CLOSING NOTE ISSUED BY

MEDIA DEVELOPMENT AUTHORITY OF SINGAPORE

CONTENT PROTECTION SECURITY REQUIREMENTS

in support of the

CROSS-CARRIAGE MEASURE IN THE PAY TV MARKET

ISSUED ON: 1 July 2011

1. Introduction

1.1. On 12 March 2010, the Media Development Authority ("**MDA**") introduced the cross-carriage measure ("**Measure**") to address MDA's concerns over the nature of competition developing in the Singapore pay TV market and, in particular, the high degree of content fragmentation which had resulted in increased inconvenience and attendant costs for consumers and created significant barriers to entry for new entrants. The Measure imposes an obligation on Supplying Qualified Licensees ("**SQLs**") (as defined in the Code of Practice for Market Conduct in the Provision of Media Services, also known as Media Market Conduct Code 2010 ("**MMCC 2010**")) to widen the distribution of their channels or programming content which are Qualified Content[1] ("**QC**"), by offering such content for access by SQLs' subscribers over the Relevant Platforms[2] of Receiving Qualified Licensees ("**RQLs**").

---

[1] "Qualified Content" means:

(i) any channel or programming content (whether in a linear or non-linear format), including any basic function in support of such channel or programming content that is specified in Part I of Appendix 1, where such channel or programming content is:

(A) subject to sub-paragraph (ii), produced or commissioned by a Regulated Person and where, on or after 1st August 2011, the Regulated Person transmits the same on its Subscription Television Service in Singapore and refuses to allow the channel or programming content to be acquired or otherwise obtained from it for transmission on any Relevant Platform in Singapore by:

(I) any other Regulated Person; or

(II) where the Regulated Person that produced or commissioned the channel or programming content belongs to a Group, any other Regulated Person outside the Group; or

(B) acquired or otherwise obtained on or after the Effective Date by a Regulated Person for transmission on its Subscription Television Service in Singapore under an arrangement, whether explicit or implicit, which prevents or restricts or is likely to prevent or restrict the channel or programming content from being acquired or otherwise obtained from it for transmission on any Relevant Platform in Singapore by:

(I) any other Regulated Person; or

(II) where the Regulated Person that acquired or otherwise obtained the channel or programming content belongs to a Group, any other Regulated Person outside the Group; and

(ii) any bundled channels or bundled programming content comprising, in whole or in part, any channel or programming content that is referred to in sub-paragraph (i) of this definition.

For the avoidance of doubt, any channel or programming content is not Qualified Content by virtue only of the incorporation of any value added service that is specified in Part II of Appendix 1 in the channel or programming content.

For the purposes of sub-paragraph (i)(B) of this definition, for the avoidance of doubt, whilst any channel or programming content that is acquired or otherwise obtained is not Qualified Content if it was acquired or otherwise obtained under or pursuant to an arrangement referred to in that sub-

1.2. Paragraph 2.7.2A(d) of the MMCC 2010 requires that the RQL has a content protection system for each of its Relevant Platforms which would reasonably prevent the security of all QC made available to it by any SQL from being compromised. Part III of Appendix 1 in the MMCC 2010 further sets out the content protection security principles which the RQL must ensure its content protection system for each of its Relevant Platform adheres to.

1.3. On 29 April 2011, MDA launched a consultation on content protection security requirements in support of the Measure ("**Consultation**"). The Consultation closed on 26 May 2011. MDA received submissions from 6 respondents, including pay TV retailers, content protection security providers, a content provider and an industry association, representing a diverse range of views.

1.4. This document sets out MDA's views on the feedback received and the implications for the guidelines on content protection security requirements ("**Guidelines**") which may be adopted by RQLs so as to facilitate compliance with their obligations in the MMCC 2010.

1.5. Throughout the Guidelines, MDA has adopted the key principles that the content protection system should be cost efficient, effective for the intended purpose and easy to implement, while balancing the valid concerns from various stakeholders.

1.6. MDA expresses its appreciation to all parties who have contributed to the consultation process.

1.7. The comments received and MDA's responses are described in Section 2, while Section 3 sets out the effective date of Guidelines on the Content Protection Security Requirements.

---

paragraph before the Effective Date, it is Qualified Content if and from the time such arrangement is extended, renewed, or otherwise re-contracted for on or after the Effective Date.

[2] "Relevant Platform" means a managed network over or using any one or any combination of the following:
(i) hybrid fibre-coaxial;
(ii) optical fibre;
(iii) Asymmetric Digital Subscriber Line.

2. MDA's Responses to Comments Received

2.1 At the close of the Consultation, MDA received submissions from 6 respondents, namely:

- ESPN Star Sports ("**ESS**");
- Motion Picture Association-International ("**MPA**");
- Nagravision Asia Pte Ltd ("**Nagra**");
- NDS Asia Pacific Ltd ("**NDS**");
- SingNet Pte Ltd ("**SingNet**"); and
- StarHub Cable Vision Limited ("**SCV**").

2.2 MDA would like to thank all the respondents for their useful feedback and comments.

2.3 The responses fall into 5 broad categories:

- Network operator headend security requirements;
- Content protection delivery system security requirements;
- Set-top box ("**STB**") content protection security requirements;
- Implementation and review of Guidelines; and
- General comments.

2.4 The comments received and MDA's responses within each category are described in detail below.

NETWORK OPERATOR HEADEND SECURITY REQUIREMENTS

Facility security and monitoring

2.5 One respondent commented that there is no need for a power backup system to support CCTV systems for at least 30 minutes. The respondent viewed that, as a minimum, the card access and the fence intrusion systems should be supported with a backup system.

2.6 The same respondent believed that CCTV recordings should only need to be retained for 7 days (so long as access logs are kept for 90 days).

