BROADBAND INDIA FORUM
"Think Tank for Digital Transformation"

BIF Response to TRAI Consultation Paper on Framework for Technical Compliance of Conditional Access System (CAS) and Subscriber Management Systems (SMS) for Broadcasting & Cable Services

At the outset, we wish to compliment TRAI for bringing out this important Consultation Paper on Framework for Technical Compliance of Conditional Access System (CAS) and Subscriber Management Systems (SMS) for Broadcasting & Cable Services.

Please find below BIF's position in this regard and our responses to the questions as provided in the CP:

Introduction:

Globally, until about 1990, it was thought that implementing a digital broadcast network is impractical due to its implementation cost. However, with the advances in digital technology in both the algorithmic and hardware implementation side, broadcasters and consumer electronics manufacturers recognised the importance of switching to digital technology for improving both the bandwidth efficiency and the robustness. Today's users require information, infotainment and entertainment anywhere, at any time and on any device, if possible, interactively and with the highest possible service quality. Modern broadcasting concepts try to cope with these demands that can only be satisfied by digital technologies. Digital terrestrial broadcasting can be designed to work with roof-top antennas but also with small antennas built into portable devices and for mobile reception.

Digital broadcasting networks have to constantly cope with changing media environments and new requirements, due to: demand for more services of higher technical quality and with improved coverage; new technology leading to improved efficiency in the use of the spectrum; changing regulations on the use of the spectrum; and a wider range of consumer devices, ranging from large screens and multi-channel audio equipment to handheld devices.

On the SMS side, the plethora of options to constantly manage and cater to the diverse requirements of each individual customer, resulted in a vastly improved set of

processes and procedures, driven by upgraded SMS systems. The challenge has always been to ensure the parallel development of both the Broadcast side as well as the Service delivery side to ensure that in tandem they provide the widest choice to the end users, while also catering to their disparate needs, while remaining competitive.

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

BIF RESPONSE

In a Digital Addressable System (DAS) based environment, CAS and SMS form an integral part, and the quality of service is dependent on the CAS and SMS systems being deployed by the DPO. Therefore, in order to ensure seamless transmission of signals of television channels from broadcasters to consumers, maintaining addressability, and preventing piracy, it is necessary that certain quality benchmarks and a proper framework be put in place to ensure that standardisation & proper certification are in place for the CAS and SMS systems.

The extant regulatory framework, vide Schedule III of Telecommunication (Broadcasting and Cable) Services Interconnection (Addressable Systems) Regulations, 2017, provides for macro level parameters/features that the DPOs must comply with. The regulations provide for certain checks under the provisions of audit of the DPO systems that entail testing of the relevant features as prescribed under the Schedule III.

Addressability is the ability of a digital device to individually respond to a message sent to many similar devices. In the pay television distribution framework (DTH or Cable or through IPTV, etc.) an addressable system enables and controls the distribution of television channels, by encrypting the signal and ensuring only authorized users can receive channels using a set-top-box (STB) and TV set.

The Security of a CAS System depends on the Algorithm used for ECM, EMM Encryption. The contents of ECMs and EMMs are not standardized and each Conditional Access System uses different ECMs and EMMs. In fact, the security of a

given CAS system depends primarily on the efficiency of the algorithm used for ECM, EMM encryption. Such algorithms are closely guarded secrets of the company. The CAS module in the STB carries relevant ECM, EMM decryption algorithms. Majority of the CAS deployed in India work either on CSA1 or CSA2. CSA3, though the advanced algorithm, may not be supported by most of the scramblers, STBs and other legacy hardware currently deployed in India. Moreover, adopting CSA3 also has significant financial implications as it would require replacement of deployed scramblers, STBs and other hardware.

Subscriber Management System (SMS) is essentially the management center of the CAS. It is a combination of hardware and software, integrated with the CAS server. SMS stores and manages details of each subscriber, and the TV channels that are subscribed to by them. Based on the channels that the subscriber has paid for, the SMS asks for Entitlement Management Messages (EMM) from the Subscriber Authorization System (SAS). It also generates the bill for LCOs as well as Subscriber enabling MSO to charge them accordingly. The SMS functions as the front end to the operators' equipment, and practically performs all operational functions required for day-to-day managing of the business. Important functions carried out by the SMS are:

A) **Subscriber related SMS** deals with subscriber (STB) activation/deactivation, bulk subscriber suspend/resume, blacklisting STBs, etc. It also stores and manages subscriber data such as subscriber name, subscriber Mobile Number, subscriber address, etc. These entries can be updated whenever changes take place. The SMS server generates unique customer IDs for each subscriber and carries out STB pairing function wherein the customer IDs are paired with the STB numbers and the Smartcard numbers (for card-based STBs) or Chip ID numbers. This is an important functionality related to activation/deactivation or blacklisting of STBs.

B) **Local Cable Operators (LCO) related SMS** contains data of the Operators like Operator Code, Operator Name, Operator Address, etc. SMS contains Admin IDs for MSOs and MSOs can generate LCO IDs for their linked operators, thus enabling them with activation/deactivation, etc. of their STBs. LCOs can also download all their STBs' details with subscriber names and addresses.

C) **Billing System SMS** provides a host of billing functions such as itemized billing, bill scheduling, supporting multiple tax systems, etc.

D) **Stock Management by using SMS** - the MSOs can manage their stocks for the STBs through SMS. SMS can individually show the entries of Activated STBs, Deactivated STBs, Faulty STBs and Blacklisted STBs.

E) **Channel Information SMS** store and manage all the information about channels available on the MSO platform, package, bouquet or scheme creation, etc. It enables management of channels and program bouquets subscribed by individual subscribers.

Since SMS is not a standardized product, different versions deployed by operators can provide various other functions and features such as subscriber alerts, LCO applications, etc. SMS is also responsible for enabling and managing the important functions of fingerprinting and OSDs (On Screen Display), etc.

