IMCL Response to CAS SMS Consultation Paper.

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

We believe that the list provided in Schedule III is sufficient to cover all the requirements for digital addressable systems. No further requirements are necessary to this schedule.

TRAI should also consider that these CAS systems are already deployed in the network. If any additional requirements are added and existing CAS systems cannot support the same, then this may require replacement not only of the CAS system but all STBs already deployed on the ground and purchasing of new CAS licenses. The purchasing and rollout of STBs is a massive investment for any MSO and particularly under the current climate where collections are extremely difficult due to the lockdowns to protect the country from the Covid19 pandemic, and every DPO is losing customer base due to customers not being able to afford even basic television packages. DPOs will be forced to ultimately get customers to pay for the STBs again, which is not in the consumer interest either.

Further, due to the current economic conditions, many MSOs/DPOs are in the process of looking at opportunities to merge operations in order to reduce their costs. This means that existing CAS will also be taken over. The cost of replacing both CAS/STBs when DPOs merge would likely make the exercise unviable for businesses if further conditions are added.

The cost of CAS licenses also needs to be considered when replacing CAS systems. Each CAS license is interlinked to a unique STB. The cost of CAS licenses of some of these CAS are too costly to make it possible to deploy within the Indian scenario and this also needs to be taken into consideration. Typical CAS licenses go from USD0.6 to USD8.0 a license.

The aim of the consultation paper was also to look at how to limit piracy within a DAS/NTO regime. The premise that piracy is caused by the use of less-secure CAS is in our opinion incorrect. The CAS that have been most hacked to date are the advanced security CAS, and this has happened in India also. Wikipedia has a list of publicly available data with respect to CAS which have been hacked at the following link: https://en.wikipedia.org/wiki/Conditional_access. This indicates that those CAS vendors that are supposed to provide "advanced security", have nearly all been compromised in the past.

In most cases piracy in India occurs not so much through the hacking of an insecure CAS, but rather through other methods. This is because the cost of content is so low in India that it is not cost-effective to spend resources trying to hack an Indian STB. Instead, piracy typically occurs in the following ways:

1. Implementation of 2 CAS or SMS servers, only one of which is declared to the broadcasters or authorities

2. Implementation of analogue or unenecrypted digital networks
3. Utilisation of another DPOs signals to feed a network (piracy). This does not require piracy but simply paying Rs. 300-500 per month for an active and valid subscription to another DPO's network.

None of these are caused by the use of "less-secure CAS", but rather in the deliberate implementation of methods to get around correct reporting of numbers by DPOs and implementation of all DAS/NTO regulations. We believe that it is more important instead for TRAI and the authorities to better police the existing environments and stop DPOs that are intentionally bypassing regulations at the cost of those who are trying to work within the regulations. We recommend that appropriate piracy cells are put in place in order to ensure compliance and closure of networks that are not complying.

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

As reiterated above, we think that Schedule III is sufficient to determine the requirements of the CAS. The current CAS and SMS certificates required as per the Audit Manual do not require the CAS/SMS vendors to certify that they conform to all requirements of Schedule III. We believe that as a first step the CAS and SMS certificates should be updated accordingly. We do not believe any additional checks are required.

However, we also believe that TRAI should put in place processes for DPOs on handling situations, which will inevitably come in the future, in the event that any CAS is hacked. Currently Schedule III says that the version of CAS must not have been hacked. However, the reality is that in the event that the CAS is hacked, it can take many months 6-18 in order to (a) come up with a fix for the hack, and (b) deploy this into the network. Every major DPO across the world, including Dish TV in the US, Direct TV etc. have all been hacked in the past and it is important that TRAI provides a process for handling these situations. It is not practical in any scenario to simply replace the CAS and all linked STBs. DPOs should be given sufficient time to work with their CAS vendors to fix the hack and deploy necessary fixes into their networks. Currently no such provision is there in regulations or law to handle this scenario.

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?