MDA's response

2.7 **MDA considers that the requirement for retailers to provide CCTV backup power is not an unreasonable requirement for pay TV retailers to implement. MDA views that if retailers can provide power backup for their card access and fence**

intrusion systems, then they should be able to do the same for their CCTV system.

2.8 **MDA also disagrees that 7 days is an appropriate minimum length of time to keep CCTV recordings. However, taking into account the respondent's feedback, MDA will reduce this requirement from 90 days to 30 days, provided that the key-card access logs are kept for at least 90 days.**

System security

2.9 A respondent felt that it should be sufficient to install anti-virus software only in systems that interact directly with customers.

MDA's response

2.10 **MDA maintains that it is necessary to ensure all systems which store or process the digital QC are secured and it is not sufficient to only cover systems that interact directly with customers. Thus, MDA views that it is reasonable to require anti-virus software to be implemented on systems that are vulnerable to outside infection.**

Fingerprinting and watermarking

2.11 One respondent considered that where required by a content provider ("**CP**"), the RQL should be obliged to implement fingerprinting and respond to any requests of the CP to shut down illegal streams.

2.12 Another respondent commented that the requirement that "SQL's application of an RQL-specific watermark should be at the option of the SQL" must be removed. The respondent went on to state that CPs will have to send customized watermarked media to both the RQL and SQL, and CPs should be reimbursed for this cost by the RQL/SQL. The respondent also viewed that RQLs must demonstrate to CPs that they have rights to specific QC before receiving it. The respondent felt that this would imply the need for a contract between the CP and RQL covering these and related requirements.

2.13 A third respondent stated that the RQL should not undertake any activity that interferes with watermarking, and should undertake any activity required to preserve watermarking.

2.14 A different respondent took the view that it is sufficient for an RQL to support a pass-through of the SQL's watermark, and not necessary for the RQL to apply watermarking itself.

2.15 Another respondent suggested amendments to Section 3.5.7 of the Consultation paper to clarify the distinction between the forensic watermarking activities that RQL should not undertake and the activities that RQL should not neglect to undertake.

MDA's response

2.16 **MDA believes it should be the responsibility of the CP and/or the SQL (and not the RQL) to use fingerprinting and/or watermarking technology to track sources of piracy as the RQL is a mere conduit for the cross-carriage of QC.**

2.17 **MDA considers that the application of RQL-specific watermarked content ought to be commercially negotiated and enforced through the respective contractual agreements between (i) the SQL and the CP; and (ii) the RQL and SQL. MDA also sees no justification in eliminating the option of the CP contractually requiring each SQL to apply an RQL-specific watermark to content that an SQL supplies directly to an RQL.**

2.18 **As such, an RQL should not incur any additional costs arising from a CP-led desire for RQL-specific watermarking through the SQL.**

2.19 **MDA agrees with the suggested amendments on forensic watermarking and has accordingly amended Section 3.5.7 of the Guidelines to clarify the policy intent.**

Early Window HD content

2.20 One respondent, whilst supporting the exclusion of advanced interactive and 3D content from the scope of the Measure, believed that Early-Window (pre DVD) HD content or Premium Home Theatre ("PHT") offering should also be exempted. The respondent suggested that this issue could be revisited when the PHT business model matures and is widely deployed in Singapore or comparative markets in the Asia/Pacific region.

MDA's response

2.21 **MDA would like to highlight that this is not the right platform to address the exemption of new media services from the Measure. MDA supports the introduction of new media services and observes that Early-Window HD VOD content[3] or PHT offering is a very new business model not currently offered in Singapore. MDA notes that this content, where available, may have additional content protection security requirements such as transactional forensic**

[3] Early Window HD VOD refers to the new and experimental business model where studios and CPs release movies online 60 days (or earlier) after the theatrical launch. In US, as an additional protection measure, studios and CPs can also turn off unprotected outputs of set-top boxes and DVD/Blu-ray players.

watermarking and selectable output controls. Given that this new business model is just beginning to evolve, it seems pertinent that this issue be revisited at a later date, in line with the respondent's suggestion. An SQL who is bringing new innovative media services such as Early-Window HD VOD content may apply for exemption from MDA under the MMCC 2010 if the RQL is unable to offer appropriate content protection security for such services. Section 3.5.8 of the Guidelines has been amended accordingly.

CONTENT PROTECTION DELIVERY SYSTEM SECURITY REQUIREMENTS

Scope of the Measure

2.22 One respondent agreed with the current list of relevant platforms, but felt that the Measure must also distinguish between operators using STBs and those that deliver content using only software based DRMs. The respondent suggested that operators using only software based DRMs, even if over a Relevant Platform, should be excluded from the Measure.

MDA's response

2.23 **MDA clarifies that Section 4.2 of the Guidelines clearly sets out that where an RQL uses software-based DRMs on a general purpose user-programmable computing device such as a PC for the cross-carriage of QC, the RQL is required to ensure that the DRM software is secured with a hardware root of trust. This should adequately address the respondent's concerns.**

CPDS content encryption algorithm

2.24 One respondent stated that the most common encryption environment used in the DVB standards is the Common Scrambling Algorithm and therefore the use of DVB-CSA, CSA(2) and CSA(3) should be included in the Guidelines.

2.25 A second respondent also felt that specific reference to the DVB Common Scrambling Algorithm should be included. The respondent went on to state that different encryption algorithms should be permitted if the RQL demonstrates that the chosen algorithm achieves similar or better security and that decrypted QC ("**DQC**") should be encrypted across the interface, and in storage, with an encryption algorithm of at least 128-bit AES or 112-bit 3DES. The respondent concluded by stating that when passing encrypted QC, the QC should be encrypted according to the native scrambling algorithm of the Content Protection Delivery System ("**CPDS**"), including the DVB Common Scrambling Algorithm. The

respondent proposed a number of wording changes to Sections 4.4, 5.5.16 and 5.5.24 of the Guidelines.