The Authority has very rightly identified two key issues in this CP, namely - (a) **content protection and (b) the factual reporting of subscriptions.**

It is essential to understand the consequence of shortcomings in these two critical areas, viz. CAS system which enables the content protection and restricts piracy of TV channels, and SMS system which reports the subscription details. The consequences are:

- A sub-standard CAS may lead to piracy of signals as it would be easy to hack or circumvent its security system. Piracy may lead to compromise of the subscribers STB and subscriber information without his knowledge, and the subscriber may be subject to punishment under cybercrime laws since his STB or VC (viewing card credentials) is being used for piracy, which will be injustice to the subscriber.
- The sub-standard CAS system may fail frequently leading to subscribed channels not available to the subscriber who would have already paid for his subscription, leading to the subscriber not being able to view the channel even after paying for the same.
- The correct information of the subscribers is not available, and therefore the billing and exchange of subscription fees will not be accurate, leading to disproportions.
- The collection of subscription fees without any records or without appropriate records cannot be shown in the DPOs or LCOs revenue. Hence it gives rise to un-accounted money due to under-declaration (declaring lower number of subscribers than actually connected to the DPO).
- The government loses equivalent tax revenues when the subscriptions are not declared correctly.
- Subscribers who are not declared may not receive a receipt for their subscription, leading to unaccounted transaction/s.
- A subscriber who is not declared may have paid the LCO/DPO, but since his subscription is not accounted, he may face disconnection after an audit and may not get to view the channels that he believes he has subscribed to. This is unfair to the subscriber
- Such an undeclared subscriber may not be able to register a complaint to any consumer redressal court/forum to resolve his problems with regard to reception of the channels at his home, leading to injustice to the subscriber.

Hence, it is very important that the features and standards of the CAS and SMS should be reviewed and updated to ensure content protection and factual reporting of subscribers.

Recommended Important features that should be part of CAS and SMS:

1. *CAS should be so configured that it should not allow to make any changes to the status of the Subscribers VC directly from the CAS system. Any changes such as activation, deactivation, packages, etc. should be through the SMS systems only. SMS data and CAS data for all subscribers must always be synchronized*

2. *CAS & SMS vendors should independently provide data of monthly subscribers count per instance to the broadcasters, from main and backup system, whether active or not at the time of reporting, unless decommissioned permanently.*

3. *Historical and continuous logs of CAS & SMS and packages with date and time stamps should be available in live/on-line servers up to the last 2 preceding years. There must be no missing data in the log files or missing log files itself. Logs provided by the CAS and SMS vendors should be encrypted. The CAS & SMS should not allow any external log file to be re-encrypted and saved as its system generated log files.*

4. *Program information should be mandatory to appear on the Electronic Programme Guides (EPGs) display generated by the STBs. These EPGs must be updated from the headend and must show the entire days EPG at least. The EPG must be displayed along with the DPO's name and logo, date and time*

5. *Any channel should not be duplicated in any form in the network. The DPO should complete all the streams and transmit it with all services as encrypted and the same should reach the subscriber. The same cannot be modified in any form by the LCO*

6. *The details of all instances of CAS and SMS installed with address and date of installation must be published on the web portal of the Autonomous body. The Autonomous body to issue unique CAS and SMS ID for each installation of each CAS & SMS and upload the same on their portal transparently. The DPO should also declare the details of its headend and network and also details of each of its LCOs on the Autonomous body's portal. Any change at the DPO's end should be updated*

in the Autonomous body's portal within 7 days. Failure to do so should attract penalties on part of the DPO

7. *Each separate CAS installation by a CAS vendor in a DPO's headend should have a unique ID, and this ID should be visible in the transport stream as part of DVB table. This information must be updated in the Autonomous body's portal and any change made must be updated on the portal within 7 days of implementation*

8. *All TS information mandated by DVB standards should be provided fully and accurately by the DPO in the network. The information should include, but not be limited to network name, network ID, NIT table with all frequency information, etc. This should be as per the information submitted to the Autonomous body and displayed on its portal. The DPO will face penalties if there are disparities.*

9. *The CAS & SMS shall be able to permanently blacklist VC and STB numbers that have been involved in piracy. Such VCs or STBs cannot be re-deployed. A list of all such VCs and STBs must be displayed on the Autonomous body's portal transparently and updated every 15 days*

10. *CAS and STB must meet the CSA-2 or CSA-3 specification and embedded SoC (System on Chip) hardware. Older generation STBs which do not comply with the security requirements should have a sunset date starting at the earliest*

11. *CAS and SMS vendors must provide 24x7, 100% engineering & local support (from India) to the DPOs. CAS and SMS system should be installed as 1+1 system for 100% availability.*

12. *SMS systems should generate reports in a structured manner clearly indicating the number of LCOs attached to the MSO, the number of subscribers under each LCO, the packages/channels subscribed, start and end dates of the subscriber's subscription per package/channel, and must include the invoice details generated by the MSO per subscriber*

13. *DPOs shall use their SMS system to authenticate their subscribers through registered mobile numbers through OTP system (MFA) at start of subscription and every 6 months thereafter*

14. *CAS & SMS of DPOs must be capable to add/modify new channels/packages within 7 days of the Broadcaster and DPO coming to an agreement on carrying the channel*

15. *CAS & SMS provider shall provide the complete setup of CAS & SMS system installed at DPOs headend including the BOM, its description for each line item, and IP address of each addressable system forming the CAS & SMS system with detailed connection drawing of the Headend*

16. *Only one watermark (DPOs logo) should appear on all STBs of DPO*

17. *In STBs with recording facility (Internal/external storage such as DVR/PVR and Cloud DVR) content should get recorded along with entitlements and should not play out if channel/STB is deactivated or subscription is disabled. Similarly, the FP must also be recorded and displayed when the recording is played back. The recorded programs should be encrypted such that without the same combination of STB and VC, the recording should not play back*

18. *Trigger and display of a minimum of 2 Finger prints per hour on a 24x7 basis throughout the year should be possible. Finger Printing schedule to be provided to broadcaster on request*

19. *DPO's STB should not allow any app download and installation. If installed, DPO must have remote control from headend to delete it.*

20. *The DPO must provide forensic watermarking which should be unique per STB, without affecting the broadcaster's forensic watermarking or BARC watermarking if available in the channel signal. The broadcaster's watermarking and BARC watermarking should pass till the subscriber without and disruption or modification.*

