Date : 22-04-2019

To,

Mr. Anil Kumar Bhardwaj, Advisor (B&CS)

Telecom Regulatory Authority of India,
Mahanagar Doorsanchar Bhawan,
Jawaharlal Nehru Marg, (Old Minto Road),
Near Dr. Zakir Husain College,
New Delhi-110002.

Subject: Response to the Consultation Paper on Audit Manual

Dear Sir,

Please find our response on the above mentioned subject, please find the enclosed document for the same.

Best Regards,

For IndusInd Media & Communication Ltd.

Subhashish Mazumdar
Senior Vice President
(Authorized Signatory)

Response to TRAI's Consultation Paper on Audit Manual for Digital Addressable Systems.

IndusInd Media & Communications Limited ("IMCL") is pleased to submit its comments to the Telecom Regulatory Authority of India ("TRAI")'s Consultation Paper on the Digital Addressable Systems Audit Manual.

As both an Multi-Service Operator ("MSO") and Headend-in-the-sky ("HITS") provider, IMCL agrees with the Authority that there should be an audit manual used by independent auditors to assess and review the digital addressability of all Digital Platform Operators ("DPOs") and not just that of the larger players. The audit manual should be created in order to ensure commonality of functionality and capability of digital addressable systems, irrespective of the platform used or the size of the DPO. This will ensure that all DPOs are assessed on par with each other without any favoritism based on size or location of DPOs.

The Authority's proposal to have independent auditors doing the assessment will also ensure that there is potentially less bias during audits from auditors who are paid for by broadcasters and therefore may not be impartial or fair when completing audits of a DPO's digital addressable system.

What needs to be clarified from the Authority, however, are the following:

1. Who will be privy to the final Audit Reports from the auditors and what processes will be followed to ensure security and confidentiality of its contents and details of each DPO's systems?

2. What is the level of non-compliance to the audit tests that will be permitted and who will make this judgement? The reality is that compliance may not be possible for 100% of DPOs for various reasons, and therefore some acceptable leeway must be given to each DPO. How can this non-compliance be managed to ensure and maintain a level-playing field for all DPOs?

3. In the event of any disagreement with respect to the audit findings by the DPOs, what recourse is available to DPOs who might be denied signals by broadcasters?

4. Will DPOs be provided with time to correct their systems and have them re-audited in order to ensure maximum compliance possible?

The aim of the Audit should be to ensure that DPOs are (a) reporting subscriber numbers correctly to broadcasters and (b) that sufficient security of content is being maintained to support the protection of broadcasters' content.

IMCL is happy to provide to the Authority the following responses to the questions specifically stated in the Consultation Paper and further provide additional comments/proposed changes with respect to the wording of the Audit Manual.

Responses to Specific Questions in the Consultation Paper:

Q1. Whether it should be mandatory for every DPO to notify the broadcasters (whose channels are being carried by the DPO) for every change in the addressable system, (CAS, SMS and other related systems)?

Due to various economic changes, including due to the new Tariff Order, we are seeing various changes to DPOs, from mergers in DTH companies, the splitting off of larger operators in order to become MSOs in their own right under a fairer NTO regulatory regime, shutting down of various headends of MSOs that could not sustain themselves etc. These changes are happening more regularly and are expected to continue for the foreseeable future as the industry matures and moves towards economic stability. We are also now 7 years in to digitization, with many STBs needing to be replaced and DPOs looking at potentials for migration to new CAS, STBs or even SMS systems to make them more sustainable going forward.

Informing broadcasters each time changes are made to an addressable system is neither practical nor required. This could result in DPOs being subject to additional audits outside of normal audit procedure by broadcasters which can be onerous and time-consuming.

In the event that notification is required, then the Authority must define exactly under what conditions such notification should be made:

1. When a new CAS/SMS platform is installed?
2. Whenever the DPO launches a new STB model?
3. Whenever the DPO sets up a new Headend/Mini-Headend? And what is the definition of a Mini-Headend in this context?
4. Whenever a software upgrade is done to either the CAS or SMS?

Notification of each time a DPO does a software upgrade to either their CAS or SMS does not seem viable, as these could be done for various reasons (new functionality that is custom developed, upgrade to latest version of software to support new functionality or requirements of new operating system/application servers/database technology etc.). These are done continuously under normal maintenance circumstances and it would be impractical to inform broadcasters of the same each time a new code version is rolled out to the CAS/SMS. Also, what level of code change in either system will warrant broadcasters being able to request a new audit of the platforms?

Notification each time a DPO launches a new STB does not seem viable and would add further delay in the capability of DPOs to launch new products to market, particularly if auditing is required prior to their launch. Further as many larger broadcasters also have their own DPOs (DTH, MSOs etc.), this would require DPO's product secrets to need to be divulged prior to launch to companies who are essentially also their competitors, which is unfair.

Notification to broadcasters launch a new Headend/Mini-Headend is also unnecessary as this can be captured in the next annual audit of the DPO. Under NTO regime where each and

every DPO can deploy their services to any DAS phase across the country and at a consistent MRP, DPOs are looking at how to now expand their businesses in areas where in the past they may have limited themselves due to differential pricing by broadcasters in pricing by location/DAS phase. Again, where many broadcasters are themselves aligned or owned by groups who also have DPOs, could use this company sensitive-information outside of the remit of any audit.

Q2. Whether the laptop is to be necessarily provided by the Auditee DPO or the Audit Agency may also provide the Laptop? Please provide reasons for your comments.
As DPO's data is very confidential both in terms of customers' information as well as from the perspective of the breadth of its network etc., it is important that the data is never taken outside of its offices and cannot be shared/used except specifically for the purposes of the audit. Many broadcasters belong to larger business groups that also have their own DPOs who could use this information for their competitive analysis which would be outside of the scope or purpose of any such Audit.
Therefore, it has been IMCL's consistent view that auditors should only use hardware that is provided by the DPO to ensure that data cannot be removed from the premises of the DPO. However, this should also apply to the audit reports and any analysis done on said raw data of the DPO, as even analysed data can be sensitive to the DPO's business and its competitive standing in the market, if inappropriately presented or leaked.