MDA's response

2.26 **The Guidelines aim to highlight the key principles for the content protection security system. Operators can adopt the various content protection standards available in the market today. MDA agrees that Section 4.4 of the Guidelines could include the DVB CSA Version 3 as an additional option, since it uses a 128-bit key and was developed as an enhancement to earlier versions of the DVB CSA that used smaller keys (the original DVB CSA Version 1 used 64-bit keys and Version 2 was restricted to using 40-bit keys). Systems using these older DVB CSA specifications are more susceptible to brute force attacks and thus would not meet the requirements. MDA has revised the Guidelines accordingly.**

CPDS revocation and renewability

2.27 A respondent stated that Content Protection Solution Providers should provide to a neutral authority all the boot-loader keys, and descrambler keys for STBs, CI and CI+ devices, and conditional access modules ("**CAMs**").

MDA's response

2.28 **MDA notes the suggestion to provide to a neutral authority all the boot-loader keys, and descrambler keys for STBs, CI and CI+ devices, and CAMs. RQLs are free to adopt such practices if they have commercial and legitimate reasons to do so.**

Simulcrypt

2.29 A respondent commented that Simulcrypt is one of the key features of the DVB Standards and should be strongly recommended. The respondent pointed out that additionally the Common Interface and the Common Scrambling Algorithm ensures no party is locked into a single provider of Content Protection.

MDA's response

2.30 **MDA agrees it is important that no party be locked into a single provider for its CPDS in order to meet the Guidelines. Simulcrypt is a CAS implementation that allows multiple CAS to exist on the same STB and may meet the applicable standard under the Guidelines. However, given the need for the CPDS to support either or both CAS systems as well as DRMs, MDA will not prescribe the**

use of Simulcrypt with the DVB Common Interface and DVB Common Scrambling Algorithm (which are both CAS related technologies.

STB CONTENT PROTECTION SECURITY REQUIREMENTS

High definition analogue outputs

2.31 One respondent suggested that the rules about circumstances under which DQC can be output over High Definition Analogue Outputs should be changed to: DQC should not be output over analogue if the DQC is marked with a Digital Only Token ("**DOT**"). In addition, if the DOT is asserted, DQC can only be output on protected digital outputs which do not further output HD or SD analogue outputs. If DOT is not asserted, DQC should be output over 1080i60/720p60/1080i50/720p50 analogue in an image-constrained format unless the SQL has CP's approval to output the DQC in HD over analogue outputs.

MDA's response

2.32 **MDA believes it is in the best interest of consumers who may own legacy HDTVs with only analogue HD video inputs to have access to such analogue HD signals. Therefore, MDA disagrees with the respondent's proposed sunset of analogue HD video outputs and the suggestion of adding a new "Digital Only Token" Usage Rights signalling that would trigger off all (standard definition and high definition) analogue video outputs on a program-by-program basis. MDA believes that the current video output compliance rules best balance the interests of CPs and consumers.**

2.33 **MDA is of the opinion that the respondent's proposal to put restrictions on HD analogue video outputs could be reconsidered in the future when the technology is more prevalent and widely adopted.**

2.34 Another respondent felt that the clause "...Over 1080i50 or 720p50 analogue component video outputs, if such HD Qualified Content is first processed into a constrained image" in Section 5.5.8 of the proposed Guidelines should be deleted as it contradicts paragraph 2.7.2A of the MMCC 2010.

MDA's response

2.35 **MDA believes that the video output compliance rule, as stated, is not inconsistent with the MMCC 2010. Paragraph 2.7.2A of the MMCC 2010 requires an RQL not to reduce the quality of an image carried to the subscriber's STB, but it does not constrain an image output from the STB. MDA also notes**

this constraining of the image in the RQL's STBs is only necessary when the SQL has also been required to do so by the CP.

2.36 **The RQL still carries QC "in its entirety and in an unmodified and unedited form", but since there is no clearly defined industry standard for copy control signaling in 720p50 or 1080i50 analogue component video signals, the QC image resolution should be constrained or downscaled before outputting over such analogue component video outputs. In any case, the RQL can still output 720p50 or 1080i50 over analogue component video outputs if they obtain permission from the SQL to do so.**

2.37 **MDA highlights to respondents that the image constraint is required due to the 50 Hz versions of these HD analogue video signals not having a defined standard for carrying copy control information embedded in the analogue video signal, unlike the 720p60 and 1080i60 video signal formats, as defined in the CEA-805-D standard.**

Digital outputs

2.38 A respondent commented that the RQL's STBs should be able to output/pass DQC to any output protected by DVB-CPCM, if configured in accordance with the CP rules and securely communicated via the SQL to RQL to the STB (i.e. through CPDS security).

MDA's response

2.39 **MDA disagrees with the comment to include DVB-CPCM as one of the listed technologies to protect STB outputs under the Guidelines, as there is no current compliance/ licensing regime yet established for implementing the DVB-CPCM technical specifications. MDA may review the above issue in the next periodic 3-year review or whenever there is sufficient evidence of market development or major technological changes that warrants an interim review.**

2.40 A second respondent believed that the RQL requirement to adopt v2.0 of HDCP is not economically justifiable. The respondent went on to state that a common and widely-adopted standard should be adopted instead of the proprietary Motorola IPRM system.

MDA's response

2.41 **The use of HDCP 1.X is already adopted under the Guidelines (see Section 5.4.9 of the Guidelines). For clarity, MDA has revised the term "HDCP" to "HDCP 1.X". MDA has not amended Section 5.4.9, bullet point 3, to reference HDCP 1.X since it refers to "HDCP 2.0", which is a more advanced version of the older HDCP 1.X**

that can be used on a wider range of digital interfaces (not just DVI and HDMI), such as wireless interfaces.

Copy Control Watermark Non-Interference

2.42 One respondent stated that an RQL must obtain permission from a CP before incorporating legitimate features including recompression, image overlays, video mixing, etc.