21. *No clone STB should be operated in the network. It is essential that in the CAS & SMS declaration, the DPO also declares that his network has no clone STB or duplicated VC. Also, DPO's CAS should have the capability to identify and eliminate such STBs. In case such clone STB is found to be operated, then the DPO should be penalized and must be delisted*

22. *For content protection, DPOs must deploy technology to insert forensic watermarking to identify which particular STB of the DPO has been used for the piracy of the signals*

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

BIF RESPONSE

It is evident that the CAS and the SMS are central to the Pay TV networks. They are the key elements governing content security and proper accounting of subscriptions and revenues. Accordingly, the regulatory framework notified by TRAI incorporates provisions regarding the minimum requirements to be complied by the CAS and SMS deployed by the DPOs. Ideally, it is expected that the CAS and SMS which complies with Schedule III is installed and the certificate from CAS and SMS vendor confirms that the same complies with Schedule III. Also, it is assumed that only one CAS and SMS system is installed in one headend. However, it has been observed that multiple CAS & SMS systems are operated in a headend and all the CAS and SMS system are not declared. Hence it is essential that the certificate from CAS and SMS vendor should be verified with the specifications and performance of the CAS and SMS system installed.

The Telecommunication (Broadcasting and Cable) Services Interconnection (Addressable Systems) Regulations, 2017 dated 3rd March 2017, and notified by TRAI, cover technical and commercial arrangements between the Broadcasters and the Distributors for providing television services to the consumers. Subsequently, TRAI

also issued Telecommunication (Broadcasting and Cable) Services Interconnection (Addressable Systems) (Amendment) Regulations, 2019 (7 of 2019) on 30th October 2019 (herein after called Amendment Regulations). As per the Regulations, the digital addressable systems deployed by the DPOs for distribution of television channels through cable & satellite, are required to meet the minimum criteria as stated in the Schedule III of the Regulations. The addressable system requirement as provided for in Schedule III is to be complied by the Distributors of television channels. In order to ensure compliance with these minimum criteria, the authority notified The Telecommunication (Broadcasting and Cable) Services Audit Manual dated 8th November 2019, which provides formalities to be followed for the Audit initiated by the Distribution Platform Operator (DPO) vide sub-Regulation (1) of Regulation 15 or by the Broadcaster vide sub-Regulation (7) of Regulation 10 and sub-Regulation (2) of Regulation 15.

The regulation also permits the broadcaster under proviso as per Sub-Regulation (2) of Regulation 15, to disconnect signals of television channels, after giving written notice of three weeks to the distributor, if such audit reveals that the addressable system being used by the distributor does not meet the requirements specified in the Schedule III.

Hence, Schedule III of Interconnection Regulation, 2017, provides the minimum criteria to be met by the digital addressable systems deployed by the DPOs for distribution of television channels through cable & satellite and sets into place a statutory framework that ensures that any change, modification and alteration made to the configuration or version of the addressable system (CAS, SMS and other related systems of the DPO and/or distribution network of DPOs) do not in any way compromise the system, and that all the equipment including software meets the statutory compliance requirements.

Further, effective compliance of statutory provisions is ensured through the comprehensive Audit Manual published by the Authority. It creates a common framework and uniformity in the technical and subscription audit. 'The Audit Manual' is a guidance document for stakeholders. This manual does not supersede any provision(s) of the extant regulations process for all digital addressable systems used in the broadcasting sector. It provides a well-defined audit procedure and a checklist of all the equipment/software/accessories, etc. used in digital addressable systems. The audit manual builds the trust and confidence among all stakeholders in broadcasting sector, which in turn, results in reducing disputes among the stakeholders arising during provisioning of TV channel/s or at the time of renewal of Interconnection agreements, etc.

With the extant policy and regulatory framework in place and supported by technology, distribution of television services should ideally be a smooth and problem free operation. However, despite being crucial in provisioning quality services to end-consumers, there are hardly any prescribed benchmarks for digital addressable systems.

Further, presently, the standards are as provided by Interconnect Regulations, which are generic in nature and merely lay down the minimum criteria to be met by the deployed CAS and SMS. These requirements allow all types of CAS and SMS systems to exist in the eco-system. The DPOs that deploy the CAS and SMS and the vendors who supply the CAS and SMS should be responsible and accountable for such CAS and SMS system's (*as supplied by them*) performance and integrity, as the certification of compliance is being provided by such CAS and SMS vendors.

Hence the following additional compliance measures are recommended to ensure that the CAS and SMS system is complaint during its operative life cycle:

a) Set up and Autonomous Body: An Autonomous Body be set up which would be the monitoring entity for CAS & SMS compliance to Schedule III. It must be made mandatory for the DPO as well as the CAS and SMS vendor, to submit all information of the installations at the DPO's headend separately to the Autonomous Body and the said information should then be displayed on the portal of the Autonomous Body
b) Empanelment of CAS and SMS vendors with the Autonomous Body: As a first requirement to ensure that sub-standard CAS and SMS systems are not deployed, the CAS and SMS vendor must be empaneled with the Autonomous Body. Further the CAS and SMS system must comply with all specifications and requirements as mentioned in Schedule III (new). The CAS and SMS vendor must submit self-declaration certificate to the Autonomous Body for the CAS and SMS system to be installed at the DPO headend along with complete details of the system installed and details as mentioned in Schedule III (*new*). This declaration is a confirmation by the CAS and SMS vendors that the systems installed comply with all the requirements of Schedule III and also an undertaking that if there are

irregularities found during audit, the same will be immediately rectified. In case of installation of sub-standard CAS and SMS systems in violation of parameters/specifications laid down in Schedule III by the CAS and SMS vendors, the same may lead to disqualification of such CAS and SMS vendors from their empanelment with the Autonomous Body

c) Audit at installation: An audit of the installed addressable systems be conducted mandatorily by the broadcaster or by any empaneled auditor appointed by the broadcaster to verify if self-declaration certificate and the installed system comply with Schedule III. The cost of such audit should be borne equally by the DPO and the Broadcaster. However, in case discrepancies are found and re-audit is required, then cost of such subsequent audit should be borne by the DPO. Deviation of parameters of the installed system from the certification produced must be considered as breach and both DPO and CAS and SMS vendor must be liable to penalties

d) Audit during operations: Audits to be conducted by the Autonomous Body every 6 months, or in case of discrepancies found on the ground by broadcasters to ensure compliance with Schedule III. During such audits in case any sub-standard/non-compliant CAS and SMS systems are found, the same are to be replaced immediately and CAS and SMS vendors provisioning such non-compliant CAS and SMS systems are to be removed from the Autonomous Body's panel and also black listed in the Autonomous Body's portal as well as TRAI's and MIB's portals.