We believe that each DPO should be able to select the CAS/SMS/STB that most suit their business model subject to them meeting specific functionality requirements as defined by the regulations. We do not think that the regulatory bodies should start to define preference towards certain vendors or solutions. This would make purchasing of these less competitive and could result in even higher pricing to DPOs and ultimately to customers. Each DPO has its own business processes, requirements and budgets. Selections of products will be based ultimately on all of these factors. Further, many SMS platforms are heavily customised to meet the business' requirements which has cost more than USD4 million. Migrating to a new SMS platform as selected by TRAI would result in heavy costs being incurred, customisations having to be re-built into any new platform and large migration exercises to move customers to the new platform. Equally our portals / mobile applications that are built to support LCOs, MSOs, subscribers and engineering staff would all need to be re-built in order to work with a new SMS platform. These would result ultimately in essentially re-building the business from scratch and would take away the business from other revenue-generating activities.

We believe that subject to the CAS / SMS / STB meeting the requirements specified in Schedule III, there is no need for any further assessment or benchmarking of products required in order for DPOs to deploy them within their networks. At most the regulator can "recommend" some preferred products, but there should not be any limit to DPOs being able to purchase or even build their own solutions subject to the requirements specified in Schedule III being met.

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?

Every DPO should look to purchase AMC from their CAS/SMS vendors in order to have support and access to software upgrades when required. This is part of the investment required in being an MSO. It is also far less expensive than having to replace an entire SMS system or a CAS and its linked STBs. Even upgrading the SMS/CAS will likely be much less expensive than replacing an existing system.

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.

TRAI should be entrusted the task of defining the framework for CAS/SMS in India with the help of both the broadcasters, DPOs, vendors and consumer forums. The intention is to ensure that a fair compromise is reached between all parties in relation to costs and effectiveness in meeting the industry's needs.

We strongly recommend that no private party or group should be formed to define the framework as corporate and other interests could be involved which would skew decisions to make it easier for any vendor or group of vendors or vested interests.

(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.

The existing consultation paper models should be used for setting up any structure / mechanism for defining criteria / guidelines / regulations for systems or processes to be used in the industry.

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.

The only designated agencies should be TRAI or BECIL to carry out testing and certification of systems against a set of clearly defined and documented requirements. Time should also be given to such platform providers to implement and new requirements that are required beyond what is already defined in Schedule III. Further, the testing and/or certification should take into accounts customisations made by DPOs on their platforms which may not be available to other DPOs and may enable the meeting of those defined requirements.

Any such testing cannot only be done on CAS and SMS. Testing will inevitably need to include all STB models also as the CAS security is ultimately governed by the security in each individual STB. The attempt to test all CAS and SMS platforms (including different versions and customisations) as well as each individual STB already deployed in India would be a massive exercise and in our view, potentially flawed and futile. No amount of testing will determine whether a CAS will in the future be hacked, even if they have been certified. It also puts an onus on DPOs to then select only from those vendors. Such an exercise could take 3+ years to complete in our opinion, during which time the products would have changed / upgraded and re-testing again would be required in order to re-certify. This would also put all current investments on hold as without a clear strategy, no DPO will look to invest in infrastructure or licenses if there is the risk that these would still need to be tested and approved by the regulator.

If TRAI wants to completely ban certain CAS or SMS, then these can be tested and appropriate timeframe of 3-5 years given to operators to migrate off these CAS systems and replace their linked STBs that they have already invested in. However, valid testing/certification and confirmation of that testing would need to be given to industry in order to provide opportunity for industry/DPOs/vendors to review and challenge any findings, if required.

(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?

