

# **EXHIBIT 1**

## **Statement of DTLA Criteria for Reviewing Recording and Retransmission Protection Technologies**

The DTLA Policy Group and Technical Group will engage in a review process designed to determine whether, from technical, legal and policy perspectives, a proposed recording or retransmission protection technology will maintain integrity and robustness for DT Data, and to consider whether Content Participants, certain other content owners and Adopters are satisfied with the level of protection provided by the technology and licensing framework. This review process is intended to be conducted by the DTLA using objective criteria, rather than subjective judgments, which criteria are set forth below.

### I. DTLA Review

#### A. Policy Review

1. The proposed technology does not impair interoperability with respect to the exchange of DT Data among licensed products.

#### B. Legal Review

1. The license agreement implements requirements that are no less stringent than the requirements of Exhibit B Part 1: Compliance Rules for Sink Functions, as set forth in the most current version of the DTLA Adopter Agreement, including with respect to maintaining the protection of DT Data through authorized digital, analog and high definition analog outputs, and prohibiting unauthorized retransmission of DT Data over wide area networks and the Internet.

2. If the technology so permits, the license agreement provides for a right of revocation or for renewability where the security elements of a particular device have been cloned.

3. The license agreement provides protections against the device interfering with a consensus watermark, in a manner no less stringent than the obligations set forth in Section 6 of Exhibit B, Part 1: Compliance Rules for Sink Functions in the most current version of the DTLA Adopter Agreement.

4. The license agreement imposes robustness requirements that are no less stringent than the applicable Robustness Rules as set forth in the most current version of the DTLA Adopter Agreement.

5. Legal recourse potentially is available in case of circumvention of the technology by persons other than licensees.

6. The license provides, or the licensor commits, that future amendments to the license that would affect the license terms and conditions that were disclosed to DTLA will not diminish the protections afforded to DT Data, as described above.

## C. Technical Compliance

The proponent of the technology should provide to the DTLA sufficient technical information to demonstrate that:

1. The recording technology provides for detection and correct response to copy control information, as defined by the DTLA Specification (in EMI, Embedded CCI or both).
2. The recording technology provides for a means of security for the making of permissible copies, as set forth in Section 2 of Exhibit B, Part 1: Compliance Rules for Sink Functions of the most current version of the DTLA Adopter Agreement.
3. The recording technology provides that removable recorded media will maintain the required level of protection when played back on a device other than the device upon which the recording was made.

## II. Content Owner and Implementer Support

1. In addition to meeting the above criteria, the proponent may provide to DTLA evidence of support for the technology and licensing terms and conditions from Content Participants and DTCP Adopters. In addition, the proponent also may provide to DTLA evidence of support for the technology and licensing terms and conditions from:

- a. Motion picture companies that are members of the MPAA, in the case of technology used to protect audiovisual works,
- b. Major sound recording labels, in the case of technology used to protect only sound recordings, and
- c. Manufacturers interested in implementing both the proposed technology and DTCP.

2. In the event that the proposed technology and licensing terms and conditions do not meet one or more of the requirements set forth in subsections B and C of Section I above, the proponent should provide DTLA with evidence of support for the technology from a substantial number of major motion picture or recording companies, as applicable.

## **EXHIBIT 2**

**Submission of  
New Digital Outputs and Content Protection Technologies**

**September 17, 2004**  
Rev. 1.4

© Cable Television Laboratories, Inc., 2004. All Rights Reserved  
858 Coal Creek Circle  
Louisville, CO 80027-9750  
[www.cablelabs.com](http://www.cablelabs.com)