Q3. Whether the Configuration of Laptop vide Annexure 1 is suitable? If not, please provide alternate configuration with reasons thereof.
Under the new NTO regime, the volume of data that is being generated is significantly higher than at any other time previously. With subscribers being given full choice in order to select from broadcasters a-la-carte, bouquets or even DPO's bouquets, the total number of commands getting generated has grown exponentially leading to large volumes of data being generated compared to pre-NTO systems where on average subscribers were subscribed to only 1 product per month. IMCL itself has seen most commonly used tables in their databases generate more than 3-5 times the quantum of data than under pre-NTO, with just the main CAS transaction table in SMS now increasing by around 90GB every month.
In order to be able to extract out all the necessary data for 2 years from the SMS and CAS systems and put them in a laptop/desktop in order to do analysis, the specifications of the machine are insufficient for such analysis particularly in terms of storage requirements and processing power. For DPO's larger than 1 million, it is likely that a mini server will be required to support any audit requirements and analysis with at least quad- or octa-core processors. At least 2TB storage will also be required in order to store all the necessary data.
Further the data source format for all operators having subscribers greater than 1 Lakh, should also include .xls, .xlsx or .sql as these formats support formatted data which is not possible in just .csv formats or .txt formats proposed in the annexure.
Completing an audit of 2 years' data will result in a very lengthy audit, particularly under NTO regime where the volume of data has now increased exponentially. It is recommended that the audit be done for only 12 months' worth of data at any stage but done on an annual basis. Otherwise, it is likely that it will not be possible for auditors to complete audits of all 6000+ DPOs that are registered across the country within the space of 12 months. This will result in

larger DPOs being audited, and potentially many DPOs never getting audited and thereby putting an unfair onus on larger DPOs to comply against smaller DPOs that can get away with not being audited.

Q4. Do you agree with the provisions regarding seeking of TS recording and ground sample information from IBF/NBA for verification/checking by the Auditor?
The TS recordings should be obtained by the Auditors themselves by doing visits to some/all DPO's headends or even from the ground. It is unclear why these should be received from IBF/NBA and what the purpose of the same would be. Further as many broadcasters are aligned to DPOs, the fairness of such recordings may not be guaranteed. Therefore, it is recommended that the independent auditors make such TS recordings if required.

Q5. Do you agree that Data Dump may be cross-checked with weekly data of sample weeks basis? If yes, do you agree with checking of random 20% sample weeks? Please support your comments with justification and statistical information.
As per the Audit Manual, the Auditors will need to take 2 years' worth of data. IMCL believes this is impractical due to the much larger volume of data and transactions now under the new NTO regime. IMCL recommends that the audit should be done on a data volume of 12 months but done on an annual basis for all DPOs, without exception.
Due to the large data volume sizes, DPOs will be forced to move data off live systems and store them in offline storage or systems to ensure performance of the databases and servers. As table sizes get bigger, then archiving/partitioning strategies will need to be implemented at the database in order to ensure that the database can remain performant and avoid impacting user experiences. The Audit Manual and regulations should be modified to reflect the practical need to archive data off line or to secondary system on a regular basis for system maintenance and performance reasons, which should not be penalized for any DPO. IMCL's HITS platform SMS database is now growing at over 500GB (0.5TB) per month. In order to store 2 years' worth of data, the database storage will need to be increased significantly, but more importantly data will need to be shifted into archive tables to ensure that database performance is not impacted.
As per the Consultation Paper, the data will be extracted from the live SMS and CAS systems. Extraction of 2 years' worth of data from the live systems will take a long time and affect live performance, particularly under NTO regime where the quantum of data has increased exponentially. It is recommended that the auditors take out the data over a number of nights (when external systems can be put in maintenance mode) to avoid it creating too much impact on live systems. Also, as discussed above, the data may have been archived off onto secondary or offline systems to ensure system performance or when systems are no longer able to handle the quantum of data involved under NTO regime.
Another pertinent point to be considered is when multiple MSOs share a common SMS/CAS infrastructure and database. This is particularly true of MSOs who have multiple JV partners whom they are supporting and hold some stake in the JV partnerships. Whilst not fully compliant with the extant regulations in their current form in terms of owning their own individual SMS platform, the reality is that this is indeed what has been implemented on the ground as it enables sharing of investment and development for DPOs. The Authority must take cognizance of the same and draft these regulations and Audit Manual in a way that does

not discredit or penalize these DPOs. IMCL's recommendation is that the Authority accept the capability for one or more DPOs to share the same CAS and SMS platforms if this is declared by the DPO(s) and completes the Audits of these same DPOs at the same time to ensure sanctity of the data and the Audit procedures.

In point (4) of page 28 of the Consultation Paper, the Authority states that the DPO must certify that there is only one SMS that serves all CAS. This is not a requirement of the current DAS regulations of April 2012 nor is mandated in the updated regulations of March 2017. There should be no reason to limit a DPO to using only a single SMS, subject to the DPO declaring all the SMS platforms that they are utilizing and declaring the data for each. There may be various reasons for DPOs to be using multiple SMS platforms:

1. Merging of DPOs which could result in multiple SMS platforms. The cost of migrating all customers to a single SMS platform and modification of existing business processes may not make commercial sense
2. Cost of development of one SMS platform may be higher, so DPO prefers to maintain 2 platforms to ensure competitiveness of costs/expenses in the event of future development or integration with new CAS platforms.

Q6. Do you agree with the proposed Data extraction methodology? If not, suggest alternates with reasoning thereof.

IMCL proposes that the following data extraction methodology is followed:

1. Data can be extracted from live or offline SMS/CAS systems depending on where the data is stored. As discussed previously in IMCL's comments and feedback, it is not practical to maintain all the data necessarily in a live database which may not be designed to hold the quantum of data now being generated under NTO regime, not just from an infrastructure perspective but also from the performance of the database queries and tables. The Audit Manual should take cognizance of the same and accept that data may be extracted from archived tables and systems.

2. Auditors must also understand how the various SMS/CAS systems function, including the fact that whilst taking out historical records is possible, that the data they are looking for many need to be re-created from the same:
    a. In order to determine the total number of active/deactive subscribers in the CAS at any particular point in time is not readily available. The auditors will need to take a snapshot and then use the logs of activations/deactivations in order to derive retrospectively the status of active/deactive subscribers at some historical date.
    b. Similarly, for many SMS platforms auditors must be able to understand how the systems generate historical data.

Q7. Do you agree with verification and reporting of city-wise, state-wise and Headend wise subscription report? Please provide supporting reasons/information for your comment.

Under the new tariff order, there should no longer be any requirement for reporting at the city/state or Headend level. Even under the pre-NTO regime, reporting was typically done by city (in DAS phases 1 & 2) but for DAS phases 3 & 4 this was not practical, particularly for DPOs like IMCL which have a nationwide footprint. This would result in generation of potentially 1000s of reports each month which would be unnecessarily onerous on the DPO. The same would apply to DTH platforms who also have a very wide-spread distribution across the country, covering literally hundreds of cities.
It is strongly recommended that reporting should be done at the most of state or national level. Further, the need for such city/state/Headend-wise reporting should be understood, as this could also be used by broadcasters to determine their performance in specific locations/cities and therefore used for supporting their advertising research and revenues where detailed knowledge of locations of where they are able to distribute would significantly help broadcasters generate higher advertising dollars with their advertisers. This is not the purpose of the Audit and the data therefore should not be used for the same.