e) Penalties for non-compliance: Imposition of significant penalties on DPOs whose CAS and SMS do not comply with the laid down parameters/specifications- TRAI has made various provisions under the Interconnection Regulations and QoS with an intent to ensure broadcasting services are provided through the digital addressable systems which are efficient in provisioning quality & transparent services, and provides wider options to consumer along with the ability to exercise

choice by consumers in channel selection. In addition to this, the regulations also intend to enable transparent business transactions based on verifiable parameters to improve the transparency in the sector. However, contrary to the intentions of TRAI, under reporting and piracy of content by various means continue to adversely impact the growth of the sector. Once such an ambiguity is proved, significant penalties must be imposed on the defaulting DPO with a clear time period of payment of such penalties and consequences if it is not made as per this time period. If the DPO is found to be in non-compliance of the provisions of the Schedule III on three occasions, then action to be initiated by TRAI against such defaulting DPOs by sending a list of such defaulters to Ministry of Information and Broadcasting ("MIB") with recommendation or request for cancellation of licenses of such non-compliant DPOs.

f) Post Audit recommendations: The Autonomous Body must audit the defaulting CAS and SMS installations along with the DPO and the CAS & SMS vendors involved. In case it finds enough evidence that the CAS & SMS do not comply with the specifications of Schedule III (new), then that CAS & SMS system is liable to be declared as sub-standard/non-compliant. The CAS & SMS system should be given an opportunity to prove that their systems comply with the standards as per Schedule III (new) within 30 days in the lab of the Autonomous Body as well as the DPO later. If the CAS and SMS vendor cannot satisfactorily prove compliance even after that, it will be declared as sub-standard/non-compliant. A list of defaulting CAS and SMS vendors to be published on the websites of TRAI, MIB and Autonomous body stating non-compliance of parameters/specifications laid down under Schedule III in the concerned make and model of the CAS and SMS. Such sub-standard/non-compliant CAS & SMS systems will be removed from the Autonomous Body's panel and will not be able to install any of their systems in India.

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

BIF RESPONSE

Yes, we believe there is a need to do so. Although Schedule III of the Interconnection Regulations 2017 sets out the minimum requirements to be met by digital addressable systems, there are several issues that arise due to deployment of non-tested and non-certified CAS and SMS. Since Schedule III requirements are generic in nature, it allows all type of CAS and SMS systems to exist in the eco-system. Most of the major vendors undertake elaborate measures and use advanced embedded security to ensure adequate mechanism towards content security. However, quite-a-few vendors do not take such measures and deploy systems based on non-standard security solutions, vulnerable to hacking. Such systems put the content security at risk, thereby distorting the markets. It is important to note that the market functions as a whole and any such distortion leads to market failure. Also, declaration of the correct number of subscribers is an important aspect, and non-standard CAS and SMS systems may not be able to report this correctly which again distorts the markets.

The regulatory framework released by TRAI establishes a trust-based transparent regime and provides opportunities to aspiring entrepreneurs to enter into television distribution business. Such new entrants may lack technical expertise and experience. Such players are likely to be beguiled by cheaper products, therefore exposing their networks to piracy and other contraventions. Many a time DPOs choose some CAS and SMS systems not fully aware about the technical complexities. However, subsequently they suffer when either broadcasters deny them the feed of TV signals on the grounds that they do not meet mandatory technical requirements for OEMs of such CAS and SMS vendors, or ask more money to provide required upgrade to fulfill technical requirements. Protection of such MSOs is also important so that all CAS/SMS systems operational in cable TV networks adhere to minimum technical requirements. There are instances, where unscrupulous operators take advantage of the gaps in the operational and oversight mechanisms and play around the system.

It is essential to form a neutral entity, an Autonomous body, who will be solely responsible to ensure that the CAS and SMS vendors comply with the requirements of Schedule III. With the changing and fast improving technology, it becomes essential to review the standards and requirements of a CAS and SMS system and update them on

a regular basis with appropriate testing and evaluation. The Autonomous body will be responsible to keep the specifications and Schedule III updated in line with the technology.

The Autonomous body must constitute a functional lab (which can be the CAS and SMS vendors lab to start with) immediately where the CAS and SMS systems would be tested, evaluated and benchmarked before the same model of hardware and software is deployed at any headend. The CAS and SMS system must successfully meet all the performance specifications as outlined in Schedule III, and only after that shall a certification be provided by the Autonomous body for deployment of that model at any headend.

The Autonomous body should chalk out the framework which would be robust as the body would be completely focused to work on these requirements. This framework is required to be defined appropriately in order to ensure that there is no possibility of manipulation of records and piracy/illegal re-transmission of signals of channels by deployment of sub-standard CAS and SMS systems.

It has also been noticed that such sub-standard CAS and SMS systems do not have an option to back up all the critical data which would render any audit exercise futile. Hence benchmarking the CAS and SMS system is a must.

The Framework for CAS/SMS systems to benchmark the minimum requirements must include the technical requirements and specifications as mentioned in the update of Schedule III.

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

BIF RESPONSE

Implications and possible threats from deployment of sub-standard CAS/SMS: The issues reported from time to time indicate that a lot of proprietary solutions have made way into the Indian market offering cheap security. Because of this, not just the

end consumer, but different stakeholders in the ecosystem such as the service providers and the Government also suffer.

Impact on Consumers: Sub-standard CAS increases the workload of the operators and creates confusion among the end consumers, who may get non-uniform services from the same operator. It may result in frequent disruptions and hence poor Quality of Service (QoS) for the end consumer. The consumers get locked in with STBs with limited functionality because of sub-standard proprietary software, which in turn, results into wastage of money for them as they may have to replace the STB many times during the subscription period.