# Table of Contents

<b>1</b>	<b>BACKGROUND</b>	<b>3</b>
<b>2</b>	<b>PROCESS AND PROCEDURE</b>	<b>3</b>
<b>3</b>	<b>ELEMENTS OF SUBMISSION</b>	<b>4</b>
3.1	LICENSE TERMS	4
3.2	SECURITY OVERVIEW	4
3.3	VIDEO TRANSPORT	5
3.4	CONTENT PROTECTION PROFILES	5
3.5	KEY EXCHANGE ALGORITHMS	5
3.6	SECURITY INTERFACES	5
3.7	SECURITY PROCESSING	5
3.8	CERTIFICATE MANAGEMENT	5
3.9	REVOCAION/RENEWABILITY OF KEY	6
3.10	POINTS OF ATTACK/POTENTIAL WEAKNESSES	6
3.11	COMMERCIAL USE	6
3.12	CONTACT INFORMATION	6
<b>4</b>	<b>REVIEW CRITERIA</b>	<b>6</b>
4.1	VIDEO TRANSPORT	6
4.2	SECURITY INTERFACES	7
4.3	POINTS OF ATTACK AND SYSTEM WEAKNESSES	7
4.4	EFFECTIVENESS OF PROPOSED TECHNOLOGY	7
4.5	SECURITY PROCESSING	7
4.6	REVOCAION AND RENEWABILITY OF KEYS	7
4.7	NEW ALGORITHMS	7
4.8	DFAST/JTS/CABLECARD CONSISTENCY	7
4.9	LICENSING TERMS	8
4.10	OVERALL IMPACT ON THE CABLE NETWORK	8
<b>5</b>	<b>CONTACT INFORMATION</b>	<b>8</b>

## 1 Background

Under the Compliance Rules of the DFAST Technology License Agreement (“DFAST License Agreement”), various digital outputs and content protection technologies are allowed on Unidirectional Digital Cable Products (UDCPs), e.g., 1394/DTCP, DVI/HDCP, HDMI/HDCP, etc. Additionally, CableLabs may approve new digital outputs or content protection technologies.<sup>1</sup>

Each digital output and content protection technology review is performed in the context of a distribution network that must protect high-value content that is encrypted at the source and which must be protected throughout the network. Unlike broadcast flag technologies that serve a more limited purpose, content protection technology in UDCPs is required to maintain the integrity of a conditional access distribution network, and must not, among other things, “technically disrupt, impede or impair the delivery of services to a cable customer.”

This document outlines the general process, procedures, elements of a submission, and the review criteria used by CableLabs in analyzing such submissions for new digital outputs or content protection technologies for UDCPs. Approval of any digital output, copy protection, or encryption technologies under this program is not deemed to be approval for any use other than UDCPs, including without limitation bi-directional digital cable products, or products intended for broadcast flag approval.

CableLabs reserves the right to modify the criteria for submissions outlined herein (including, but not limited to changing the fees for output/recording approval), and the criteria under which CableLabs will review such submissions.

## 2 Process and Procedure

Any party desiring to obtain approval of a protected digital output, content protection, digital rights management, or secure recording and storage technology may submit such proposal to CableLabs at the address provided in Section 5. Complete submissions must include all information necessary to evaluate the submission in detail, and the associated submission fee posted at <http://www.cablelabs.com/udcp/downloads/2004pricing.pdf>.

Some of the minimal essential elements are included herein. Detailed documentation, generally in the form of a specification, should be provided by the proponent in order for CableLabs to perform a complete review. Where appropriate, reasonable non-disclosure restrictions may be accommodated (e.g., covering third party security reviews exposing weaknesses or vulnerable points of the proposed system). Failure to provide complete information may result in disapproval of the proposed technology, and/or delay in a response from CableLabs.

CableLabs will evaluate all submissions in a reasonable, objective, and non-discriminatory manner. Decisions will be made on the effectiveness of the proposed technology, the license terms governing the secure implementation of the technology, and other objective criteria as described herein.

If approved, the new digital output, content protection, secure recording, or DRM technology will be added to the Compliance Rules (Exhibit B) of the DFAST Technology License Agreement in the appropriate section(s), along with any accompanying restrictions or additional information on the use of the output or technology (e.g., Robustness or Compliance Rules). Approval of any particular technology under this program does not automatically result in changes to the Joint Test Suite (“JTS”) that must be used by all manufacturers to verify compliance of individual UDCP models prior to marketing such models as “Digital Cable Ready.”

After a technology is approved by CableLabs for use in UDCPs, any material or substantial changes to the technology must be submitted to CableLabs for re-approval. Material or substantial changes include, but are not limited to: 1) mapping to a new transport or media; 2) changes in the encoding or treatment of content; 3) changes

---

<sup>1</sup> See DFAST Technology License Agreement, Exhibit B (Compliance Rules) Section 2.4.4. The FCC Second Report and Order (FCC 03-225) provides that CableLabs shall make such initial determinations, subject to FCC review.

that may have a material and adverse affect on the integrity or security of the technology; 4) changes in the cryptographic method used (except where the algorithm is unchanged and only the key length is expanded); 5) changes in the scope of redistribution; and 6) any fundamental change in the nature of the technology.