MDA's response

2.43 **MDA clarifies that the intent of Section 5.4.12 is to allow an RQL to incorporate these legitimate video processing features, as long as its STBs do not strip, obscure or interfere with the Consensus Watermark in DQC. In consideration of the respondent's concerns and for clarity, MDA has clarified in Section 5.4.12 of the Guidelines to limit the processing to the RQL's STBs. This means that an RQL would not be allowed to modify the programming at the head-end prior to transmission. The language of this section is then essentially identical to the same section in the CableLabs tru2way Agreement and should address the concerns of the respondent.**

Audio Watermarks

2.44 A respondent commented that licensed devices should include a Cinavia™ Audio Watermark detector and screening process for the presence of the "No Home Use" and "Trusted Source" Audio Watermarks in all content that is decoded and played back on the licensed device. The respondent stated that if a watermark is detected, the device should prevent playback.

MDA's response

2.45 **MDA considers the use of Cinavia™ Audio Watermarks a relatively new market development that has not yet been fully deployed in its first application as part of the Advance Access Content System ("AACS") copy protection for the Blu-ray Disc format. Given the fact that the Cinavia™ copy control watermarking addresses camcorder piracy and optic disc ripping and not QC piracy, MDA considers that such watermark detection obligations should not be included in the Guidelines at this stage. MDA may review this issue in the next 3-yearly review or whenever there is sufficient evidence of market development or major technological changes that warrants an interim review.**

Mere buffer for display

2.46 Section 5.5.14 stated that "RQL's STB receivers may store DQC temporarily for the sole purpose of enabling the immediate display of DQC, provided that (a) such storage does not persist after the DQC has been displayed, and (b) the data is not stored in a way that supports copying, recording, or storage of such data for other purposes."

2.47 One respondent commented that it should not be mandated that the RQL is required to store DQC, rather that the relevant parties should resolve this requirement on a bilateral basis. A second respondent commented that this section was not applicable.

MDA's response

2.48 **To signal the intent of the Guidelines clearly, MDA has added clarifications in Sections 5.4.13 to 5.4.25 of the Guidelines to describe the basic set of four Copy Control Usage Rights states. MDA would also like to clarify that the RQL should deliver QC to its subscribers with the same Copy Control Usage Rights, subject to the agreement between the SQL and the RQL.**

Copy Never

2.49 A respondent made the point that Section 5.5.16 should be deleted because only CGMS-A or Macrovision implement Copy Never, while all other variances are meant for DVD usage. The respondent went on to state that for personal video recorder ("**PVR**"), controlling of copying is done via applications rather than through CPDS signalling.

MDA's response

2.50 **With regard to the above comment, the CPDS conveys the Copy Control Usage Right of Copy Never and can also be used, along with application(s), to provide PVR pause recording of Copy Never marked QC. MDA believes that the original requirements set out in the Guidelines should be maintained.**

Approval mechanism

2.51 A second respondent commented that the approval mechanism and indicative timetable for amendments to approved technologies should be stated.

MDA's response

2.52 **The Guidelines are not intended to provide a comprehensive list of allowable standards. Any specific standards and protection technologies mentioned are used purely as illustrative examples and are not exhaustive. A formal approval mechanism for new technologies is therefore not necessary.**

Methods of making functions robust

2.53 In reference to Section 5.6.9, one respondent stated that it is considered insufficient to only require protections that "cannot be reasonably foreseen to be defeated or circumvented merely by using general purpose tools or equipment that is widely available…", given the sophistication of tools owned by most current hackers.

2.54 A second respondent noted that it is essential to maintain research and development specifically targeted to maintaining the technological advantage over "Pirates".

MDA's response

2.55 **MDA believes that the current robustness requirements are adequate and have already been accepted by major studios in the CableLabs tru2way License Agreement. MDA highlights that Robustness Rules need to balance the interests of CPs with those of the system operators who would have to incur higher implementation costs with more restrictive robustness requirements.**

2.56 A third respondent commented that the life-span of STBs averages 5 years, and so the proposed 18-month timeline requirement would generate unnecessary capex, given the difficulty in forecasting new technology when ordering/commissioning STBs. The respondent went on to state that these increased cost would be passed on to end-consumers and raise customer dissatisfaction.

MDA's response

2.57 **MDA sees no need to change the robustness requirements since any significant security compromise to an RQL's STB receivers should be addressed in a timely fashion.**

Usage Rights Information

2.58 A respondent commented that the Guidelines must support Usage Rights Information ("**URI**") for QC and enable the CPs to select such URI, e.g. through CAS; and support transfer to and adherence by the STB of the authorized usage rules. The respondent stated that the URI should be applicable to QC, with the ability to:

- Control propagation (view, move, copy) of QC across subscriber devices;
- Limit re-distribution of content;
- Selectively enable outputs for QC including specific protected digital interfaces; and
- Require devices to reduce QC resolution when passed through analogue outputs.

2.59 The respondent considered that DVB CPCM USI specification provides information that should be used to enhance the Measure over time.

2.60 The same respondent commented that URI associated with individual QC should be transferred from the SQL to the RQL and that RQLs should be required to process and distribute QC in accordance with URIs received. The respondent opined that the MMCC 2010 should specify a minimum URI but allow flexibility in how information about the rights is communicated to the RQL from the SQL or CP.