Q8. Do you agree with the tests and procedure provided for checking covert and overt fingerprinting? Provide your comments with reasons thereof.
The Authority will need to define what their understanding of a covert fingerprint is. In many cases this covert fingerprint is simply an overt fingerprint that is displayed only a for a single frame and therefore not visible to the human eye under normal operation.
As part of the fingerprint testing procedures, the Audit Manual suggests that fingerprints be generated for a continuous period of 5 minutes. Many CAS platforms do not support this length of fingerprint and only deliver fingerprints for 1 minute at any time. Including a feature that is not as per the original DAS regulations would create unnecessary burden on DPOs and most likely require development of new functionality from the CAS vendors to support this. The Authority must therefore accept that this functionality will take time and should not be used as a reason for failing the Audit by any DPO.

Q9. Any other suggestion/comments on the provisions of methodology proposed in the Audit Manual.
IMCL proposes the following comments/changes to the Audit Manual consultation paper.

1. Section 1.16 – In this section, the Authority states that “A Broadcaster may separately audit additional parameter(s), in case Interconnect Agreement between a DPO and a Broadcaster have additional stipulations that require checking/verification (e.g., stipulations pertaining to offering of discounts, territory, etc.), based on their mutual agreement.”

   There needs to be a common structure agreed as to how the broadcaster will conduct these additional audits and what level of auditing will be required for the same:
   a. Will the Broadcasters conduct a full audit similar to the one proposed by the Audit Manual? In this event, then what is the purpose of having an independent Audit done?
   b. Would it not be easier for the Audit Manual also cover off the additional audit requirements of Broadcasters to reduce onus on DPOs to support multiple audits

as much of these (assessment of penetration within specific territories and LCNs used) can be done as an extension of the existing audits with little or no additional data required to be collected by the auditors.

c. This does not prevent broadcaster wanting to audit DPOs for additional criteria that may not be within the new regulatory frameworks or regulations but included in their contracts unfairly and without the ability of DPOs to be able to challenge these without losing the capability of transmitting these channels. In many cases these additional criteria and conditions are included by the Broadcasters but not by "mutual agreement".

2. Section 2.1(c) – the definition of "addressable" system needs to be further clarified as this is regularly used by broadcasters to challenge DPOs that the SMS/CAS platforms must necessarily reside within the same physical location, which is not mandatory or required, particularly when a DPO has a distributed network and may therefore implement a distributed platform across its headends. The same applies to the HITS platform of IMCL, where broadcasters have in the past raised concerns regarding the SMS platform being located in a different location from the earth station, even after this has been audited and certified as being compliant by BECIL.

3. Section 2.1(aa) – whilst this Audit Manual is being proposed for all DPO platforms under digital addressable regulations, this is not in any way covering the requirements for OTT (Over The Top) platforms which are also transmitting the same content but under far less onerous conditions than those being imposed on DPOs. We would request the Authority to look into this inequality of conditions between platforms even though, ultimately, they are transmitting the same content to end-subscribers.

4. Section 3.1.1(a) – the "Pre-signal audit" should be implemented only for those new DPOs that have never received signals from broadcasters. This pre-signal audit should not be used by broadcasters for re-validating DPO's systems each time they launch a new channel in their networks or before renewal or revision of the existing agreement between the broadcaster and DPO.

5. Section 3.1.3 – This section requests that "DPOs must initiate their Audit as soon as possible". The Authority should provide a timeframe for the same, as well as define the impacts/procedure to be followed whilst each DPO awaits its turn for auditors to schedule and complete their audits, considering the number of DPOs that will need to be audited across the entire country.

6. Section 3.1.4 – as discussed previously in our comments to the Audit Manual, IMCL believes that it is not appropriate to inform broadcasters within 7 days "if any changes, modification and alterations are made to the configuration or version of the

addressable system (CAS, SMS and other related systems)". The statement is very broad and would require a DPO to inform a broadcaster even if a simple bug fix is applied to either the CAS or SMS platform, or when a STB software upgrade is done or a new STB is launched, or even when new products are added to the platform such as new broadcaster bouquets (configuration). This is simply too onerous on the DPO considering that software updates and changes are made regularly in order to meet changing business requirements and additional functionality that the DPO may want to launch. Requiring the same to be notified to all broadcasters continuously would be impractical and would put the DPO at risk of having the broadcaster use this to unnecessarily trigger audits of the DPO continuously. It is the belief of IMCL, that any changes in systems should be identified at the time of Audit if this is done on a regular annual basis.

7. Section 3.1.6(b) – The Audit Manual should also consider the impact of those SMS/CAS platforms that are shared between multiple entities (typically JV partners). In this case, a common Audit should be completed so that all data is extracted and the audit of each entity is completed at the same time.

8. Section 3.1.6(c) – Auditors will be extracting out confidential data (including customer information, location of customers, subscriber volumes, invoice and revenue information etc.) of the DPO, and DPOs must have a way for ensuring that this data is protected and not misused or distributed to any 3rd parties (including broadcasters etc.) outside of the remit of a final audit report.

9. Section 3.1.6(d) – Under what conditions can a broadcaster challenge an auditor's report or the DPO's undertaking "that the changes do not in any way compromise the system and the set-up and all the equipment including software meets the statutory compliance requirements". As per clause 10(7) of the Interconnect Regulations 2017, any change in configuration or the version of the addressable system of the distributor could cause a new audit to be requested by broadcasters. As discussed previously, the definition of a change needs to be clearly defined as even a small software bug-fix, upgrade, STB software change, new STB deployment, database upgrade, hardware upgrade, deployment of new Headend etc. can be defined as a "change in configuration". In the case of HITS, this could include the set up of a new Mini-Headend at a cable operator Headend, which requires configuration in CAS and SMS for the same. Multiple of these mini-headends are set up each week and notifying broadcasters of the same would be impractical. Therefore, it is imperative that the Authority define more precisely the types of changes that would warrant the need for notification and potential for a new audit more clearly and carefully.

10. Section 3.1.6 – DPO should be given up to 15 days in order to provide their comments on the draft audit report. However, it is not clear whether the auditors are required to take cognizance of the DPO's comments and what impact these would have.