### **3 Elements of Submission**

The technologies covered under this evaluation program include protected digital interfaces, secure recording and content storage and playback, and digital rights management. The specific security measures used by these technologies may vary. Additionally, different output technologies may employ transport mechanisms and protocols that require certain limitations or implementation restrictions. This section identifies several crucial elements that should be common to all submissions, but is not an exhaustive list that precludes other types of information that may be necessary for fully evaluating a particular technology. Submissions must not omit or misrepresent material specifications, facts, or other details necessary for CableLabs to conduct a thorough and accurate review of the technology. CableLabs may request additional information or clarification as reasonably necessary to fully assess the proposal. Until such information or clarification is provided, the submission will not be considered complete.

Submissions may incorporate mixed elements of protected digital interfaces, secure recording and content storage, and digital rights management technologies. In this situation, one complete submission may be sufficient for conducting the review, and only one submission fee will be charged.

#### ***3.1 License Terms***

License terms, if any, should be included with the submission. Preferably the complete, executable, license should be included. Essential terms should minimally include:

- royalty (or royalty-free)
- commitments to offer on a reasonable and non-discriminatory (RAND) basis
- Robustness Rules and implementer guidelines or checklists (see note below)
- Compliance Rules (see note below)
- Enforcement provisions (conformance or certification testing, implementation auditing, etc.)
- Approval procedures for downstream technologies and recording methods
- Change provisions (to the technology or the license terms), including change process participants
- IPR indemnity or other IPR arrangements (e.g., a patent pool)
- Warranty Provisions
- Term
- A list of known essential patents
- Authority and limitation, criteria, process, and participants required for revocation of devices or outputs.
- Compliance with applicable encoding rules.

#### Note on Robustness and Compliance Rules:

A UDCP containing any digital output or content protection technology must comply with the Robustness and Compliance Rules in the DFAST Technology license. The DFAST robustness and compliance rules are controlling for the overall UDCP product. As a result, the robustness and compliance rules in any manufacturer's technology license must not be contradictory to such rules in the DFAST license. Any proposed language to add the digital output or recording technology to the allowed outputs/ recording technologies listed in the Compliance Rules of the DFAST license should also be submitted.

#### ***3.2 Security Overview***

The security specification and documentation should include an introduction and security overview that includes:

1. An overview of the security architecture, its components (e.g., Packaging Server, License Server, Client, etc.), their functions, and key interfaces; connectivity requirements for output/security.
2. A detailed block diagram of the security architecture identifying the key components and interfaces necessary to implement the solution from end-to-end, including receiver and other media elements (PCs, storage, display, etc).

3. This overview should also clearly identify video transport options where there are alternatives in implementation. For example, video transport cipher algorithms (AES, 3-DES, etc.), and key exchange algorithms, (Diffie-Hellman, RSA, etc).

### ***3.3 Video Transport***

The security specification should include details regarding the video transport method and the specifics of how the Copy Control Information (CCI) presented by the CableCARD across the CableCARD-Host Interface is translated into the proposed environment/profile. The specification should also detail how the video transport is associated with any content protection profiles and the methods for authenticating and protecting the content protection profiles.

In addition, specifications or other technical descriptions must be provided to fully explain how the proposed digital output supports one or more video transport protocols capable of delivering all defined<sup>2</sup> audio-video services associated with a UDCP without disrupting, impeding or impairing the delivery of such services to the final display device. Such services also include, but are not limited to delivery, decoding, or display of analog and digital closed caption data, content advisory ratings, and emergency alert system messages. CableLabs will review only the transport mechanisms and protocols that are included in the submission. Technology approvals will be made on a transport-by-transport, or media-by-media basis. Submitters may re-submit previously approved technologies for approval on a different transport, and CableLabs will use reasonable commercial efforts to expedite approval of the proposed new transport, providing that the submitter provides a complete and thorough explanation of all legal and technical modifications that result from the new transport. Approval of a particular technology should not be considered a “blanket approval” for that technology on any transport.

### ***3.4 Content Protection Profiles***

The security specification should include details regarding the format and use of any digitally signed content protection profiles used in the system. The security specification should also define the structure and options that are employed in this system and all messaging and signaling needed for implementation.