MDA's response

2.61 **MDA agrees that the Guidelines should specify a minimum set of URI but should allow flexibility in how information about the rights are communicated to the RQL from the SQL or CP.**

2.62 **However, MDA believes that the respondent's suggestions for usage rights signalling are too broad and may not be supported by existing CPDSs that are deployed worldwide. For example, most CPDSs do not support domain-based copy control or Selectable Output Control, which are two usage rights suggested by the respondent. MDA therefore views that a minimum set of Copy Control URI be specified that encompass the basic set of four copy control usage states, which are:**

- **"Copy Never" – which is QC that may not be copied or redistributed over the Internet but may be temporarily recorded to facilitate pause functionality;**
- **"Copy One Generation" – which is QC of which a secure, first generation copy may be made;**
- **"Copy Control Not Asserted, No Internet Redistribution" – which is QC where no numeric restrictions are placed on making protected copies of, but where such copies may not be redistributed over the Internet; and**

- **"Copy Control and Redistribution Control Not Asserted" – which is QC having no restrictions on making copies or redistribution.**

2.63 **The RQL's CPDS should support a means to securely convey and/or manage the Copy Control URI for QC that the SQL has negotiated with the CP.**

2.64 **Text to this effect has been added to the Guidelines.**

Other Comments

2.65 A respondent voiced the opinion that the CableLabs technical specification is an appropriate base for the STB content protection security requirements in the Guidelines, but that a licensing body is required to be effective.

2.66 Another respondent suggested that Section 5 of the Guidelines may be expanded from STBs to any enabled devices perhaps using a DVB Common Interface (CI and CI+). The respondent further suggested that the section should not refer to any specific standards and that limiting standards to CableLabs may inhibit parties from achieving the same results in different environments and in a non-proprietary manner. Finally, the respondent stated the belief that reference to a US based environment may not be relevant to the Singapore market.

MDA's response

2.67 **MDA wishes to clarify that in coming up with the Guidelines, we had referenced and adapted the guidelines from technical specifications (e.g. DVB, ETSI, IEC), video formats and resolutions (e.g. 576i, 720p50, 1080i50) used in other jurisdictions, including Europe, Australia and other ASEAN countries. It is therefore not accurate to assume that the Guidelines are solely US based. More fundamentally, MDA is neither setting any specific standards nor adopting CableLabs standards, but rather providing these as examples. Therefore, the Guidelines are not intended to inhibit the use of any content security solution providers.**

2.68 The same respondent argued that the MMCC 2010 must limit access to infringing content from STBs that are used to consume QC. The respondent stated that for any STB, or other QC-access device, that allows users to install applications:

- The RQL must certify applications (including existing or new versions) to ensure they do not provide access to infringing content or pose a security threat, before the applications are made available to end users;
- Licensed devices must ensure that they can execute only certified applications;

- MDA must enable enforcement action to be taken against devices or applications that compromise device security or provide access to infringing content; and
- The RQL must have a program to disable applications and devices that are not suitable.

2.69 The respondent also proposed that the Guidelines should include provisions that any licensed devices that allow access to the open Internet:

- Shall ensure no access to sites on a URL Blacklist. The URL Blacklist, and secure access to it, should be maintained by the MDA or CPs; and
- Shall check for URL Blacklist updates on every boot, or on first IP connectivity.

MDA's response

2.70 **MDA is fully committed to promote legitimate access to copyrighted material but note that this consultation is not the appropriate platform to address the concerns raised by the respondent. Therefore, MDA will not explicitly include the proposed changes to the Guidelines which are intended to focus on the delivery of QC between the SQL and RQL. Content owners may like to pursue a commercial arrangement with the content acquirer to address such issues.**

IMPLEMENTATION AND REVIEW OF GUIDELINES

Compliance process

2.71 One respondent opined that the certification of each RQL/SQL network is the responsibility of the RQL in conjunction with their security service provider. The respondent went on to suggest that an independent certification may lead to issues of shared or dissolving responsibility to rectify issues, and that the SQL must be able to ensure that their security meets the CP requirements, and ensure (receive certification) that the RQL also conforms to these rights.

2.72 A second respondent considered that self-certification may be appropriate, but that joint certification is preferable. The respondent's view was that CPs should be allowed to be involved in the certification to the extent they wish to be, quoting a decision by Ofcom in the UK allowing CPs to set requirements for QC, rather than the regulator.

2.73 A third respondent took the view that RQLs should be allowed to self-certify compliance.

2.74 A fourth respondent agreed with MDA that the MPAA guidelines are a good starting point for RQL security, but highlighted that they are only guidelines. The respondent suggested that individual CPs may have different requirements to the MPAA guidelines and that where required by a CP (or SQL), RQLs should:

- Perform security audits before QC is made available; and
- Implement additional security measures or technologies to receive specific QC, i.e. different technology to receive QC from different CPs, or ISO/IEC 27001 (Information Security Management System) compliance.

2.75 A respondent proposed that MDA should set up a certification association to support independent certification.

MDA's response

2.76 **MDA views that the certification process should be cost efficient, effective for the intended purpose and easy to implement.**

2.77 **In consideration of the diverse views and to provide more options for the industry, MDA will support certification of compliance with the content protection security principles, through self, joint or independent certification.**

2.78 **In a self-certification process, MDA will require an RQL to obtain a testimony from a provider of content protection solutions used to support delivery of premium content by Pay TV operators in mature markets such as US and UK, and/ or prove that their content protection systems have been accepted by premium content providers for the Singapore market.**

2.79 **As for the suggestion to set up a certification association, MDA considers that given the size of the Singapore market, setting up such an association would not be cost efficient. MDA also notes that both self and joint certifications are credible as both the SQL and RQL will have experts who are well versed in the various security requirements of system operators that include the headend operation, the CPDS, and STB receivers.**

Evolution of Guidelines

2.80 A respondent considered that the 3-year review cycle for the Guidelines should be reduced in time, and possibly changed so that it happens on request of any involved party.

2.81 A second respondent pointed out that it is expected that the security requirements from CPs will continue to change and it will be difficult to maintain specific regulations consistent with the requirements of each individual CP.

2.82 Whilst a third respondent stated that a review cycle of 3 years is too long, and an annual review is more appropriate. The respondent suggested that developments in piracy and anti-piracy measures should not be discussed in public, with a provision made for detailed parts of the Guidelines to be protected by Non Disclosure Agreement at the least.