11. Section 3.2 – in order to maintain 2 years' worth of data, DPOs may resort to keeping the data in archive tables or even in a separate database or file system in order to ensure maximum performance of their systems. Especially under NTO where the volume of data has grown exponentially each month, it is not practical to keep storing this data in live databases where not only infrastructure would need to be increased significantly, but more so that the applications may need to be re-architected to support handling such enormous tables that are getting generated for logs, transactions and bill events.
    DPOs storing their data offline or in archive tables should not be penalized for the same, so long as they can prove that the data is still complete and available to auditors for extraction.

12. Section 3.4 – Each Auditor organization must sign appropriate Non-Disclosure Agreements with the DPO at the time of audit to ensure that DPOs are covered for any intentional or unintentional leakage of their confidential data held within SMS or other IT systems in their organization. Further, the final Audit Report must also be subject to distribution only after appropriate NDAs are signed with broadcasters or other authorities to ensure that the report is not made public and is unavailable to anybody except those for whom the DPO has given express permission for its distribution.

13. Section 4.1(i) – according to this section, the audit should "check all the head-ends including the Headend for backup or mini headends (if any)". This is not practical in the case of HITS technology where IMCL has now more than 1500 deployed mini-headends across the country. This section should be clarified and made more specific in the case of HITS, that this should apply to the earth station and sample number of mini-headends (e.g. 3-4 mini-headends). Whilst IMCL is happy for Auditors to audit every single mini-headend, the timeframe and cost of doing the same would, in IMCL's opinion, not be effectively best use of Auditors' resources and time.

14. Section 4.1(vi) – this section refers to a network audit including a "self-declaration by the DPO of the Network Configuration and Territory/Areas covered by each headend". It is not clear what network audit will be required to be done by the Auditors, nor the nature of this self declaration with respect to the Network Configuration. Further, in the case of HITS and MSOs, the last-mile is not owned by the DPOs as such the network configuration for the same is not managed or necessarily known to the DPO. IMCL therefore requests that this statement be clarified and more detailed as to the nature of what is being requested here by the Auditors and the Authority.

15. Section 4.1(ix) – this section refers to the TS recordings provided by IBF/NBA. IMCL strongly recommends that the TS recordings be done by the Auditors directly at their discretion, rather than through IBF/NBA to ensure total impartiality and no chance of any bias, considering most of the larger broadcasters also have interests in various DPOs across the country and to avoid any potential semblance of favoritism or partiality.

16. Section 4.1(x) – this section refers to "seeking ground sample information from IBF/NBA". It is not clear here what ground sample information will be provided or offered by the IBF/NBA to the Auditors. It is not possible to comment on this section without better understanding what information the Authority expects IBF/NBA to provide to auditors with respect to this section.

17. Section 4.2(A)(b) – This section makes references to DPOs being required to provide "BIS certificates for all makes and models of STB deployed by the DPO (applicable for boxes purchased after 2012)". The TRAI must be very clear as to which BIS certificates it is requiring from DPOs:

    a. BIS 13252 (part 1): 2010 – this is the certificate for "Information Technology Equipment – safety – part 1: General Requirements" that is provided by each STB manufacturer and required at the time of import of STBs into the country. This is typically not renewed by manufacturers unless the DPO continues to purchase those same models of STB. Also, why do these BIS certificates of already deployed STB models need to be continuously be re-certified if the underlying specifications have not changed either of the standard or of the STB that is anyway already deployed in the network? It would be better simply to take the BIS certificate of the STB at time of import (in the case of foreign-manufactured STBs) or at time of delivery (in the case of natively-manufactured STBs) as confirmation that the STBs of that model are compliant with specifications.

       Further until a few years ago (post 2012), it was not mandatory to get the BIS certificate when purchasing this STB, and now it will be impossible to get manufacturers who may no longer have any business with the DPO to get these BIS certificates made retrospectively due to cost and manufacturers may also not be inclined to support DPOs for the same for older STBs that are no longer manufactured. Further there are a significant number of manufacturers that no longer exist or have gone out of business which would make it impossible to have this certification completed. In this eventuality, it is suggested that the DPO give a self-declaration that the STBs meet BIS specifications for these STBs.

b. BIS 15245:2002 – this is the standard for Digital Set Top Box Specifications (MPEG2)

c. BIS 16128:2013 – this is the standard for Set Top Box for MPEG4 Digital Cable TV Services Specification.

In the case of (b) and (c) above, the STB manufacturers have in the past approached the BIS testing companies in order to obtain certification of STBs under these specifications. However, in all cases, the BIS authorities have stated that they have not defined any tests for the same and therefore do not know how to test any STBs against these specifications. Please advise how DPOs are therefore to complete this necessary BIS certification against these specifications?

Further, are there any other BIS Certificates that are required to be provided to Auditors in order to meet audit requirements? Authority should make it very clear which BIS certification they are requesting for here to ensure that there is no doubt both for DPOs and Auditors.

18. Section 4.2(A) – "The Auditor shall request IBF/NBA for information referred to in clause 4.1.ix and 4.1.x ten (10) days prior to the commencement of the audit". IMCL's view is that auditors should collect their data independently of any broadcaster or broadcasting association to ensure that the collection is fair and impartial to every DPO.

19. Section 4.2(II) – the Audit Manual requests "area-wise" or city/state-wise STB or package data. It is not clear here why the data is required area-wise, nor what the definition of "area" is in this context. Even city/state-wise data is not possible in DTH/HITS environments where operators have data across literally hundreds of sparse locations which would generate large number of reports.

Under NTO where all contracts are now no longer related to a specific DAS phase, city or state, there should be no requirement for any area-wise data, unless this is very specifically for auditing penetration results as required by broadcasters. Under NTO, there is no requirement to provide area/city/state-wise reporting of packages/products and therefore if the aim of the Audit is to validate the accuracy of the reports, then there should be no need for these to be extracted out in this way by auditors. Further, this information is beneficial to broadcasters for commercial purposes and can have direct impact on their advertising revenues and should not be provided unless the DPO is willing to do so on a voluntary basis.

In the additional notes at the bottom of this section it further states that "Raw data or data dumps for at least 20% of the weeks (random sampling basis) during the audit period. The Broadcasters' report to be regenerated based on this data and compared with the actual reports submitted/sent to the broadcasters". In the case of certain SMS platforms, just re-extracting this data will not actually provide the data required for the broadcasters' reports. For this purpose, many DPOs take the snapshot of SMS data into a separate database on the report dates (e.g. 7/14/21/28th of each month under NTO and 01/31st of each month in pre-NTO regime). This ensures that the data being assessed is correct as on that date. It would be better for the auditors to sample these data extracts and make their assessments based on this data and determine whether the broadcasters' reports are correct as on that date.