### ***3.5 Key Exchange Algorithms***

The security specification should include details regarding the authentication of receiving devices, storage devices, and any devices connected thereto. The security specification should also include authentication methods of the License server, packaging server and the client. All of the session keys exchanged and the cryptographic protocols used should be well defined for a complete review. Non-encryption alternatives may also be employed, but should be explained thoroughly.

### ***3.6 Security Interfaces***

The specification should include details that completely define the security interfaces of the overall system and the creation and protection of symmetric and asymmetric keys. Detailed definitions of the security components implemented in hardware and software need to be defined so that these security interfaces can be reviewed.

### ***3.7 Security Processing***

The specification should include details that demonstrate how the keys and secrets are protected from reading and writing during the cryptographic calculations, and how the CCI, image constraint and other parameters are protected throughout the system.

### ***3.8 Certificate Management***

The specification should include details that completely define the certificate usage, methods for protecting RSA private keys, revocation methods and how certificates relate to content and the packaging/license servers. Details on

---

<sup>2</sup> See for example, ANSI/SCTE-40 2004; Section 8.1

installation, signing, chaining to the root, as well as the overall structure, validation of security, and protection against cloning of certificates should be included.

### ***3.9 Revocation/Renewability of Key***

The specification should include details on how system key revocation is accomplished, and how key renewability is accomplished.

### ***3.10 Points of Attack/Potential Weaknesses***

The specification should include reviews or threat analyses that may be available to review the possible weaknesses/threats and the trade-off versus the applied costs. Independent security reviews should also be provided. As appropriate, non-disclosure restrictions can be put in place to cover the review.

### ***3.11 Commercial Use***

The submission should include any known commercial use of the proposed output or technology, as well as any known affects on performance of devices, and interoperability issues. Submitter should provide a list of adopters (implementers) and supporters (owners, content developers, etc.), and identify any commercial relationships between the technology submitter and any content owners.

### ***3.12 Contact Information***

The submission should include the names and contact information for the security specialist and other individuals who may be contacted with questions concerning the submission.

## **4 Review Criteria**

CableLabs will evaluate all proposals in a reasonable, objective, and non-discriminatory manner. Depending on the specific output or technology submitted, criteria for evaluation will include the following:

### ***4.1 Video Transport***

- Are the methods defined for translating and delivering CCI from the CableCARD across the CableCARD-Host Interface into the proposed device environment or profile?
- A: Compressed Digital Outputs:
- Is the original digital compression system utilized on the interface, or is the signal re-compressed?
  - If recompressed, what system, profile, resolution and data rates are required?
  - If the original compression is preserved, is the full transport multiplex sent over the interface, or is the interface limited to single program streams sent after demux?
  - If the output carries the full transport stream, how does the system information (e.g., OOB data) get transported?
  - What methods are used to ensure uninterrupted flow of programming across this interface, regardless of other traffic that might be present on the interface (QOS)?
  - What is the minimum guaranteed data throughput provided on the interface?
  - What methods are used to enable delivery, decoding, or display of analog and digital closed caption data, content advisory ratings, and in-band emergency alert system messages?
  - How are analog programming services preserved seamlessly on this interface?
  - How does the interface deliver MMI screens over this interface?
- B: Uncompressed Digital Outputs:
- What is the minimum guaranteed data throughput provided on the interface?
  - How are analog programming services preserved seamlessly on this interface?
  - What methods are used to enable delivery, decoding, or display of analog and digital closed caption data, content advisory ratings, and in-band emergency alert system messages?
  - How does the interface deliver MMI screens over this interface?

## **4.2 Security Interfaces**

- How is the security used on the video transport and how is the transport associated with content protection profiles and the methods for authenticating and protecting the content protection profiles?
- What are the key generation, key protection and key exchange methods used?
- Are there obvious areas where content is in the clear?

## **4.3 Points of Attack and System Weaknesses**

- Can technology be circumvented somewhere?
- Where are the lowest barriers to be attacked?
- Where will the hacker attack and what resources are required?
- What are possible weaknesses/threats and what is the trade-off of security versus the applied costs?

## **4.4 Effectiveness of proposed technology**

- Does the proposed technology adequately protect content passing through the digital output or being securely recorded or stored for later playback?
- What is the scope of content redistribution? Does the digital output or DRM technology effectively protect content from unauthorized redistribution through localization control or other geographic or user restrictions?