MDA's response

2.83 **Notwithstanding these comments, MDA currently considers that a periodic 3-year review is adequate. There is already provision in the Guidelines for review "whenever there is sufficient evidence of market development or major technological changes that warrants an interim review".**

2.84 **MDA reiterates that the Guidelines are not intended to preclude future technological developments but rather provide references to specific technologies as examples that meet the guidelines.**

2.85 **MDA also considers that the Guidelines should be published for transparency and ease of compliance. Moreover, MDA notes that these are guidelines setting out the minimum requirements to be met, whilst actual implementation is a function of the RQL and SQL's requirements. Therefore, the Guidelines should not contain confidential information which cannot be published.**

Implementation date

2.86 One respondent believed it is unlikely that their concerns can be addressed before 30 June 2011 and therefore recommended a postponement or abandonment of the Measure.

2.87 A second respondent opined that 30 June 2011 is too aggressive to be achievable.

MDA's response

2.88 **MDA notes the concerns of these two respondents. However, in view that the two nationwide subscription television service licensees, SingNet and SCV, which will likely be designated as RQLs, are both already broadcasting premium television content, including live content, and have already deployed content protection systems and anti-piracy systems accepted by premium content owners, MDA does not consider it necessary to delay the effective date of the Guidelines and the implementation date of the Measure further. As such, MDA**

the Guidelines will come into effect on 2 July 2011, in time for the Measure to be implemented on 1 August 2011.

GENERAL COMMENTS

Obligations on RQLs and right of action for CPs

2.89 One respondent felt that each RQL should be required to take immediate and effective action to close down program streams being used to feed unauthorized redistribution (including from the internet). It was felt that this was important given that QC may include live content.

2.90 The same respondent commented that the Guidelines should include obligations to create the necessary structures and procedures for carrying out various aspects of the Guidelines (e.g. responsible RQL officials who can be real-time points of contact for remedial action).

2.91 A second respondent added that a mechanism must be included to add protected digital interfaces to the STB requirements over time. The respondent commented that any digital outputs added to the STB guidelines, however, should always be protected with the appropriate link protection scheme (such as HDCP or DTCP). The respondent also felt that the license agreement should contain the standard terms that are usually found in content protection technology licenses to offer greater protection to CPs and right of action against RQLs breaching the Guidelines.

2.92 A third respondent commented that MDA should offer the security requirements as "reference" requirements, that CPs and RQLs are free to negotiate on a case-by-case basis.

MDA's response

2.93 **MDA reiterates that the Guidelines provide a baseline that MDA will reference to determine whether the RQL has fulfilled its obligations stated under the MMCC 2010 for Content Protection Security Requirements.**

2.94 **MDA notes the copyright concerns of the respondents and views that the SQL and the RQL could incorporate such copyright protection terms into their cross-carriage agreements.**

2.95 **RQLs and SQLs are free to create the necessary structures and procedures to enable compliance with the Guidelines, through commercial negotiation.**

2.96 A respondent agreed with the market-based approach of commercial negotiation between SQL and RQL regarding QC put forward by MDA. However, the respondent felt that the commercial agreement between the RQL and SQL should be able to include the same QC security obligations on the RQL as those agreed between SQL and CP, and allow the CP to obtain compensation from the RQL for breaches in security or harm caused from leaks/theft by the RQL or its subscribers.

MDA's response

2.97 **MDA agrees with the respondent that security obligations, including any compensation issues, should be incorporated in the cross-carriage agreements between the SQL and the RQL. Where an SQL and an RQL are unable to reach a mutually acceptable cross-carriage agreement, the affected parties may request MDA's assistance through the conciliation and/or dispute resolution processes as set out in the MMCC 2010.**

Impact of the Guidelines upon RQLs

2.98 A respondent commented that any requirement imposed by the MMCC 2010 should only take effect upon finalisation of the MMCC 2010 and only be applicable to new headend, CPDS and STBs, excluding those already ordered or commissioned.

2.99 The same respondent also stated that the RQL's business viability should not be adversely affected in the effort to uphold an ideal level of security requirements.

MDA's response:

2.100 **MDA clarifies that the Guidelines and the requirements imposed by the MMCC 2010 will apply to all equipment, both existing equipment and any equipment yet to be purchased or ordered, once the Guidelines are implemented.**

2.101 **This is considered reasonable in order to adequately protect QC. The Guidelines aims to strike a balance between adequate protection of QC and fair and reasonable obligations on the RQLs. MDA considers that these requirements are not unreasonable given that an RQL is likely to already have in place suitable protections in place for its existing content.**

Application of the Guidelines to existing pay TV retailers

2.102 One respondent commented that SingNet and SCV must meet both the requirements of the Guidelines, as well as any individual CP security requirements, before being approved as RQLs that can receive QC from that CP.

2.103 The respondent pointed out that the fact that some CPs already sell content to these two operators was not evidence in itself that they meet the required content protection security standards. The respondent noted that CPs assess the content protection systems and anti-piracy measures provided by potential licensees on an individual basis.

2.104 The respondent requested that MDA must clarify that the Guidelines are not CP "guidelines" that "should" be observed but rather CP requirements that device manufacturers and RQLs must meet in order to receive and process QC prior to any proposed implementation of the Measure.

2.105 A second respondent stated that SQLs and RQLs should continue to be free to negotiate the requirements for carriage of QC. The respondent also sought clarification on whether the SingNet and SCV already have sufficient systems for the MMCC 2010, or if they need to change to comply, or if they are exempted through "grandfather rights".