We see huge industry challenges in standardisation of CAS and SMS in the Indian market. Firstly it will take significant amount of time to assess each CAS/SMS, and then too this should be done on an individual DPO basis as many products have been heavily customised in order to meet business requirements or processes of each individual DPO. Further, even if a set of preferred SMS/CAS platforms is finalised upon, these will need to be continuously monitored to ensure that they continue to meet requirements and it will create a potential oligopoly of products which could actually increase pricing to DPOs both for licenses, and customisations. Any such implementation will have to take at least 5 years to implement as this cost would be enormous for DPOs. Further the vast majority of DPOs impacted would likely be smaller DPOs who have invested less in products and the impact to them in terms of investment could potentially cripple or bankrupt these DPOs. These DPOs have the right to be supported by the TRAI, if they are meeting current Schedule III requirements without having to then implement a new set of products that would put them at risk of closing their businesses and/or being swallowed up by larger DPOs who can afford to make the necessary investments.

Further, the standardisation should then also include the STBs which are also important in the security aspects, if that is the ultimate aim of the Regulator. Most DPOs run platforms where there can be anywhere between 10-30 different STB models. If the intention is to look at CAS security, then without keeping in mind also the STB, the security will not be maintained throughout the chain.

We strongly recommend that the TRAI continue its current approach of defining the requirements that need to be met, which can be tested during annual audits by empanelled auditors. Any further activities to standardise and certify CAS / SMS / STBs would result in blocking of investments for the foreseeable future whilst these certifications take place and potentially lead to the bankrupting of many DPOs to the detriment of the entire industry.

(c) What should be the oversight mechanism to ensure continued compliance? Please provide your comments with reasoning sharing the national/ international best practices.

Compliance and oversight of Schedule III should continue to remain with TRAI and through a set of empanelled auditors including BECIL. This will ensure that no broadcaster, DPO, vendor or other interested party can control or veer the requirements to their interests and away from the overall industry's interests.

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?

We reiterate that we believe that no new framework is required to be established. The issues identified in the consultation paper are not related to any deficiencies of the SMS or CAS platforms, but rather caused by the non-oversight and monitoring of DPOs and how they use the same platforms.

Instead, TRAI should focus on setting a monitoring cell for DPOs where any issues related by consumers are effectively investigated by TRAI and in the case of piracy or unencrypted signals, the DPO in question are handled effectively as per law in order to stop and prevent these illegal activities which disrupt the industry and lead to huge impacts on those DPOs who attempt to follow the regulations faithfully.

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.

We do not believe that standardisation of CAS and SMS will bring economic efficiency and nor will it deliver quality of service. Each DPO will have their own business requirements and processes and as such there will never be a small set of SMS platforms that can meet all requirements. DPOs will then necessarily have to customise the solutions to their specific requirements and processes.

With respect to certification of CAS/SMS systems, this can indeed be done against the requirements of Schedule III which is anyway part of each annual audit. Auditors should at least indicate those SMS/CAS solutions which are not meeting Schedule III requirements and allow DPOs to work with the vendors to modify the software to meet requirements to avoid having to re-invest in new products, wherever possible.

However, TRAI will need to consider what will be the impact if certification includes other aspects including whether they are SoC, card or software based. Ultimately, any CAS system is susceptible to hacking and even advanced CASs are at risk of the same, if not a higher risk of the same as more premium content is secured by it and makes the effort worthwhile for hackers. Even a change from CSA 1 to CSA2 or CSA3 would require replacement of all STBs on the ground. These are not simple changes to implement and require a massive investment to an industry that is still trying to recover from investments made to meet digitisation and NTO requirements.

Q9. Any other issue relevant to the present consultation.

TRAI has documented that there are 3 main security related issues identified by broadcasters:

1. Transmission of unencrypted signals, unauthorised transmission of signals
2. Fingerprinting / watermarking not supported by the system
3. Cloning of STBs.

In the first instance, the transmission of unencrypted signals indicates not necessary the unavailability or incapability of a CAS system, but rather the fact that some DPOs are illegally transmitting intentionally in unencrypted form their video signals or even still transmitting analogue video signals. This has been raised to TRAI and other authorities to bring these DPOs to account, but so far not much seems to have been achieved. We strongly believe that much better policing and legal recourse being taken by the Regulator or Ministry to stop these analogue or unencrypted signals being transmitted by operators needs to be put in place to stop these illegal networks. It is not just broadcasters that are suffering, but also DPOs who are attempting to follow the regulations but are instead getting out-competed due to such illegal practices actually happening on the ground. There are networks that are selling all broadcaster channels for as low as Rs. 150 per month to subscribers when in reality this content is costing Rs. 400-500 and DPOs following the laws cannot drop their prices to these levels. TRAI should look into these illegal practices and illegal pricing schemes that are becoming more prevalent on the ground to ensure that there is effective competition for all.