An additional note at the bottom of this section that states that "During the first recorded audit all logs to be provided for preparing a first-time reference document". From the DPO's perspective, it must be clarified exactly which logs will be required here to ensure that appropriate archiving and database cleanup activities do not affect required logs. Each DPO will have archiving and performance cleanup strategies, particularly for databases to ensure maximum level of performance of tables and the application as a whole. In order to ensure that DPOs do not delete any data that might be required for auditors to complete their "reference document", it is necessary for the Authority or the Auditors to clearly define in this Audit Manual which logs will be required by the Auditors.
The Section 4.2(II) (10) - refers to extraction of inventory of all VC/UA/Mac-ID from SMS system for the past 2 years. It is not clear as to why this is required for audit

20. Section 4.2(II)(12) – this section refers to the extraction of information from the SMS systems of the DPO. What isn't clear is whether this data needs to be extracted and collected by the auditors independently or whether a report needs to be created in the SMS platform in order to extract this information for the auditors. Clarity is required on the same. Also, should this data be extracted as on date of extraction, or is the expectation that this data will be extracted for a specific historical date?

    It should be clarified whether the report requested at (b) is only for those products that are purchased on a-la-carte basis or whether this includes those channels that are also part of a broadcaster/DPO bouquet.

    Clarification is required with respect to report at (c) with respect to how ageing is to be calculated. In the event of packages/channels not being renewed for a contiguous period (e.g. package expires and is renewed only 1 day later), how does the ageing of

this product need to be shown in this report? Further should this report be generated automatically by the SMS platform in both PDF and XLS formats?

In the background note (3) at the bottom of the page, it states that the "report should be able to generate data for time period as per requirements (day-wise, week-wise, month-wise, year-wise). It is not clear what is required here exactly and how the ageing report will work on a time-period basis.

21. Section 4.2 (III) (a)- As per this section, DPO should declare all admin login access to CAS and SMS servers. The purpose of this statement is not clear as to whether the DPO is required to provide the admin access to CAS and SMS servers to the auditors. Providing all admin access to CAS and SMS servers to the third-party auditors is against the Information Security policy of any DPO / organisation

22. Section 4.2(III)(b) – Whilst the DPO may provide auditors with the facility to extract the data/logs/reports from the live SMS and CAS systems, this must be done at times agreed to by DPOs to avoid affecting live services and may need to be done in early hours of the morning. As also referred to by the Audit Manual, any data that has been backed up either on a separate reporting server, backup server or offline can be extracted and provided to Auditors where such data may be stored there.

23. Section 4.2(III)(c) – As per our previous comments, the Authority will need to provide direction as to how DPOs who are using shared infrastructure (including hardware and software/database) can have their audits done in tandem to ensure auditors can access full data and avoid having to repeat audits continuously separately for each DPO sharing infrastructure.

24. Section 4.3(A) Serial No. (1) of table –

(iii) As part of the technical audit the auditor must obtain the network diagram of the DPO. Clarity required on whether this is the internal network diagram of the DPO in their headend or should include the entire fibre network diagram of the network. In the case of MSOs/HITS, the entire fibre network is not owned by the MSO/HITS and as such, the entire complete network diagram will not be possible to provide. Further in HITS, the cable/fibre networks are owned by the linked cable operators and as such the HITS operator has no knowledge of these.

(iv) It is not clear which proxy servers would be in the headend of a DPO. What proxy server is being referred to here? Also, what IP credentials of all servers including MUX are being referred to here? It is not clear what is being requested.

(vi) In case of an audit mandated by broadcasters , DPO may not allow auditors recording screen shot of TS streams from the MUX since the TS streams from MUX will include channels of different broadcasters

(x) Confirmation that insertion of watermarking network logo for all channels is from the encoder. In reality, many DPOs (particularly MSOs) have implemented the network logo on the STB. Whilst this is not in line with the DAS regulations, the Authority should take cognizance of this and determine whether there really is a problem with this and what the implications are for these DPOs in terms of being found non-compliant during these audits. Ultimately, the broadcaster and platform fingerprints can be used to identify the feed that is being used in those channels and whether piracy (if any) is occurring. The need for watermarking logo is not particularly required in terms of reducing piracy or ensuring security of the video signals for broadcasters.

25. Section 4.3(A) Serial No. (2) of table – In part (b) of this section, it states that “Auditors are not to accept any pre-extracted data/reports from SMS & CAS system”. However, this should be qualified to ensure that any data that has been backed up to offline or other systems, or extracted for broadcaster reports in the past and to provide snapshots of status at specific points in time are not to be considered in this exclusion.

    In part (a) where the DPO needs to “declare all admin/super admin login access”, this needs to be clarified to limit this request to the user IDs and the reason for those access. No passwords will be provided to these accounts for security reasons by the DPO.
    In part (d) where it is referring to the “the fact that no STB/VSC is left out from the database”, it is worth noting here our previous comments with respect to the process that will need to be employed when doing audit of those platforms where SMS/CAS platforms may be shared between multiple different DPOs.
    In part (e) the Audit Manual refers to the need for “auditor should issue a communication as per annexure 6 (minimum 7 days before the activity) to News Broadcasters’ Association and Indian Broadcasting Foundation for nominating an observer for oversight during the data extraction process. It is to be clarified by the Authority why an IBF/NBA representative should be present at a normal audit of a DPO, when clause 10(7) of the Interconnection Regulations of 2017 only state that these audits will be done either by BECIL or “any other auditor empaneled by the Authority for conducting such audit”. There is no mention in this regulation that any

broadcaster should be present during any or all part of this audit exercise. It is not clear what value-addition having a broadcaster present will have on the audit exercise.

26. Section 4.3(A) Serial No. (4) of table – this states that auditor must check that logs for last 2 years should be in SMS. It needs to be clarified here, that data may be archived offline or on a secondary/backup server where logs are too big to be able to store on production environments or would cause performance issues to the application/database server. This is particularly going to be important going forward under the NTO regime where the volume of data has increased exponentially and will impact the performance of existing SMS systems that have been implemented.

    In part (b) there is also a requirement for "DPO to certify on its letterhead that there is only one SMS that serves all CAS". This is not a defined requirement in the DAS regulations of April 2012 nor in the Interconnect Regulations of 2017. As such many DPOs may have implemented more than one SMS platform for various operational or economic reasons, including partitioning of certain STBs, when merging or taking over other networks (e.g. Videocon/DishTV merger) or simply to ensure that DPO is not beholden to a single vendor which can then increase development pricing etc. It is unclear why this requirement has since been added as part of the audit manual requirements as this is not a limitation set in any current regulation in place.
    Further, in the event that the DPO has multiple SMS platforms, then migration to a single SMS may not be economically feasible for the MSO and may take significantly more than 90 days depending on the development work required to support business process, integration work required to integrate potentially other CAS platforms or migration work to move customers to new SMS platform and training work required to re-train linked cable operators/subscribers to use different portals/applications which will need to be re-built or have different flows based on system capability.