MDA's response

2.106 **MDA clarifies that there will be no "grandfathering of rights" since under the MMCC 2010, it is stated that the RQL should ensure its compliance with the content protection security principles set out in the MMCC 2010 through certification, and on an ongoing basis. Furthermore, CPs could allay their concerns through contractual agreements with SQLs in relation to the protection of cross-carried QC.**

3. Conclusion and Issuance of Guidelines

3.1 MDA has studied all the comments submitted by the respondents and has developed the Guidelines on minimal content protection security requirements to enable compliance with the MMCC 2010 obligation on RQLs to protect the security of cross-carried QC. The Guidelines balance the interests of various stakeholders and will not hinder CPs, SQLs and RQLs in their ability and flexibility to develop content protection security requirements to protect the integrity of the content while complying with the requirements of the Measure.

3.2 The Guidelines will take effect from 2 July 2011.

3.3 MDA will review the Guidelines in the next 3-yearly review or whenever there is sufficient evidence of market development or major technological changes that warrants an interim review.

Annex A: References

A1 "5C Digital Transmission Content Protection Release 1.0", as amended by the Digital Transmission Licensing Administrator, LLC (DTLA)

A2 CableLabs' tru2way Host Device License Agreement, July 1, 2010

A3 CEA-805-D (November 2008): "Data Services on the Component Video Interfaces"

A4 Content Protected Digital Output License Agreement, December 20, 2005

A5 Digital Transmission Content Protection Adopter Agreement

A6 Digital Transmission Content Protection Specification

A7 EnCentrus Content Protected Digital Output Port System Description, Revision 1.2, January 2006

A8 ETSI EN 300 294 V1.4.1 (2003-04): "Television systems; 625-line television Wide Screen Signalling (WSS)"

A9 High-Bandwidth Digital Content Protection License Agreement

A10 High-Bandwidth Digital Content Protection Specification

A11 "High-Bandwidth Digital Content Protection System, Rev. 2.0 Interface Independent Adaptation" as amended by the Digital Content Protection, LLC (DCP)

A12 IEC 62375 International Standard "Video systems (625/50 progressive) – Video and accompanied data using the vertical blanking interval – Analogue interface"

A13 Motion Picture Association of America Digital Services Content Security Best Practices Version 1.0

A14 Motion Picture Association of America Distribution Content Security Best Practices Version 1.0

A15 Motorola IPRM System Submission of New Digital Outputs and Content Protection Technologies; Revision 2.7

A16 Recording Protection System for Portable extension Technical Specification, Revision 0.92, November 2009

A17 "Specifications of the Macrovision Copy Protection Process for STB/IRD Products" Revision 7.1.S1, October 1, 1999

A18 Video Content Protection System Agreement, September 1, 2004

A19 Vidi System Description Version 1.0, March 2004

Annex B: Glossary of Terms

3DES – 112-bit, triple data encryption standard.
576i (interlace scan) – standard-definition interlaced video usually used in traditionally PAL and SECAM countries.
576p progressive scan outputs – standard progressive video display resolution.
AES – advanced encryption standard, a symmetric-key encryption standard adopted by the U.S. government. The standard comprises three block ciphers: AES-128, AES-192 and AES-256, adopted from a larger collection originally published as Rijndael. Each of these ciphers has a 128-bit block size, with key sizes of 128, 192 and 256 bits, respectively. The AES ciphers have been analysed extensively and are now used worldwide, as was the case with its predecessor, the Data Encryption Standard (DES).
APS – analogue protection system, also known as Copyguard, is a DVD copy prevention system originally developed by Macrovision.
Automatic Gain Control – an adaptive system found in many electronic devices. The average output signal level is fed back to adjust the gain to an appropriate level for a range of input signal levels.
CA – conditional access, the protection of content by requiring certain criteria to be met before granting access to the content.
CAS – conditional access system, a technology used to control access to digital television services to authorized users by encrypting the transmitted programming.
CCI – copy control information, the use of data that is provided within or in addition to media that is used to enable or disable the ability of devices to make copies of media.
CCTV – closed-circuit TV, the use of video cameras to transmit a signal to a specific place, on a limited set of monitors.
CEA-805-D – standard that specifies how data are carried out on analogue component video interfaces and addresses the signal format and data structure of information when carried.
CGMS-A – analogue Copy Generation Management System.
Colorstripe – part of Macrovision's Analogue Copy Protection (ACP) for DVD-Video.
Consensus Watermark – a copy control watermark that has been developed on a multi-industry basis pursuant to a broad consensus in an open, fair, voluntary process, and that has been adopted and is being used by major content providers.
Constrained Image – an image having the visual equivalent of no more than 520,000 pixels per frame (e.g. an image with resolution of 960 pixels by 540 pixels for a 16:9 aspect ratio). A constrained image may be attained by reducing resolution, for example, by discarding, dithering, or averaging pixels to obtain the specified value. A constrained image can be displayed using video processing techniques such as line doubling or sharpening to improve the perceived quality of the image. By way of example, a constrained image may be stretched or doubled, and displayed full-screen, on a 1000-line monitor.
Copy Control Usage Rights Information – information relating to the copying and Internet redistribution rights for content that a system operator has negotiated with the content owner.

CPDO – the secure digital recording method as specified by EnCentrus Systems, Inc. in its document entitled *EnCentrus Content Protected Digital Output Port System Description*; Revision 1.2 dated January 2006.

CPDS – content protection delivery system, a term used to encompass conditional access security (CAS) systems and digital rights management (DRM) systems.

CSA – Common Scrambling Algorithm, the encryption algorithm approved by the Steering Board of the DVB Project, is comprised of the Common Descrambling System and Scrambling Technology. It is used to provide content protection and conditional access support for MPEG video streams within digital broadcasting systems. The latest version, DVB CSA3 has been approved by the Steering Board of the DVB Project, is comprised of the DVB CSA3 Descrambling System and Scrambling Technology. The specification for each is distributed separately under arrangements with the European Telecommunications Standards Institute (ETSI), which acts as custodian for the 6 companies which have developed the DVB CSA3 algorithm.

