following was mentioned:
"STB should not have feature to download (direct or side download) any 3rd party App/APK (Including on Hybrid STB's if any) and should not have access to any browser."

312. In response, a few MSOs and an association suggested that STB may have a feature to download 3rd party App/APK directly from in-built app store and may also have access to a browser. However, side loading of

any third-party app should not be allowed on the STB. At the same time, STB having an integrated browser to serve relevant Hybrid STB features, it should not allow any unauthorized access to IPTV through browser.

313. A few stakeholders and an association suggested that the clause needs to be removed. Another stakeholder opined that this is a very valid point and the same to be amended for other DPO platforms like DTH Hybrid boxes. Two stakeholders suggested that STB should be allowed to download / side load app or apk to install 3rd party apps. Until unless it is not counterfeiting the copyrights law.

314. Another association suggested that the clause should read as follows: IPTV STB should not have feature to download (direct or side download) any 3rd party App/APK and should not have access to any browser."

Analysis:

315. The Authority is of the view that STB/unique consumer subscription while using IPTV infrastructure should not have feature to download (direct or side download) any 3rd party App/APK and should not have access to any browser. Accordingly, modifications have been made in the Regulation.

Table 4 (17) of CP

316. In the CP, the following was mentioned:
"STB should not be able to access the authorization keys from any other source except from the IPTV system through the IPTV closed network. DRM must ensure that the authorization keys are not received by the STB from any other source other than the one specified by the IPTV system."

317. In response, one stakeholder enquired about the meaning of authorization keys.

Table 4 (18) of CP

318. In the CP, the following was mentioned:
"STB should not have any play store to download 3rd party App."

319. In response, a few stakeholders and an association suggested that STB may have a feature to download 3rd party App/APK directly from in-built app store and may also have access to a browser. However, side loading of any third-party app should not be allowed on the STB. At the same time, STB having an integrated browser to serve relevant Hybrid STB features, it should not allow any unauthorized access to IPTV through browser.

320. Another association suggested that the clause should read as follows: IPTV STB should not have any play store to download 3rd party App.

321. A few stakeholders and an association suggested that the clause needs to be removed. A few stakeholders suggested that STB can have Play store / app store to download 3rd party app. Another organization opined that it is not what modern STBs and operators offer. There can be an App Store with a limited set of allowed apps. Another MSO suggested that the same should be amended for other DPO platforms like DTH Hybrid boxes.

Analysis:

322. The Authority is of the view that no play store should be accessible for enabling download, etc. when STB/unique consumer subscription, is functioning in the IPTV network.

Table 4 (19) of CP

323. In the CP, the following was mentioned:
"STB should have copy protection – HDCP with version 2 and above, DHCP, CGMS & macrovision with version 7 and above."

324. In response, a few stakeholders and an association opined that Schedule III regulations can be followed which is more than enough for content security. Another stakeholder opined that the point lacks merit. They mentioned that majority of the cable TV viewers are having legacy TVs. It is very unlikely that the mentioned protocols would be supported by these legacy TVs and other devices. Another stakeholder suggested that STB should have copy protection – HDCP with version 2.

Analysis:

325. The Authority is of the view that the Regulation should specify STB/unique consumer subscription should have copy protection and the means of achieving the same should be left to the service providers.

Table 4 (20) of CP

326. In the CP, the following was mentioned:
"DPO system should have capability to maintain un-editable logs of all activity and configurations including download of any App at STB end."

327. In response, a few stakeholders and an association opined that with all these content protection and anti-piracy systems which are requested by TRAI and broadcaster can be met out by the DPOs DRM, SMS and STBS/APP. There is no compromise in security. So, restricting internet and OTT for anti-piracy is baseless. Another MSO opined to amend for other DPO platforms like DTH hybrid boxes.

Analysis:

328. The Authority is of the view that DPO system should have capability to maintain un-editable logs of all activity and configurations including download or upgrade of IPTV services App (if any) at STB/unique consumer subscription end. Accordingly, modifications have been made in the regulation.

Table 4 (21) of CP

329. In the CP, the following was mentioned:
"The DRM should not allow delivering linear TV channels on HLS, Smooth Streaming, Dash & HTTP/TCP."

330. In response, a few stakeholders and an association suggested that the DRM may allow delivering linear TV channels on HLS, Smooth Streaming, Dash & HTTP/TCP subject to IPTV service being not accessible on Open Internet, i.e., IPTV Service should strictly be accessible in a managed network with DRM protection.

331. Another set of a few stakeholders and an association opined that IPTV transmission via multicast will not prevent content theft and piracy. With TCP HTTP even a better security can be provided and Quality of service can be improved as it has feedback for every single session of customer. And even in case of hacking it can be easily identified with feedback from session.

332. Another stakeholder suggested that the DRM should allow delivering linear TV channels to any protocols as desired by DPO. Another stakeholder suggested that only the DRM supported streaming containers/formats (MPEG-TS, MpegDash, hls etc) and network protocols (http, hls, TCP, UDP etc) should be deployed. Two stakeholders suggested that DRM may allow delivering linear TV channels in any mode enabling content protection to avoid piracy. One stakeholder opined that it's about blocking OTT, which contradicts the common modern trend.

Analysis:

333. The Authority is of the view that the DRM should not allow delivering linear TV channels on Internet. The delivery of multi channel television programmes should remain in a closed network within the device. Accordingly, modifications have been made in the regulation.

Table 4 (22) of CP

334. In the CP, the following was mentioned:
"The STB should have forced messaging capability including forced finger printing display."

335. In response, a few stakeholders and an association suggested that the word 'STB' should be replaced with 'STB/APP'.