27. Section 4.3(A) Serial No. (6) of table – This section discusses the fact that the CAS does not have the facility activate/deactivate the STB directly from the CAS terminal. This is an unfeasible request and requirement of the new Interconnect Regulations. Each CAS will have the facility for administrators to activate/deactivate the STBs directly from the CAS terminal. This facility is used for testing the CAS system communication with STBs and checking whether there are any issues. Also, this is used for testing STB commands when doing CAS upgrades or changes. This facility cannot be disabled and is a requirement of the system. Whilst this can be limited to specific user IDs at the CAS level, it is unclear how the facility is to be disabled completely.

    In part (c) it states that "auditor to check that the CAS does not have any access to DPO staff who are involved in business related operation regarding activation and deactivation of STBs". It is unclear how this can be proved to the auditor by any DPO. Clarity required on how this will be verified to the Auditor.

It is suggested that the DPO provides a declaration that a process will be followed to ensure that th facility available to administrators will be restricted to minimum number of personnel and used only to activate/deactivate STBs for the purpose of testing.

28. Section 4.3(A) Serial No. (8) of table – this section states that "The distributor of television channels shall validate that the CAS has the capability of upgrading STBs over-the-air (OTA), so that the connected STBs can be upgraded". It is to be noted that the CAS is not the only system that can be used for sending down OTA software to the STBs, and this functionality can be delivered by a PSI/SI server also. In the DAS regulations of April 2012 there was no limitation to the OTA being delivered by PSI/SI server. It is not clear why this now has to be delivered by the CAS server when this is simply a data carousel for sending out software upgrades on specific PIDs. This section should be generalized to allow distributors of television channels to send OTA using any method directly from the headend, which can include, CAS, PSI/SI or other data carousel tool.

29. Section 4.3(A) Serial No. (9) of table – most CAS platforms cannot send out fingerprint for more than 1 minute. The requirement to send out fingerprint for 5 minutes duration may not be possible on many CAS platforms. This needs to be validated by the Authority to check whether the majority of CAS platforms in use across the country under the DAS regulations can support this functionality. In the case of IMCL, it is clearly stated that its CAS platforms cannot support this functionality, and these CAS platforms are known to be use in many other DPOs across the country.

30. Section 4.3(A) Serial No. (11) of table – it should be clearly stated that this section applies only to those STBs that are card-based and that it should not be seen as a limitation of a card-less based STB.

31. Section 4.3(A) Serial No. (13) of table – in part (e) it states that customer reports should be "city, district and state wise". Under NTO regime, where all DPOs are able to deliver content across the nation, it is to be clarified why this data is required under these filters both by broadcasters and auditors.

32. Section 4.3(A) Serial No. (14) of table – requirement to generate reports both city, district and state wise under NTO regime should not be a requirement and this requirement is not defined in Schedule III of the Interconnect Regulations of 2017. There is no clarity for the rationale for requiring the reports to be generated for any specific region or area. Unless this is being used for penetration reporting for broadcaster incentives which can be tested by auditors, there does not seem to be any rationale for requiring this functionality from the SMS platform.

33. Section 4.3(A) Serial No. (15) of table – in part (a) it states that "auditor should generate all reports city, district and state wise as per Schedule III A (13) from the CAS. The CAS does not hold any "personal" data against each STB/vUA including where the STB is located. So how will it be possible to generate these reports city, district or state wise. The CAS is used to provide data only on whether an STB is active for specific packages/channels or deactive. Further Schedule III A (13) does not define the requirement to be able to provide the logs on a city, district and state-wise fashion and more importantly this clause in schedule III is specific to the SMS and not the CAS. This test should therefore be removed as it is irrelevant to the audit.

    In part (b) of this section it also states that the CAS should ensure that report also includes DPO name, address and unique ID and date/timestamp of the report. It is to be noted that the CAS server does not generate "reports" but rather the auditor must extract out its logs and use it to collect the data required for auditing. As there is no reporting engine in the CAS, it will not be possible generate any report with DPO name and time/date stamp. This requirement should be removed as it is not possible to achieve by a CAS system.

    In part (e) it states that "Annexure 2 should mention that CAS logs are available for up to preceding two consecutive years for each command executed in the CAS". It should be clarified that this data may be archived on other tables or offline in order to ensure that CAS system can run in a performant fashion.
    Section 4.3(A) Serial No. (16) ,part(e) it is not clear what is meant by the statement that the auditors must carry out reconciliation of VC and STB for each channel obtained from logs Transactional logs as well as configuration logs) of complete CAS and SMS Logs with the Broadcasting report of each month of the audit period. Broadcaster reports is generated for Broadcaster bouquets and a-la-carte channels and the logs will also be created for activation and deactivation of Broadcaster bouquets and a-la-carte channels. Clarification is required about this reconciliation

    Section 4.3(A)Serial No. (16), part (g) A 3 way reconciliation on channel wise count of Broadcasting report, CAS and SMS should be done at count level for the day of Audit and on sample basis. Broadcaster report is generated for a month based on average of subscriptions of broadcaster bouquet and a-la-carte and it may be a arduous task to carry out such a reconciliation for one day that too at a channel level. This needs to be clarified

    Section 4.4 (A) Serial no. (16),part (p) This is not a relevant verification. Payment can be received for outstanding from the customers whose STB/VCs are not active as part of the collection recovery process

34. Section 4.3(A) Serial No. (16) of table – in part (i) the auditors must do a reconciliation of the LCN and genre used by DPOs. This is required only for incentives purposes and are not defined under any specific regulations in the Interconnect Regulations.

    In part (k) it is unclear why IBF/NBA would need to provide STB/VC field samples and what the purpose of this analysis is. The audit should be done independently and impartially to ensure that this is completely transparent to everyone in the value chain.

    In part (k) it is unclear why there is any requirement for TS recordings to be provided by IBF/NBA and why this cannot be done instead independently and impartially by the auditors themselves.

    In part (q) it states that "auditors to report if TS was configured in such a way that local insertion of channel was not possible in an un-encrypted mode during Audit Period". It is unclear how the TS needs to be configured in order to ensure no un-encrypted local channel insertion is possible. Clarity is required from the Authority on how the TS needs to be configured in order to ensure that this un-encrypted insertion cannot be done.