With respect to fingerprinting and watermarking, TRAI has already issued its notifications to make all DPOs use watermarking from the encoders and that no encoders purchased after 2017 should be without watermarking. As old equipment comes up for renewal, the watermarking functionality will also be brought in as per this notification. Further, nearly every DPO who did not provide watermarking via its encoders, anyway provided the same through their STB so that broadcasters could at least determine where the signal was coming from. It is important for TRAI to investigate those cases where neither encoder-level watermarking and STB watermarking were both not taking places as these are the DPOs that are of most concern to broadcasters.

TRAI should inform affected DPOs when they learn of such cloning of STBs. This will ensure that DPOs work with their CAS vendors to stop the capability of cloning. TRAI should put in place a “piracy” cell in order to investigate these cases and help the industry and its DPOs close these gaps. Cloned STBs would be a huge impact to the DPOs themselves who would lose revenue and income and it is in the DPO’s interests to know and handle these cases when they are identified.

With respect to many of the other issues identified by TRAI including CAS/SMS integration, these issues exist even with advanced CAS and SMS platforms. There will always be situations where due to some issue, that the communication between CAS/SMS may not be working properly. Regular reconciliation activities should be implemented by each DPO to ensure that these are corrected on a regular basis.

In Appedix II of the consultation paper, the analysis done is inaccurate and doesn’t reflect that many of the issues identified in “sub-standard” CAS have also been identified in many of the “advanced” CAS platforms in the past. Any analysis of recent hacking of CAS will show that most hacking happens on these “advanced” CAS as they are typically used to protect expensive content abroad. Any CAS will be hacked at some point, and vendors are required to do the necessary R&D to develop new strategies and fixes to improve their security continuously. Previously card-based CAS platforms from even the most advanced CAS vendors have nearly all been hacked and now the move has happened towards SoC security. Even the CAS vendors themselves are changing their technologies. Non SoC based CAS can be of use, as in the event of a major hack, then a complete new software and keys can be pushed to the STBs, rather than SoC based CAS which would need to be replaced if the keys were compromised. The question, should be instead on how effectively can DPOs be informed if there is an active hack of their CAS system and how can they work with their CAS vendors to fix these in the shortest times possible.

We hereby enclose a table of key issues identified and other actions TRAI can take to fix these issues more effectively.