Impact on the Broadcasters: Broadcasters and content developers are impacted directly by deployment of sub-standard CAS/SMS, as security of their content is compromised. It leads to content piracy and redistribution without the knowledge and permission of the broadcasters and the operators. Further, certain features such as LCN, etc. cannot be implemented seamlessly across all STBs in a network, owing to sub-standard proprietary software. Sub-Standard CAS/SMS deployment also results in increasing the probability of misreporting usage and subscription numbers, which may result into revenue loss to the broadcasters, and disputes with the operators in cases of under/excess billing. Frequent disruption of services leads to creating a lot of issues on the ground as the revenue collection is disrupted. It may attract lawsuits against the operators which may have the potential to disrupt their entire business operations.

Impact on MSOs/DPOs/Pay TV Distributors: Since the majority of the CAS companies do not have their own SMS, Middleware (MW) and User Interface (UI), it increases the dependency of the MSOs on several Third party (TP) software solution providers. Since most of the MSOs lack in technical expertise as they have migrated from Analog Cable TV regime, they fall prey to sub-standard solutions and face support issues subsequently. MSOs get locked down to only one kind of boxes/STB original equipment manufacturer (OEM) with non-standard implementation of middleware features, and incur high maintenance overhead to maintain and execute such proprietary software. It increases their operational cost as technical issues arise. Their flexibility to extend features is reduced. Additionally, it creates tension with broadcasters, as there is a potential to manipulate the readings and log numbers which may result into misrepresentation of the data and may affect the revenue for all parties concerned due to excess/under billing. Since deployment of a sub-standard proprietary software can result into content leakage and piracy, it may lead to various legal and commercial actions by the content owner and hence disrupt the complete operations of the MSOs. Further, in absence of Hardware Specifications and Performance Parameter standards, MSOs may keep on investing into poor/cheap quality hardware which results into wastage of time, generation of a lot of e-waste,

resource wastages in terms of financial resources, human resources as well as management resources.

Impact on the Government: Sub-standard CASs defeat the very purpose of the Government of India's DAS (Digital Addressable System) initiative. Sub-standard CAS/SMS deployment results into increasing the probability of misreporting the usage and subscription numbers which may result into revenue loss to the operators, broadcasters, as well as to the government in form of taxes. Further, CASs which follow accepted global standards can be useful when changes from the middleware perspective such as STB Interoperability, are implemented by the government.

To ensure that consumers and other stakeholders do not suffer from want of regular upgrade, proper checks and balances should be put in place so that whenever a new method for piracy is deployed for piracy of signals, the same may be addressed by ensuring a mandatory upgrade. It is observed that in most cases with every new method invented for piracy, an upgrade of the CAS or/and SMS system and/or STB becomes necessary for fixing the piracy. In the absence of regular updates and upgrades by CAS & SMS vendors, typically for the ones which are patches of known security vulnerabilities, the security of CAS, SMS and STBs will be compromised, making the system more vulnerable and prone to piracy of broadcasters' channels, resulting in revenue loss for DPOs, broadcasters and the government. Subscribers will also suffer since (a) they might not be able to change the channels as per their choice, (b) they might be unknowingly infringing the Intellectual Property Rights of the content, (c) they might suddenly experience disconnection of their STB due to hacking of their STB or their credentials in the DPOs SMS system, and many other issues. Also, the unsupported CAS and SMS will be unable to meet the quality of standards as mandated by regulation.

The safeguards which are necessary to ensure that the consumers and all other stakeholders do not suffer for want of regular upgrade/configuration by CAS/SMS vendors are as follows –

1. An active Service Level Contract between the DPO and the CAS & SMS vendor is a must.

2. CAS and SMS systems should be installed on CAS/SMS vendor recommended servers with proper IT security systems and protocols such as firewalls and other secure features as specified.

3. CAS, SMS and Set Top Boxes ("STBs") should be secure and should run with latest security features which makes regular upgradation of system essential.

4. A CAS / SMS vendor who is unable to provide local technical support and SLA, should be deregistered and disqualified to operate in India, and should not be allowed to install any of its systems in India. Such list of CAS and SMS vendors should be always published in the portals of the Autonomous Body, TRAI and MIB.

5. Regular examination of quality of signals (video and audio) provided to subscribers catered by small DPOs shall also be undertaken. The Autonomous Body can conduct regular checks of the signal quality delivered to the subscribers at regular intervals or as requested by a large number of subscribers of a particular DPO on a regular basis. The findings of the Autonomous Body will be final, and their recommendations would have to be honored and implemented by the DPO. In case a DPO is unable to rectify the same for more than 6 months, penalties may be applicable till such time that they are able to resolve the issue.

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

BIF RESPONSE

There is a clear need to consider developing an overarching framework for standardization, certification and testing of various components of addressable

systems, i.e. CAS and SMS. Further, effective compliance of statutory framework is essential to build the trust and confidence among all stakeholders.

In India, the technical benchmarks and standards for security testing of digital addressable systems are not in place presently. Therefore, it would be appropriate to study the process of development of a technical framework, its adoption and implementation consisting of testing methodology, certification and accreditation. A general process of establishing a testing framework follows different modes, including the following, amongst others:

a. Emergence as de facto framework/standard: tradition, market domination, etc.

b. Developed by a common industry body in a closed consensus process: Restricted membership and often having formal procedures for due process among voting members in a full consensus process. Open to all interested and qualified parties, and with formal procedures for due-process considerations.

c. Written by a government or regulatory body.

d. Written by a corporation, union, trade association, etc.

Once the framework/test document is ready and notified, a formal certification adds credibility to the process. It is the provision whereby an independent body gives a written assurance, i.e. a certificate that the product, service or system in question meets specific requirements. Accreditation is the formal recognition by an independent body, generally known as an accreditation body, that a certified body operates according to international standards.