DQC – decrypted qualified content, a term describing qualified content which is not encrypted in any way.

DRM – digital rights management, a term for access control technologies that can be used by hardware manufacturers, publishers, copyright holders and individuals to impose limitations on the usage of digital content and devices.

DTCP – method of encryption, decryption, key exchange and renewability that is described in the specification entitled "5C Digital Transmission Content Protection Release 1.0", as amended by the Digital Transmission Licensing Administrator, LLC (DTLA) from time to time.

DVI – digital visual interface, a connection that can transfer a digital video signal from a source component directly to a video display that also has a DVI connection without an analogue conversion.

Displayport – a digital display interface standard put forth by the Video Electronics Standard Association (VESA). It defines a royalty-free, digital audio/video interconnect intended to be used primarily between a computer and its display, or a computer and a home-theatre system.

EEPROM – electrically erasable programmable read-only memory, a type of memory used in computers and other electronic devices to store small amounts of data that should be saved when power is removed, e.g., calibration tables or device configuration.

EMI – encryption mode indicator, allows for a method and system for transferring information.

EPN – encryption plus non-assertion, technology that allows users to make as many copies of their content as they would like.

ETSI EN 300 294 – specifies the wide screen signalling information, the coding and the way of incorporating the coded information into a 625-line system

HDCP – method of authentication, encryption, decryption, and renewability that is described in the specifications entitled "High-Bandwidth Digital Content Protection System" as amended by the Digital Content Protection, LLC (DCP) from time to time.

High definition analogue form – a format or output that is not digital, and has a resolution higher than Standard Definition Analogue Form or Output.
HDMI – high-definition multimedia interface, a compact audio/visual interface for transmitting uncompressed digital data, and an alternative to consumer analogue standards.
ICT – image constraint token, a protocol flag that can cause down-sampling of high-definition video content on Blu-ray and HD DVD to slightly-better-than-DVD quality video.
IEC 62375 – standard for video systems, video and accompanied data using the vertical blanking interval – analogue interface
Internal interface – any internal interconnection not defined as a user-accessible bus and includes, but is not limited to, any signal on a chip bonding pad, JTAG, or other testing point (any place signals move onto and off of a silicon die).
IPRM – IP rights management, in accordance with the Motorola IPRM System Submission of New Digital Outputs and Content Protection Technologies, as amended.
IPTV – Internet protocol television, a process of providing television services through the use of Internet protocol networks.
JTAG – Joint test action group, a type of port initially devised for testing printed circuit boards using boundary scan but more generally can be used as a means of interface with chips.
MAC address – a unique identifier assigned to most network adapters or network interface cards (NICs) by the manufacturer for identification, and used in the Media Access Control protocol sub-layer.
MPAA – Motion Picture Association of America, a non-profit trade association formed to advance the interests of the movie studios. Its members consist of seven major studios: the Walt Disney Company, Sony Pictures, Metro-Goldwyn-Mayer, Paramount Pictures, Twentieth Century Fox, Universal Studios, and Warner Bros.
MPEG – Moving picture experts group, an asymmetric compression standard for audio and video compression and transmission.
NGNBN – the Next Generation Nationwide Broadband Network, Singapore's next-generation fibre network.
PAL RF – phase alternate line radio frequency, an analogue television encoding system used in broadcast television systems in large parts of the world
RCI – redistribution control information, as defined in CEA-805-D (November 2008): "Data Services on the Component Video Interfaces".
Reprotection – the application of an approved, protection technology, when required, to DQC received from the RQL's service that is to be output from the RQL's STB receiver, and the integrity of the system and methods by which such application is assured.
RGB – an additive colour model based on red (R), green (G), and blue (B) light; RGB is used by computers, televisions, and film recorders to display colours; mixing equal amounts of red, green, blue light will produce white light.
RPSP – the secure digital recording method as specified by Samsung Electronics Co. Ltd, in its document entitled *Recording Protection System for Portable extension Technical Specification*; Revision 0.92 dated November 2009.
SRM – system renewability message data, which is transmitted to set-top boxes, or other devices, using a transport protocol such as an Internet protocol-type data stream.

S-video – Separate Video, an analogue video signal that carries video data as two separate signals: luma (luminance) and chroma (colour).
Triple DES - triple data encryption standard, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block. Because of the availability of increasing computational power, the key size of the original DES cipher was becoming subject to brute force attacks; Triple DES was designed to provide a relatively simple method of increasing the key size of DES to protect against such attacks, without designing a completely new block cipher algorithm.
tru2way – a brand name for interactive digital cable services delivered over the cable video network.
User-accessible bus – a bus which is designed for end-user upgrades or access such as SmartCard, PCMCIA, Cardbus or PCI that has sockets or is otherwise user accessible, but not memory buses, CPU buses and similar portions of a STB receiver's internal architecture.
VGA – Video Graphics Array system, typically implemented as a computer video output that is 640x480 pixels.
VOD – video-on-demand, an interactive TV technology that allows subscribers to view programming in real time or download programs and view them at a later stage.
Y, R-Y, B-Y – the formula used to convert RGB into the various signals used for TV/video. This designation is also found on video equipment to represent analogue component video inputs and outputs, although they are also designated as Y, Pb and Pr (YPbPr). The Y represents the luma (brightness), and B-Y and R-Y represent colour difference signals. For TV/video storage and transmission, RGB signals are converted to either YUV (NTSC/PAL composite video), YPbPr (component analogue) or YCbCr (component digital).
YUV – the colour encoding system used for analogue television worldwide (NTSC, PAL and SECAM). The YUV colour space (colour model) differs from RGB, which is what the camera captures and what human eye can interpret.
VCPS – Video Content Protection System for recording encrypted content on DVD+RW and DVD+R optical digital media protected by VCPS technology.