Issue Identified	Cause of Issue	Potential Actions To Be Taken
Transmission of unencrypted signals, unauthorised transmission of signals	This is neither a CAS or SMS related issue. Any CAS at the very least should be able to encrypt the channel, be it securely or otherwise. This is therefore simply the case of a DPO opting to not encrypt the signals and allowing their subscribers to view all content. This affects not only broadcasters but also competing DPOs that try to ensure that they follow the regulations.	This can only be fixed through appropriate policing by TRAI and/or other bodies who can then enforce the encryption requirements or shut down these operations.
Fingerprinting not supported by system	This is a core requirement of Schedule III and original 2012 DAS regulations. Any CAS system not support this regulation should not have passed any audit since 2012.	Such CAS systems that cannot meet requirements of Schedule III should be banned or rejected by TRAI
Watermark not supported by system	This is nothing to do with either the CAS or the SMS. This is related to the encoders used in the headend. However, most MSOs implemented the watermark feature in their STBs. Therefore customers still see a watermark on their content which enables broadcasters to determine the source of the signals.	TRAI has already notified that any encoder purchase from 2017 onwards must support watermarking to avoid DPOs having to spend large investment in replacing their entire headends to support this requirement. Any DPO that currently utilises no watermark at encoder or STB level should not be allowed to pass their audits.
Cloning of STB	This is an STB related issue and how the CAS security is implemented within the STB. Even STBs containing advanced CAS have been cloned and/or compromised.	Cloning of STBs has been done of both CAS based, SoC and software based CAS. Each of these architectures can be hacked. The question is how easy and cost-effective is it to update the STB in the event of hacking in order to block such hacking events. Card-based CAS require replacement of all smart cards in the network which is logistically nearly impossible and highly costly to the DPO. SoC based changes can be done up to a certain extent. Software based systems are actually the most flexible as it requires a software upgrade to modify encryption keys and change the way the CAS works.
Integration issues between CAS and SMS	This is a development exercise and not related to any specific SMS or CAS. Each SMS has to have its integration customised in order to work with a specific CAS and version of CAS. These activities are done by an SMS vendor specifically for each DPO as it also needs to implement the specific business rules that may be required by that DPO. It is the quality of this integration work that affects the full functioning of the SMS/CAS integration. That said, as with any software system, there is always the chances of systems having issues for any number of reasons, including software bugs, high load, hardware issues etc. that could cause the integration on occasion not to work properly.	Each DPO should be forced to complete proper reconciliation activities on a weekly basis to ensure that any discrepancies between SMS and CAS are cleared and corrected in the event of failed commands or any synchronisation issues.

Issue Identified	**Cause of Issue**	**Potential Actions To Be Taken**
Absence of creation/modification logs in system	These requirements are defined in Schedule III and any CAS/SMS deployed must meet these requirements. As such the CAS/SMS vendors must certify the same.	Ensure that CAS/SMS vendors certify the same. Any CAS/SMS vendor who cannot certify this should be put on a list of products that should not be used going forward.
Absence of blacklisting feature in SMS	The blacklisting feature can be customised into any SMS platform. It is up to the DPO to ensure that this process is developed into their SMS platform in order to meet this requirement in Schedule III	Ensure that this is tested as part of the Schedule III audit by 3rd party empanelled auditors
Support from CAS vendors	Once a CAS platform has been purchased, the DPO will inevitably become a "captive customer". It is up to the DPO to negotiate pricing for development/customisation as part of their contract negotiations. If the customisation relates to a Schedule III requirement, then this should be advised by CAS vendor at the time of purchase.	Every CAS or SMS vendor has to certify that they meet the Schedule III requirements as required by the current regulations.
Support from SMS vendors	Once an SMS platform has been purchased, the DPO will inevitably become a "captive customer". It is up to the DPO to negotiate pricing for development/customisation as part of their contract negotiations. If the customisation relates to a Schedule III requirement, then this should be advised by SMS vendor at the time of purchase. Even the NTO regulations required significant changes to the SMS platforms and development to support the requirements. Every DPO had to work with their SMS vendor to make the necessary changes required by the new regulations. This is an expected aspect of doing business.	Every CAS or SMS vendor has to certify that they meet the Schedule III requirements as required by the current regulations.
No protection against CW sharing	There are many CAS platforms, including those that are indicated in the Consultation Paper as "advanced security" systems that have been hacked and permitted CW sharing. A minimum set of requirements to avoid CW sharing can be defined but this should take into account that card-based, SoC and software based CAS are all genuine architectures and should all be supported.	Already Schedule III defines that the CAS cannot have been hacked. If the CAS has not been hacked then there can be no question of CW sharing taking place.
Weak encryption of ECM and EMM	As a minimum of ECMs and EMMs should be encrypted.	Potentially update Schedule III to ensure that ECMs and EMMs be encrypted
Unsecure boot loader	The boot loader is not a function of the CAS but a function of the STB and the responsibility of the STB manufacturer. The STB manufacturer must ensure that the boot loader is made secure and is signed by the CAS manufacturer.	TRAI should organise training sessions for DPOs technical teams so that they can discuss the same with their OEMs and ensure that they get the best out of their purchases
Poor support for detection of security breach	As a minimum DPOs must ensure that they meet Schedule III requirements. With respect to content being pirated and distributed online, this can happen to even the most secure CAS-protected STB. Online piracy has to be handled differently and separate regulations need to be put in place for the same. This includes monitoring of content that is online and help on identifying its source.	The cyber police and laws need to be strengthened in order to ensure that any piracy can be handled quickly and that cloud-vendors are forced to accept take-down orders on immediate basis when a content owner, DPO or other authority ask for content that is pirated to be removed. Process piracy take-down processes and regulations need to be created and implemented to ensure that any piracy can be handled efficiently by the legal and judicial systems.
Blacklisting of STBs	Blacklisting is simply a suspension or deactivation of STBs. This is typical functionality in any CAS. Even if they cannot suspend, a DPO can at least send disconnection commands to STBs. Even a blacklisting command will only work if the STB is on at the time the commands are sent.	This is already a requirement in Schedule III and should be tested during audit times of each DPO
Issues with CAS hardware	Many CAS servers, including those supplied by the "advanced CAS" are	No further actions required.