Standardization, Certification and Accreditation Process in India:

A) **Bureau of Indian Standards (BIS):** The standards process in India is largely government led with the Bureau of Indian Standards publishing a majority of products and services related Standards. The Bureau of Indian Standards (BIS) is the National Standards Body of India established under an Act of Parliament (The Bureau of Indian Standards Act, 1986, revised as The Bureau of Indian Standards Act, 2016) and represented as the India member on ISO. Only standards published by BIS have the status of Indian Standards. BIS is involved in various activities like standards formulation, certification of products, hallmarking, testing and calibration scheme, and more.

(i) **Product Certification by BIS**: Product Certification by BIS has been put into place since July 2013, and is intended to guarantee quality, safety and reliability. BIS Certification is provided in India under different types of schemes as follows:

a. Product Certification

b. Systems Certification

c. Foreign Manufacturers Certification Scheme (FMCS)

BIS certification is normally voluntary in nature. However, BIS requires compulsory certification and registration for products which impact the health and safety of consumers. BIS Act, 2016, empowers the Central Government to notify compulsory BIS Certification or Registration of a product. Penal provisions for better and effective compliance and to enable compounding of offences for violations have also been made stringent under BIS Act, 2016. Compulsory Registration Scheme (CRS) has been adopted by ministries such as Ministry of Electronics & Information Technology (MeitY) and Ministry of New and Renewal Energy (MNRE) for mandating product conformance to Indian Standards. The grant of licence and its operation under Compulsory Registration Scheme are carried out as per the conformity assessment scheme under Scheme - II of Schedule - II of BIS (Conformity Assessment) Regulations, 2018.

(ii) Further, government agencies may make it compulsory for foreign manufacturers to obtain a BIS product certification license for the products they intend to export to India under the **Foreign Manufacturers Certification Scheme (FMCS).** Under the provisions of this scheme, license is granted to a Foreign Manufacturer for use of Standard Mark on a product that conforms to an Indian Standard.

Apart from BIS, there are other **sector specific SDOs (Standard Development Organisations) viz. TSDSI in case of Telecom** which are involved in the process of developing or formulation of standards, testing and certification.

B) **Quality Council of India (QCI)**: QCI is an apex body responsible for establishing a transparent and credible accreditation system. QCI is governed by a Council comprising of 38 members and has an equal representation of Government, Industry and other Stakeholders. QCI has four Accreditation Boards involved in accreditation programmes. Each board is functionally independent and works within their core areas of expertise: i. National Accreditation Board for Certification Bodies (NABCB); ii. National Accreditation Board for testing & calibration Laboratories (NABL); iii. National Accreditation Board for Hospitals and healthcare providers (NABH); and iv. National Accreditation Board for Education & Training (NABET). Further, QCI develops accreditation standards to support accreditation programs where such standards are not available at the national/international level.

C) **Telecommunication Engineering Centre (TEC)**: Telecommunication Engineering Centre (TEC) is a technical body representing the interests of the Department of Telecommunications (DoT), Ministry of Communications & IT, Government of India. The main services of TEC include:

i. Standardisation: Prepare specifications of common standards about Telecom network equipment, services and interoperability. Published specifications of TEC are of three types namely Generic Requirements (GRs), Interface Requirements (IRs) and Service Requirements (SR).

ii. Testing and Certification: The Indian Telegraph (Amendment) Rules, 2017, provide that every telecom equipment must undergo prior mandatory testing and certification. TEC has been designated as the Telegraph Authority for the purpose of administration of Mandatory Testing and Certification of Telecom Equipment (MTCTE) procedure and Surveillance Procedure, and for formulation of Essential Requirements as per Indian Telegraph (Amendment) Rules, 201714, ART XI, Testing & Certification of Telegraph, (Rule 528 to 537)

D) **Standardization Testing and Quality Certification (STQC) Directorate:** Standardization Testing and Quality Certification (STQC) Directorate is an attached office of MeitY, Government of India. It provides quality assurance and conformity assessment services in the area of Electronics and Information Technology (IT) related to Information Security, Software Testing/Certification and Development of National Level Assurance Framework in IT and software sectors through countrywide network of laboratories and centres. They are one of the Registered Certifying Bodies (RCBs) for various International Standards. STQC laboratories have National/International accreditation and recognitions in the area of testing and calibration. In the area of IT & e-Governance, STQC offers quality assurance services as per National and International standards to the industry.

An independent, autonomous, neutral body ("Autonomous Body") should be set up for defining the framework for CAS and SMS in India. This body shall be entrusted with the task of defining the framework for CAS and SMS through a consultative process and with the involvement and support of relevant stakeholders. The recommendations made by the Autonomous Body will be final and binding and acceptable by all stakeholders and TRAI. This Autonomous body will perform the following functions –

a. Prepare a framework for specifying the common standards with regard to CAS and SMS systems.

b. Through its research and lab tests, come up with various recommendations every 12 months on various upgrades and updates that should be implemented in the CAS, SMS and STBs to make the complete eco system very robust and at the same time ensure very high customer experience and satisfaction as they would be focusing their energies in solving these issues.

c. Come up with new ideas and policy recommendations to TRAI and MIB after studying the practical on-ground situation and issues, and ways to resolve the same keeping the entire eco system in focus.

d. Develop expertise to imbibe the latest technologies and results of R&D.

e. Provide technical advice to TRAI and Telecom Disputes Settlement Appellate Tribunal.

f. Carry out regular audits of deployed CAS and SMS systems in order to check for compliance of the parameters/specifications laid down in Schedule III.

g. Issue certificates of approvals.

h. Work on a Block Chain solution to ensure that there is complete transparency of the number of subscribers connected to any DPO. This system, if implemented properly, will be very close to eliminating the under declaration faced by the industry. A very brief approach to guidelines of the Block Chain mechanism is that every transaction that a DPO does with his subscriber will be recorded and will be transparently available to all stakeholders and will be conducted through the “miners” in the block chain. The movement of a subscriber from one DPO to another will be possible once all dues owed to the DPO are cleared. If the LCO / DPO attempts to migrate the subscribers from one DPO to the other without clearing the dues, the transaction would not realise due to existing uncleared dues and so on in the Block Chain solution. Eventually all subscribers and the channels subscribed information will be

available transparently to all the stakeholders. Information of any DPO who might have got delisted would be available transparently as no transaction with that DPO will be possible to be executed. In short, this mechanism will benefit the entire eco system and all its stake holders.