35. Section 4.3(A) Serial No. (18) of table – as discussed previously, it is possible that some log information will be stored in backup database or offline CAS server in order to ensure performant functioning of the CAS servers, particularly under new NTO regime where the volume of data is exponentially higher than previously and database tables must be kept at optimal size in order to ensure performance of application.

36. Section 4.3(A) Serial No. (19) of table – bills are usually created for postpaid customers. In the case of IMCL's MSO and HITS platforms, nearly all direct subscribers and the LCOs billing and their subscribers are in prepaid. Therefore, we are generating a statement-cum-receipt indicating for what products they are being charged and the validity period for the same. This audit requirement should be re-phrased to cater for prepaid scenarios where a bill/invoice is not generated like in postpaid.

37. Section 4.3(A) Serial No. (22) of table – in part (b) of this section, it states that the "auditor to list down broadcasters' inventory details for DPO's each distribution network headend" and in part (c) it states "auditor to visit DPO's digital sub-headends having multiple headend(s) and undertake headend validation as per audit manual. The following is not clear from these sections:

a. What broadcaster inventory details will need to be given to the auditors? What exactly is being requested to be done here?
b. In the case of a HITS platform where there are thousands of mini-headends across the country, visits to each digital sub-headend is not practical. It should be clarified that in the case of HITS, that the earth station will be audited and may be 3-4 sample digital sub-headends of operators.

38. Section 4.3(A) Serial No. (23) of table – As per the Interconnect Regulations 14(1) of 2017 and defined more specifically in Schedule VII of the Regulations, the broadcaster reports to be submitted to the broadcasters in a format that does not require to be given city/district/state wise, nor does it include the monthly fee. It is unclear, therefore, why the audit manual would request that auditor check "subscription report details with city/district/state and monthly fee" when this is not required by the regulations.

39. Section 4.3(B) Serial No. (2) of table – in part (b) of this section it states that "For covert type: Auditor should ensure this capability is mentioned in the STB certificate (annexure 8)". It was not possible to find Annexure 8 in the Audit Manual and which STB certificate is being referred to in this section?

40. Section 4.3(B) Serial No. (3) of table – as mentioned previously, most CAS platforms cannot support displaying a fingerprint for more than 1 minute at a time. This test therefore will need to be modified accordingly.

41. Section 4.3(B) Serial No. (5) of table – as mentioned previously, most CAS platforms cannot support displaying a fingerprint for more than 1 minute at a time. This test therefore will need to be modified accordingly.

42. Section 4.3(B) Serial No. (10) of table – the requirement for scroll-based OSD messaging was only included in the QoS regulations of March 2017 and as such older STBs purchased prior to this date will not have this facility. The audit assessment section should be re-phrased to ensure that DPOs who have STBs older than 2017 are not penalized for not having this functionality available.

43. Section 4.3(C) Serial No. (1) of table – in part (2) it states that "in case of middleware capability, auditor should also ascertain if the middleware in each model STB has interactive services capability. It is not clear how this assessment or verification relates to the actual requirement of "All STBs should have a conditional access system" and what will be the purposed of obtaining this information by the auditors.

44. Section 4.3(C) Serial No. (5), (6) and (8) of table – the requirement for scroll-based OSD messaging was only included in the QoS regulations of March 2017 and as such older STBs purchased prior to this date will not have this facility. The audit assessment

section should be re-phrased to ensure that DPOs who have STBs older than 2017 are not penalized for not having this functionality available.

45. Section 4.3(C) Serial No. (9) of table – in part (a) it states that "auditor should take copies of BIS certificates from the DPO for each make & model of STB procured after the BIS standards came into effect". It needs to be clarified by the Authority, what the dates for the same are, and when the same BIS standards tests were actually made available for each required BIS certification by the testing authorities of BIS. As mentioned previously, when our STB manufacturers have previously approached BIS testing centres for testing against all BIS certifications, except for IS 13252 (part 1):2010, they have not been able to test STBs as no tests were in place for certification against the standards. Further, the Authority should be clear as to which exact BIS certifications each DPO must be compliant.

    On part (c), it further states that "As of the audit date, the certificates should be valid". In the case of IS13252 (part 1): 2010, this is done at time of import of STBs. It is unclear why this certification should be renewed each year by OEMs when DPOs may no longer be purchasing these STBs again and once certified, this should be sufficient unless the underlying standards have been modified in any way. In this event, the standard would anyway be updated and new certificates issued. This requirement of renewing the certificates each year is therefore unnecessary and creates additional cost and work for DPOs without any obvious advantage either to DPOs or broadcasters.

    Please advise where on BIS website, the auditors will be able to validate and crosscheck the certificates for each DPO's STBs as per part (d) of this section.

46. Annexure 1 – in the "data source location (local/server) row of the table it states "RDP". Please advise what the definition of "RDP" is in this context as this is not clear. Further under data source formats for all columns, it should include the following:
    a. .txt
    b. .csv
    c. .xls or .xlsx
    d. .sql

    This will ensure that even data extracted directly as a database structure or excel formats can be provided to auditors for any size of DPO, depending on the requirements.

47. Annexure 2 – IMCL has the following comments:

a. It states that "Database Detail" is required. What exactly is being requested here? Does the CAS vendor have to provide details of the database software and version used? Why is this information required as part of this declaration?

b. In part (1) it states that "CAS certificate to be in two parts – DPO and CAS vendor", however Annexure 2 only refers to the CAS vendor declaration. What declaration is required from the DPOs?

c. Whilst CAS vendors have to declare whether the version used has been hacked or not, the Authority should look at the regulations and how eventualities of hacking will be dealt with going forward. In the event of hacking, it can take many months for CAS vendors to be able to deploy a fix to overcome the hacking exploited. Will DPOs be penalized by the auditors and broadcasters during these times with the risk of essentially shutting down their businesses? A separate discussion and procedure needs to be put in place to handle such eventualities.

d. In part (9), it states that the CAS must maintain logs for the period of 2 years. As discussed previously, the Authority must be open to DPOs moving their logs and data to offline or backup systems due to the large volume of data now being generated under NTO which will result in highly ineffective applications, irrespective of the underlying hardware deployed if large tables and files are not truncated, archived or architected correctly.

e. In part (10) it states that "the CAS has the capability of upgrading STBs over-the-air (OTA), so that the connected STBs can be upgraded". As discussed previously, the CAS is not the only device in a headend that can be used for distributing OTA software to STBs. PSI/SI servers are also capable of achieving this functionality and many DPOs use the PSI/SI server for this purpose. This requirement in the CAS declaration should therefore be removed as it is at the discretion of the DPO whether they wish to use CAS or PSI/SI data carousel functionality for delivering OTA software to STBs.