Issue Identified	Cause of Issue	Potential Actions To Be Taken
	off-the-shelf servers. This is not a question just for sub-standard CAS. The CAS vendor typically implements a separate card that is installed in these servers which handles the secure encryption. Further, it is to be proven whether a normal server is inherently less secure that one purchased by CAS vendor from the same hardware supplier. Today CAS vendors are offering solutions for DRM and CAS that are "cloud-based" which again rely on standard servers from cloud companies. This does not mean that they are inherently insecure. It is up to the CAS vendor to ensure security of their software and technology.	
Auto expiry and disentitlement of services	All CAS offer the capability to auto-expire services. It is up to the DPO to choose whether they want to provide auto-expiry or prefer to use the activation/deactivation methods for their business case. There are advantages/disadvantages to both options and it is up to the DPO to determine what works best for them. It is also very much in the interest of any DPO to ensure that their customers' STBs are getting deactivated on ground and regularly additional disconnection commands are sent to ensure that STBs are getting disentitled from their packages, otherwise no revenues will accrue to the DPO.	No further actions required.
Issues with addressability	Many CAS systems do offer this functionality, but it is up to the DPO to implement the same as this requires specific business cases to be drawn up and appropriate tagging of groups/regions etc. in the SMS and delivered to the CAS. This is not just a CAS requirement. Currently in Schedule III there are no specific requirements for the same.	TRAI to define what types of groups / regions it expects DPOs to implement in SMS and CAS.
Generation of CAS reports and databases in editable format	Every CAS utilises a database from any one of the main database technology providers. The lack of capability of backup should be assessed by TRAI, as it is unclear why basic IT backup cannot be done on products like MySQL, DB2, Oracle or other standard database technologies using 3rd party off-the-shelf backup softwares. Reports being available in editable formats is not an issue per-se as CAS teams may legitimately use this data for reconciliations or other data analysis. But rather a specific requirement can be added into Schedule III to ensure that those submitted to the broadcasters are generated from system in an un-editable format like PDF by the system itself.	Update Schedule III to also require CAS reports to be generated by system in non-editable format
Bmails / Alerts	There is no requirement either in DAS regulations or Schedule III to require the need for Bmails. Not all DPOs use this functionality for their customers. If TRAI believes this is an essential requirement, then Schedule III should be updated accordingly. OSD (on-screen display) messages are already included in Schedule III although there is lack of clarity around the need to send these as scroll messages. Previously TRAI had informed that DPOs could implement this functionality as and when new STBs are deployed as it was not possible to implement this on older STBs for which no support may be available from manufacturers. However, this has now been added to Schedule III. TRAI should clarify its stance on the same.	TRAI to clarify requirement of scroll messaging on STBs and ensure that only STBs manufactured post 2017 are required to have this functionality and that DPOs should not be penalised for older STBs not being able to support such functionality.
Impact on Customer of Sub-standard CAS/SMS	The impacts on the customer are not some much due to sub-standard CAS but rather due to sub-standard STBs. However, due to the heavy competition in the market, all DPOs have to look at ways of reducing their STB expenditure costs and try to reduce the costs to themselves and customers of the same. TRAI has not defined a minimum set of functionality that an STB must offer customers beyond what is in Schedule III and must therefore explain what this additional functionality is. Further, any additional functionality developed by DPOs will no longer be necessary available to Customers once a technically interoperable STB is in place as this will depend on the capabilities of the STB rather than the DPO going forward.	TRAI to define what its expectations are for minimum functionality required on STBs.
Impact on Broadcaster of sub-	Piracy issues impact all DPOs. As previously stated, most cases of	TRAI to explore training for DPOs