## **4.5 Security Processing**

- Are the keys and secrets protected from reading and writing during the cryptographic calculations?
- Are CCI, image constraint, and other controls protected throughout the system design?

## **4.6 Revocation and Renewability of keys**

- Does the product provide a system key revocation solution?
- Does the product provide a system key renewability solution?
- What criteria and processes are used for revocation and renewability? Who are the participants in the process?
- What is the minimum and maximum size of the system renewability message (SRM), and what format is it delivered in?
- How is the SRM generally delivered? What operational and infrastructure impacts would the revocation/renewability solution have on a cable network (including capital equipment or network upgrades that may be required)? What must a cable operator or other content distributor do to adopt the proposed revocation and renewability solutions?

## **4.7 New Algorithms**

- What is the relative strength of the algorithm?
- What is the relative strength of authentication with respect to other technologies?

## **4.8 DFAST/JTS/CableCARD Consistency**

- Does the proposed output/technology interfere with a UDCP device's meeting its DFAST or testing obligations? Is analog source switching or high definition pass-through required for the proposed digital output, and if so, what is the resulting impact to the JTS?
- Does the proposed output/technology interfere with OpenCable devices and interfaces?
- Does the proposed output/technology raise interoperability issues with other CableCARD devices and interfaces?
- Is the proposed interface interoperable with products from other manufacturers, or is it a proprietary or otherwise exclusive solution?
- Is the interoperability defined by industry standards (which ones) or license, or both?
- What specific changes would be required in the JTS? (Submitter should propose new PICS items and ATP modifications associated with the proposed technology.)

#### ***4.9 Licensing Terms***

- If licensable to third parties, does the license include the Robustness Rules, Compliance Rules, Conformance testing, Change provisions (to the technology or the license terms), IPR indemnity or other IPR arrangements (e.g., a patent pool), Warranty Provisions, Term, and other standard terms?
- Do the Robustness and Compliance Rules adequately cover any software being licensed with the technology?
- Does the license identify and grant appropriate rights for known relevant patents?
- How are downstream outputs and recording technologies approved by the licensor? What process is used to help ensure interoperability between technologies from different proponents?
- Is the technology offered royalty-free, or does it include commitments to offer reasonable and non-discriminatory (“RAND”) license terms? If software is part of the technology solution, does the license provide adequate software developer tools or other reasonable support for implementers?
- How do the Robustness rules fit with other licensing requirements?
- Are licensing terms compatible with and complimentary to the Encoding Rules applicable to Digital Cable Ready products?
- What license fees are required annually and on each device?
- Are the terms of use reasonable and fair?
- What is the scope of content usage rights for any proposed DRM technology?
- If not licensable to third parties, how does proponent assure the above?

#### ***4.10 Overall Impact on the Cable Network***

- What operational and infrastructure impacts would the proposed technology have on a cable network (including capital investment or network upgrades that may be required)?
- What must a cable operator or other content distributor do to adopt the proposed technology solution?

After receipt of a complete submission, CableLabs will document the reasons for approval, or disapproval, of the submission within the applicable timeframe.

### **5 Contact Information**

Should you have further questions regarding this document, please contact:

CableLabs  
858 Coal Creek Circle  
Louisville, CO 80027-9750  
Attn: Project Director, Business Relations, APS Department  
303 661-9100

## **EXHIBIT 3**



**Digital Transmission  
Licensing Administrator**

**REQUEST BY  
DIGITAL TRANSMISSION LICENSING ADMINISTRATOR LLC  
FOR APPROVAL OF DTCP-IP AS A  
NEW DIGITAL OUTPUT PROTECTION TECHNOLOGY**

Michael B. Ayers  
President  
Digital Transmission Licensing  
Administrator, LLC  
(949) 461-4714  
michael.ayers@tais.toshiba.com

Seth D. Greenstein  
Chair, DTLA Policy Committee  
McDermott, Will & Emery  
(202) 756-8088  
sgreenstein@mwe.com

Michael Andre  
Chair, DTLA Technical Working Group  
Intel Corporation  
(503) 712.1211  
michael.andre@intel.com