i. It shall be the responsibility of the CAS and SMS vendors to get themselves accredited from the Autonomous Body once in 6 months.

j. Any CAS or SMS system which is decommissioned must be reported back both by the DPO as well as the CAS and SMS vendor to the Autonomous body and the broadcaster. On the date of decommissioning, the list of final subscribers report, logs etc. must be shared with the broadcaster. If during any audit the decommissioned system is found to be alive and existing and not reported to the Autonomous body in advance, it would be a violation and would result in penalties up to cancellation of the DPO license as well as delisting of the CAS and SMS vendors. A list of such defaulters will be made available on TRAI's, MIB's and the Autonomous Body's websites. Further, such a defaulting CAS and SMS vendor shall not be empaneled, and the CAS and SMS system will not be allowed to be installed for the next 3 consecutive years in India. Furthermore, such defaulting CAS and SMS vendors will be obligated to fulfill their obligations under any existing contract/s.

k. The Autonomous Body should have the responsibility to set up systems and protocols for monitoring of piracy and the novel ways being devised each day for piracy of TV signals.

l. The Autonomous Body will be responsible for carrying out regular audits, recognizing and suggesting required upgrade/change in configuration in the CAS and SMS of any DPO.

m. The Autonomous Body will issue certification of compliance to CAS and SMS vendors basis a live CAS and SMS lab installation before being implemented. These certifications should have a validity of 6 months. The CAS and SMS suppliers have to ensure that their certificate is valid at all times when they are conducting any business with any of the DPOs licensed to operate in India.

n. Only the CAS and SMS systems of the vendors empaneled with the Autonomous body to be used by DPOs.

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

BIF RESPONSE

There are different frameworks and standards that are used globally for creating and administering television broadcast standards. Some of the major standards are listed below:

1. European Standards

2. Digital Video Broadcast (DVB) Standards

3. Integrated Services Digital Broadcasting (ISDB) Standards

4. Advanced Television Systems Committee (ATSC) Standards

5. MovieLabs ECP Specifications

The structure and process of European Standards Organization is similar to BIS. However, all the other standards like DVB, ATSC and ISDB are made by industry

consortiums/associations. For example, DVB project is an international industry consortium that develops international open standards for digital television broadcasters and receivers.

There is an absence of an overarching regulatory framework for standardization, testing and certification of CAS and SMS deployed in India. Although Schedule III of the Interconnection Regulations, 2017, sets out a macro level framework, it only provides for the minimum requirements to be fulfilled by digital addressable systems. Since the criteria laid out in Schedule III are generic in nature, it does not control deployment of sub-standard solutions which are vulnerable to hacking, thereby putting content security at risk. The extant regulatory framework vide Schedule III, only ensures conformity with Regulations, under the provisions of Audit of the DPO systems that entail testing of the relevant features, whereby if in the opinion of a broadcaster the addressable system being used by the distributor does not meet requirements specified in the Schedule III, he is permitted to disconnect signals of television channels, as per proviso to Sub-Regulation (2) of Regulation 15. There is no regulatory requirement for checking conformity to Indian Standards. However, this does not protect the interest of small MSOs who have installed sub-standard CAS and SMS due to lack of technical knowledge.

There is also an absence of an overarching regulatory framework for standardization, testing and certification of conditional access systems deployed by distributors. CAS and SMS are pivotal for the Digital Addressable Broadcast eco-system and are responsible for delivery of the content in a secure & encrypted manner only to authorized subscribers. Hence, there is an immediate need for drafting and deployment of adequate standards for content security for conditional access systems.

Existing Digital Video Broadcasting (DVB) standards are already an industry and worldwide accepted standard for unidirectional broadcast for sending digital TV programs over satellite, cable, and terrestrial networks, as is evident by its wide adoption by all major technology vendors. Under the DVB standard, conditional access system (CAS) standards are defined in the specification documents for DVB-CA (Conditional Access), DVB-CSA (Common Scrambling Algorithm) and DVB-CI (Common Interface). However, these standards only define a method by which one can obfuscate a digital-television stream, but the contents of ECMs and EMMs are not standardized and as such, they depend on the conditional access system being used, which as discussed earlier, are proprietary in nature. In addition to conformity with DVB Standards, major CAS vendors in India also comply with MovieLabs Enhanced Content Protection specifications for new deployments, and undergo Cartesian Robustness Tests in order to license premium UHD content from production studios. These specifications have been developed by a consortium of major Hollywood

studios. Though, these are not statutory standards, they've become a de-facto standard for premium content protection in the industry.

Apart from industry driven standards, Bureau of Standards (BIS) is also in the process of formulating standards for conditional access system (CAS). In BIS, the Audio, Video, Multimedia Systems and Equipment Sectional Committee, LITD 07 is responsible for preparation of Indian Standards relating to: a) Audio, video and multimedia systems and equipment, and b) Acoustics, electroacoustic and related instruments. LITD 07 Sectional Committee has representation from relevant ministries of the Government, TRAI, CDAC, STQC, major distribution platforms, 42 major CAS vendors, chip manufacturers, device manufacturers and academicians. Presently LITD 07 Sectional Committee, in collaboration with all its members is in the process of developing draft standards for security testing of conditional access system (CAS). Presently, an ad-hoc group consisting of the operators, chip manufacturers, concerned ministries and organizations of the Government has been formed to further deliberate on the need, title, scope and roadmap for this draft standard.

In view of the above, it is evident that establishing recognized standards, certification, accreditation and testing procedures can be done in a number of ways. It can be industry driven where specialized agency(ies) can develop and publish standards in their domain areas. Subsequently, underlying provisions can be incorporated in requisite licensing and regulatory framework.