Issue Identified	Cause of Issue	Potential Actions To Be Taken
standard CAS/SMS	these on the ground are not related to substandard CAS/SMS but rather the deployments by the DPOs themselves through unencrypted signals, piracy of other DPOs signals etc. LCNs not being seamlessly implemented across a network are again not a function of either the CAS or SMS, but rather the PSI/SI server and STB software. This is mainly due to the deployment of cheap STBs by operators wishing to save money or not being able to work with their manufacturers to define (a) a set of clear technical and functional requirements for their STBs and (b) testing of the same before deployment. TRAI should instead look at training sessions for DPOs on the types of functionality and requirements that DPOs can build into their STBs with their manufacturers and why it is important to test these and how to maintain a set of test cases to be done before any deployments of new software to the same.	on STB software, requirements and testing
Impact on DPO of sub-standard CAS/SMS	There are very few CAS vendors that provide also SMS, middleware and UI functionality. Limiting the choices in India to just these manufacturers would create an oligopoly which would increase prices to DPOs and ultimately to consumers. Further, DPOs would be limited to the capabilities that these manufacturers would be able to deliver and their delivery organisations. Most of the issues faced today by MSOs are related to the STBs rolled out at the time of initial digitisation which were aimed at rolling out the STBs in the fastest time possible to avoid having customers poached by other competing DPOs. Little care was taken as to which STBs were purchased and the capability for these manufacturers to provide support going forward. Further many indiscriminate DPOs purchased STBs on credit and never fully paid off their STBs resulting in manufacturers going under or stopping support entirely. This behaviour caused issues throughout the industry. Now DPOs are forced to manage multiple varieties of STBs on the ground making changes slow to implement and difficult to manage. As these STBs slowly stop working they are typically getting replaced by higher quality STBs for which DPOs are spending more time working with manufacturers on software to meet their business requirements. It is in most DPOs interest to be able to shut down STBs in the network which would otherwise impede the capability for them to collect. To help DPOs, TRAI, either directly or via BECIL, should provide training and support on typical industry issues to help them make informed decisions on what product capabilities are, what to look for, what impacts these could have in the long term for the business etc. This would be more helpful in ensuring that smaller DPOs, that do not have strong technical teams, can learn how to implement a digital strategy more effectively. TRAI should also look to BECIL to provide consulting to these DPOs to help them in their implementations and support issues.	TRAI can look at implementing training courses or BECIL support for those DPOs that require help in making technology related decisions and do not have a strong technical team for the same.
Impact on government of sub-standard CAS/SMS	Correct reporting is definitely a requirement for government to ensure correct revenue collections from taxes etc. Schedule III already covers those requirements and it is up to TRAI to put in place appropriate measures to handle those DPOs whose infrastructure does not meet the Schedule III requirements. Further TRAI should have the powers to investigate those DPOs that are intentionally hiding reporting through, for example 2 SMS or 2 CAS servers, only one of which is reported to the broadcasters. This is not connected to whether these are sub-standard or advanced systems, but rather a DPOs choice to explicitly hide data from the auditors and authorities which is far more serious.	TRAI to investigate and bring cases in TDSAT against those DPOs that explicitly hide additional SMS or CAS servers for the express purposes of non-reporting numbers accurately.