Date: April 8, 2005

## Table of Contents

Introduction and Background	1
I. Section 3.1: Licensing Terms	4
A. Fees	5
B. Reasonable and Nondiscriminatory Licensing	6
C. Compliance and Robustness Rules	7
D. Enforcement Provisions	8
E. Approval Procedures for Downstream Technologies and Recording Methods	8
F. Change Provisions	10
G. IPR Arrangements	12
H. Warranty Provisions	14
I. Term	14
J. Patent List	14
K. Revocation	15
L. Applicable Encoding Rules	15
II. TECHNICAL DESCRIPTION OF DTCP AND DTCP-IP	16
A. Section 3.2 -- Security Overview	16
1. Authentication and Key Exchange (AKE)	17
2. Content Encryption	17
B. Section 3.3: Video Transport -- Copy Control Information	18
C. Section 3.4: Content Protection Profiles	20

D.	Section 3.5: Key Exchange Algorithms	21
E.	Section 3.6: Security Interfaces	21
F.	Section 3.7: Security Processing	21
G.	Section 3.8: Certificate Management	21
H.	Section 3.9: Revocation/Renewability	21
I.	Section 3.10: Points of Attack/Potential Weaknesses	23
J.	Section 3.11: Commercial Use	23
K.	Section 3.12: Contact Information	23
	Conclusion	23

Attachments:

1. Adopter Agreement
2. Content Participant Agreement
3. DTCP Volume 1 V1.4 (Informational Version)
4. DTCP Volume 1 Supplement E V1.1 (Informational Version)
5. IP Statement



## **Introduction and Background**

The Digital Transmission Licensing Administrator, LLC (“DTLA”), pursuant to the CableLabs document “Submission of New Digital Outputs and Content Protection Technologies v. 1.4” (September 17, 2004) (hereinafter, “Submission”), hereby submits its request for approval by CableLabs of the use of the Digital Transmission Content Protection technology (“DTCP,” also known as “the 5C technology”) over Internet Protocol (known as “DTCP-IP”) as a protection technology for digital outputs on Unidirectional Digital Cable Products (“UDCPs”) and on Bidirectional Digital Cable Products (such as CHILA).

In 1996 and 1997, representatives of the motion picture, consumer electronics, information technology and cable and satellite industries met in the Digital Transmission Discussion Group (“DTDG”) of the Copy Protection Technical Working Group (“CPTWG”), to define in a Call for Proposals the technical parameters for a system to protect digital transmissions between devices connected over a home network. After the conclusion of more than a year of effort by the DTDG, Hitachi, Intel, Matsushita, Sony and Toshiba -- the “5C Companies” -- jointly produced the Digital Transmission Content Protection Specification, providing a simple and inexpensive method affording a high degree of protection for copyrighted commercial entertainment content transmitted over high-speed bi-directional digital interfaces.

DTCP defines a cryptographic protocol for protecting audio/video entertainment content from unauthorized copying, interception and tampering as it traverses high performance digital interfaces. Only commercial entertainment content delivered to a source device via another approved copy protection system -- including, but not limited to, conditional access systems used for digital cable and satellite video transmissions and, pursuant to the Federal Communication

Commission's adoption of regulations relating to the "Broadcast Flag," Unscreened and Marked Content -- are to be protected by the DTCP technology.

DTCP initially was mapped to the IEEE 1394 transport, in accordance with the terms of the CPTWG DTDG Call for Proposals in 1996. DTCP since has been mapped to protect other digital transports as well, and can be mapped to protect any high-speed bi-directional transport. DTCP has been mapped for use over Internet Protocol ("DTCP-IP") for wired and wireless transports, including Ethernet and 802.11 transports, for the MOST interface, for the USB transport, for Bluetooth and for Op-iLink. Work is underway to complete a specification mapping DTCP to the IDB 1394 interface for mobile environments.

DTCP was designed to coexist with current copy protection technologies, including conditional access systems for digital television transmission, and to be compatible with other content encryption and watermarking technologies developed in the future. DTLA works with technology proponents to render content protected with DTCP compatible with other digital output and recording protection technologies, and to authorize the interchange of protected content between DTCP and such other technologies.

DTCP has been authorized for use as a protection method for digital output of recorded content protected with DVHS, CPPM, CPRM, CPS for BD-RE, MG-R(SVR) for Memory Stick PRO and Hi-MD, and VCPS. In addition, the DVD Copy Control Association recently approved the use of DTCP for protection of motion picture content output from CSS-encrypted DVD video discs over DTCP-IP, and for automotive use over the MOST and IDB 1394 digital interfaces.