48. Annexure 3 –

a. In the declaration, DPOs must indicate "SMS database detail with number of instances". It is not clear what database detail is required to be submitted here and clarification is therefore requested.

b. In part (7) it states that "SMS shall be independently capable of generating, recording and maintaining logs for the period of at least immediate preceding two consecutive years". As discussed previously, it should be clarified that this data may be stored in backup, offline or additional separate database

tables/servers to ensure that systems run efficiently, and more so due to the exponential increase in data and log volumes being generated under the new NTO regime in large numbers of tables of the SMS systems.

49. Annexure 4 Table A –
    a. Under the section titled “CAS Make”, for cardless STBs the table requests data on “video scrambling”. It is not clear what information is required to be provided here. All cardless CAS support video scrambling, so what data needs to be added here?

    b. Under the section titled “STB Make”, the column called “Embedded CAS Name” should be renamed “CAS Name” as the CAS name, irrespective of whether it is embedded CAS or card-based CAS should be added in this column.

    c. Under section 9 and 10 it states “Is CAS able to provide reports at any desired time about…”. It is to be clarified that the CAS servers do not provide reports, but instead logs can be generated from the system. Even Schedule III of the Interconnect Regulations refers to CAS logs and not CAS reports in A(14) where it states that “The CAS shall independently capable of generating, recording and maintaining logs …”.

50. Annexure 4 Table B –
    a. In section 9, it states that “Is overt finger printing displayed by the MSO without any alteration with regard to …”. This statement should be re-phrased to clarify that this relates to the “broadcasters’ overt fingerprint”.

51. Annexure 4 Table D –
    a. In section 1, it states that “valid” BIS certificates need to be available. It needs to be clarified whether BIS certificates need to be renewed each year even if the standards have not changed at any time or whether STBs should be certified only at the time of purchase of the STBs, subject to standards not undergoing change. And even if the standards do undergo changes, then the certifications under new standards should be applicable only to new STBs deployed going forward.

52. Annexure 7 –
    a. Table of contents:
        i. 6.6 – as IMCL is nearly 99% prepaid, then this should be rephrased as “itemized bill/statement-cum-receipt” depending on whether postpaid or prepaid customers are being supported.
        ii. 6.16/6.17/6.18 –monthly log”. The use of the word “report” should be limited to SMS as in the CAS only logs are available and not reports.

b. Main Audit Report
    i. This report is focused only on MSOs and there is no equivalent provided for HITS, IPTV and DTH DPOs. Throughout the Audit Report, it refers to "digital cable" and is not generic for all DPOs types.
c. Digital Addressable System Infrastructure
    i. Part (f) – this refers only to carded CAS, but many DPOs have deployed cardless CAS
    ii. Part (g) refers to "Control Word (CW) information". It should be clarified that the control word in most DPO architectures is not generated by the CAS, but is actually generated by the MUX or an external scrambler. Therefore, this section should be re-phrased accordingly.
d. Content Reception at End User Point
    i. Part (a) refers to "At present only FTA channels are being turned around at the headend" – this section needs to be modified to reflect the fact that free/pay channels may be offered by any headend. This seems to be a different audit report that has been used here that is not necessarily applicable most DPOs.
e. Compliance Checks - CAS and SMS
    i. Part (a) (ii) and (iii) – these should be removed as these two may not be delivered by the CAS system in a digital addressable system as they can be delivered by multiplexors or external scramblers and there is no requirement in either DAS 2012 regulations or latest Interconnect Regulations that state that these must be provided by the CAS.
    ii. Part (b) – it should be made clear that the CAS system does not have to be sized for 1 million subscribers but the system should be capable of being expanded to support 1 million subscribers in the event that this required. This would otherwise require smaller DPOs to invest in infrastructure that would be unnecessary for their subscriber base.
    iii. Part (c) - it should be made clear that the SMS system does not have to be sized for 1 million subscribers but the system should be capable of being expanded to support 1 million subscribers in the event that this required. This would otherwise require smaller DPOs to invest in infrastructure that would be unnecessary for their subscriber base.
    iv. Part (e) – this section is not relevant to most DPOs. Authority should considering re-phrasing the same.
    v. Part (f) – this is applicable only for postpaid customers, as prepaid customers are given statement-cum-receipts towards payment of their services.
    vi. Table 1 section 9 – it is not clear why the "SMS and CAS should be able to handle at least one million concurrent subscribers on the system". This is not as per Schedule III requirements, and even in the DAS regulations of 2012, the word "concurrent" was not included in Schedule I. The word

"concurrent" should be removed as it would unnecessarily impose on all DPOs that need to be able to handle 1 million subscribers each accessing the system "concurrently" or at the same time which would force DPOs to size their systems for an unnecessarily large base that no DPO supports. Even larger DPOs with subscriber bases of 10million+ subscribers would only size their systems to support up to 10% of their subscriber base using the system "concurrently" i.e. at the same exact time.

f. STB
    i. Part (c) states that the "STB OEMs have submitted the BIS compliance certificates as per mandate of TRAI regulations". Again please see previous comments with respect to the BIS certifications already discussed above.

g. Following TRAI listed STB Requirements were checked
    i. Part (10) refers to "There should be a system in place to secure content between decryption & decompression within the STB". Please advise how the auditors will test and validate this requirement.

h. Audit Conclusion
    i. In the event that DPOs are not able to meet 100% of requirements as specified in the audit for historical (e.g. old STBs still deployed in network, multiple CAS/SMS due to merger of operators etc.), technological or other reasons, it needs to be clarified what will be done and how they can continue to operate. What is the leeway being provided to DPOs who cannot comply with every single requirement, particularly if it doesn't impact either broadcaster reporting or security of content for broadcasters?

53. Annexure 8

a. In this annexure DPO must certify "that CAS does not use facility to activate and deactivate a STB directly from CAS terminal". All CAS platforms have this facility to deactivate and activate STBs directly from CAS terminal as this is used for testing purposes both of the CAS and STBs under development and during any CAS/SMS outages for troubleshooting.

   This statement should be removed from the declaration. Alternatively, it is suggested that this be re-phrased as "We also certify that we, DPO, do not use the CAS facility to activate and deactivate STBs directly from CAS terminal except and exclusively for purposes of testing and trouble-shooting."

****

Corporate Office: IN Centre, 49/50 MIDC, 12th Road, Andheri (E), Mumbai-400 093
Tel: (+9122)28208585. Fax: 28248366/28248363