Another option exists where the Licensor (MIB in India) or the Regulator (TRAI) can formulate and issue the technical compliance framework. The framework may be developed through their own consultative processes or, by adopting/incorporating relevant Indian/International standards. In such case, the task of effective oversight and implementation may also be performed as per license/regulatory conditions. The Regulator/Licensor in the process will have to ensure that the technical framework is developed with the support and involvement of industry stakeholders. Such involvement can happen through structured committees or through wider stakeholder consultations. 'Technical Criteria' should be formulated in a transparent manner through a consensus process by the committees comprising of experts from all concerned areas such as technology vendors, producers/manufacturers of devices, R&D centers, regulatory bodies, etc. In case the framework is defined by the licensor/regulator, there will be a case for conducting the testing of systems for conformity of such standards. There are independent accredited labs that can help in establishing such conformity tests and issuing relevant certifications. In such a scenario, the licensor/regulator may authorize empaneled organizations such as Broadcasting Consultants India Limited (BECIL) to conduct tests that establish conformity of CAS/SMS systems to such license condition/regulatory

provisions. Alternatively, the technical framework for Content Security in Digital Addressable Systems can be developed by an independent agency/industry body or standards organization. Conformity assessment for compliance to such framework/standards may be entrusted with existing certification agencies like BIS, STQC Directorate, QCI, etc. Such assessment may include product testing, product certification and conformity to quality management systems, etc.

It is suggested that the Autonomous Body should carry out testing and certification of CAS, SMS and STBs. The Autonomous Body shall be responsible for carrying out audits (*extensive review and detailed assessment of the CAS and SMS systems*) for testing and certification of the CAS and SMS systems once in 6 months and provide reports of such audits to the broadcasters. These audits may be conducted by the Autonomous Body on any given day with prior notice of three working days. Such testing of the CAS and SMS systems at regular intervals by the Autonomous Body will ensure compliance of the laid down framework

At present there are already CAS and SMS systems put in place by the DPOs. The DPOs have made large investments in setting up their systems and the STBs which work with such CAS and SMS systems have been bought and placed by them on the ground. The biggest challenge would be to ensure that such STBs work with the new/upgraded CAS and SMS systems. If not, then the DPOs would face huge losses. The DPOs should be accorded a period of 6 months to ensure that the new/upgraded CAS and SMS systems are installed, and such STBs connect and work with the new/upgraded CAS and SMS systems. Further it shall be the responsibility of all CAS and SMS vendors to get compliance certification from the Autonomous Body within 4 months from the implementation of the new framework. Furthermore, a sunset date, i.e. 1 year from the date of implementation of the new framework, to be laid down for removal of non-compliant CAS and SMS systems.

The Autonomous Body will be responsible for carrying out an audit of the CAS and SMS of DPOs to check for compliance and/or upgradation at any given point in time. Post audit, the reports will be made available to broadcasters and TRAI. In case any DPO is found to be in non-compliance of the provisions of the Schedule III on three occasions, action to be initiated by TRAI against such defaulting DPOs by sending a list of such defaulters to Ministry of Information and Broadcasting ("MIB") with

recommendation or request for cancellation of licenses of such non-compliant DPOs. Penalties extending up to cancelation of license (*in case of repeated violations*) by MIB be implemented in order to ensure compliance. Further, in case of deployment of sub-standard/non-compliant CAS and SMS systems, a list of defaulting CAS and SMS vendors to be published on the websites of the Autonomous Body, TRAI and MIB stating non-compliance of parameters/specifications laid down under Schedule III in the concerned make and model of the CAS and SMS systems deployed by such defaulting CAS and SMS vendors in India. In case of more than 1 such default, such defaulting CAS and SMS vendors should be removed from the Autonomous Body list of empaneled CAS and SMS vendors after 1 event of default.

It is submitted that there is no element of deterrence vis-à-vis DPOs who are found in violation of Interconnect Regulations. It is imperative that financial disincentive in the form of appropriate penalties, extending up to cancelation of license (*in case of repeated violations*) by MIB be implemented before formulation of any suitable model in order to ensure compliance. To make any model work it is imperative that deterrents be put in place in order to ensure that the laid down parameters/specifications are complied with by one and all.

The TRAI Act, 1997, as amended, empowers TRAI under Sec. 29 to impose a fine up to INR 2 lakhs for every contravention of its directions. However, in many cases where violations of the laid down regulations have come to TRAI's notice, no directions have been issued. In certain cases, where directions have been issued there have been no penalties imposed.

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

BIF RESPONSE

Once the new Common Minimum Framework is established after public consultation with all stakeholders in the ecosystem, the implementation mechanism laid down within the framework will be the guiding principle to be followed. While all new HW & SW will have to necessarily conform to the new framework, the existing systems would also have to be migrated in a phased manner to support the new framework. This could be in a space of 1-3 years. Once the new framework is established, the same should be made a part of the license conditions.

Yes, the existing CAS and SMS systems should be mandated to conform to the new framework. A period of four months from the date of establishment of the framework may be provided for such compliance (i.e. Upgradation/installation of the CAS and SMS and thereafter synchronization of the same with the STBs on ground). This will ensure level playing field conditions and the achievement of common minimum framework.

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

BIF RESPONSE

Standardisation and Certification in CAS & SMS, which are the two key arms of Digital Addressable Systems, are crucial to improve efficiency, quality of service and thereby improve end consumer experience. The same has been elaborated in great detail in our responses to Qs. 1-5 as presented above.

Yes, standardization and certification of CAS and SMS will definitely bring economic efficiency as the losses of broadcasters and government would be reduced considerably. Since standardization and certification of CAS and SMS will prevent revenue leakage in the revenue chain, all stakeholders will get their due revenue, provided the CAS and SMS systems are made tamper-proof and the DPOs do not have the ability of modify these systems to their advantage. Hence, enforceability of all the features of CAS and SMS as listed in our response to Q1 is a necessary condition and penal provisions as suggested should be put in place to ensure compliance as suggested in our response to Q2 of the Consultation Paper. The quality of service will

improve as with installation of new/upgraded CAS the customers will be able to view channels of their choice, thereby improving end-consumer experience. With CAS and SMS systems complying with the parameters/specifications laid down in Schedule III, the consumer will not be tied down due to the limitations of the DPOs' systems. Further, it will enable complete implementation of the Telecommunication (Broadcasting and Cable) Services Standards of Quality of Service and Consumer Protection (Addressable Systems) Regulation, 2017 dated March 3, 2017 issued by TRAI.

Q9. Any other issue relevant to the present consultation.

BIF RESPONSE

None