DTCP has been licensed by more than 120 companies, including manufacturers of television receivers, STBs and digital recorders; IT companies; cable system operators; semiconductor manufacturers; and component resellers. Numerous digital television products

currently on the market, including high definition digital television sets, D-VHS and DVD-R, -RAM and -RW recorders and cable STBs, utilize DTCP for protection of digital video outputs. Information on representative 5C-enabled DTV, STB, DVR and semiconductor products from non-5C Companies are attached at Appendix 1.

Two major motion picture studios, Sony Pictures Entertainment and Warner Bros., have signed Content Participant Agreements granting them an affirmative right to encode or have encoded DTCP for their Commercial Entertainment Content. MPAA member companies have expressed support for the use of DTCP to protect content marked with the Broadcast Flag. Pursuant to an “IP Statement” first issued by DTLA in July 2001, DTLA has represented that it will not enforce its intellectual property rights in DTCP against content owners that wish to use and require use of DTCP without a license, so long as they encode or direct to be encoded their content with DTCP in accordance with the applicable Encoding Rules. *See* IP Statement, <http://www.dtcp.com/data/IPStatement07102001.pdf> Thus it is unnecessary for any content owner to enter into a Content Participant Agreement in order to be able to use DTCP to protect its commercial entertainment content. DTLA anticipates that a majority of content owners will avail themselves of the IP Statement rather than to incur the expense and responsibilities appurtenant to a Content Participant Agreement with DTLA.

The DFAST License Agreement, the Nonexclusive POD-Host Interface License Agreement (“PHILA”) dated August 1, 2003, and the Amended and Restated Nonexclusive CableCard-Host Interface License Agreement dated March 11, 2005 (“CHILA”), authorize the use of DTCP as an approved digital output protection technology for any licensed Unidirectional Digital Cable Product having an IEEE 1394 output. *See* DFAST License, Exhibit B (Compliance Rules) ¶ 2.4.1; PHILA, Exhibit C (Compliance Rules) ¶ 2.4.1; and, CHILA,

Exhibit C (Compliance Rules) ¶ 2.4.1. Moreover, under the PHILA, a licensed product may pass “Controlled Content “ to any digital output protected by DTCP; in other words, a product licensed under PHILA may use DTCP over IEEE 1394 or any of the other wired and wireless transports supported by DTCP.

In August 2004, the Federal Communications Commission certified the use of DTCP over 1394, USB, MOST and Op-iLink for protection of Unscreened Content and Marked Content (*i.e.*, content marked with the “Broadcast Flag”). Certification of DTCP-IP was conditioned upon submission by DTLA of the final Specifications for DTCP-IP incorporating the additional localization requirement of a Round Trip Time (“RTT”) of no greater than 7 ms. Order FCC 04-193 released August 12, 2004 (“Certification Order”), ¶ 74. On March 11, 2005, DTLA fulfilled that condition by submitting a Supplement to Certification of Digital Transmission Licensing Administrator LLC for Approval Of DTCP-IP as an Authorized Output Protection Technology.

**I. SECTION 3.1: LICENSING TERMS**

The Submission requests an explanation of the licensing terms and conditions under which a proposed technology will be offered. DTLA submits herewith a copy of the Adopter Agreement and Content Participant Agreement, and in this section summarizes in detail the basic terms under which DTCP is made available. These license terms are equally applicable to DTCP-IP as well as all other mappings of DTCP.

DTCP is licensed by the Digital Transmission Licensing Administrator, LLC.<sup>1</sup> DTLA makes available two basic types of licenses to the DTCP technology:

---

<sup>1</sup> Administration services for licenses to DTCP are provided pursuant to contract with an independent entity, License Management International, LLC.

(continued...)

- **Adopter Agreement**, for the manufacture of Licensed Products and Licensed Components that implement the DTCP Specification, submitted at Tab A<sup>2</sup>
- **Content Participant Agreement**, for encoding of Commercial Entertainment Content with DTCP, submitted at Tab B<sup>3</sup>

DTLA responds below to the specific points identified in section 3.1 of the Submission.

**A. Fees**

The DTLA agreements provide for payment of annual administration fees, and fees for generating device certificates. Content Participants pay an annual administration fee of \$18,000. Adopters have a choice of balancing a lower administration fee with a higher per certificate cost (which would result in lower costs for Adopters that use DTCP on a smaller scale) or a higher administration fee with a lower per certificate cost (which would result in lower costs for Adopters that use DTCP on a larger scale). The specific administrative fees and per certificate costs are set forth in the following table from the Procedural Appendix of the Adopter Agreement, Exhibit A:

Category	Annual Administration Fee (US \$)	Per Certificate Fee		
		Restricted	Full	Restricted/Full
<hr/>				

<sup>2</sup> DTLA also makes available agreements that permit the resale and distribution of Licensed Components: a “Reseller Agreement,” for the resale of Licensed Components to fellow Adopters, and a “System Operator Agreement” for the secure download by a cable or satellite system operator of a monolithic software module, including certain Licensed Components, to an authorized set top box on consumer premises. These agreements are submitted at Tabs C and D, respectively.

<sup>3</sup> As noted, DTLA also has represented in an IP Statement that it will not assert its intellectual property rights in DTCP against any content owner that encodes or directs to be encoded DTCP consistent with the DTCP Encoding Rules. That IP Statement is attached at Tab E.

Evaluation Fee	\$10,000	N/A	N/A	N/A
Adopter-Small	\$14,000	.06	.06	.07
Adopter-Large	\$18,000	.05	.05	.06
Shipping and Handling - \$200.00 / order				

**Table 1. Adopter Administrative Fees**

DTLA established these fees based on principles of cost recovery, thereby to help ensure long-term funding for necessary licensing administration and cryptographic key generation facilities.<sup>4</sup>

As noted above, DTLA has stated that it would use commercially reasonable efforts to reduce administrative and per certificate fees to Adopters and would limit increases in administrative fees to Content Participants commensurate with any increases in expenses. The above-referenced fees have been in place for Adopters since 1999, and have been in place for Content Participants since 2001, and have not been increased.

**B. Reasonable and Nondiscriminatory Licensing**

All agreements have been offered by DTLA to any potential Adopter (including Resellers and System Operators) or Content Participant on a nondiscriminatory basis. Similarly, DTLA has extended the IP Statement to all content owners on a nondiscriminatory basis. The Adopter Agreement has been made available by DTLA to any Adopter on a nondiscriminatory basis since first it was offered in 1998, and in revised versions dated October 1999 and July 2001. The current versions of the Content Participant Agreement and the IP Statement have been made available since July 2001. The Adopter Agreement, Content Participant Agreement and IP

---

<sup>4</sup> DTLA does not impose administrative fees for either the Reseller Agreement or the System Operator Agreement, inasmuch as these entities require no ordinary administration resources from DTLA aside from the execution of the Agreement itself, and their activities do not alter the Licensed Component that is subject to the Compliance and Robustness Rules imposed upon the Adopter that provides such Licensed Component to the Reseller or System Operator.

Statement have been and continue to be freely available to the public for download from the DTLA website at <http://www.dtcp.com>

The terms of these agreements are reasonable. In this connection, DTLA notes that the terms and conditions of its agreements were reviewed by the Federal Communications Commission in connection with DTLA's request for certification of DTCP as an authorized digital output protection technology for use with Marked and Unscreened Content in the "Broadcast Flag" proceeding, pursuant to regulations that required reasonable and nondiscriminatory licensing practices, and that DTLA's request for certification was granted.

**C. Compliance and Robustness Rules**

The DTCP Adopter Agreement includes Compliance Rules, which incorporate the DTCP Robustness Rules.<sup>5</sup> DTLA submits that its Compliance Rules and Robustness Rules are consistent in all material respects with the Compliance Rules and Robustness Rules set forth in the DFAST Technology License Agreement.

The DTCP Compliance Rules set forth in Exhibit B to the Adopter Agreement consist of three parts: an Introduction applicable to all DTCP Licensed Products; Part 1, which sets forth the additional Compliance Rules specifically applicable to devices that have "Sink Functions," *i.e.*, the function of receiving content protected with DTCP; and, Part 2, which sets forth the additional Compliance Rules specifically applicable to devices that have "Source Functions," *i.e.*, the function of transmitting content in protected form using DTCP. Devices that have both Sink and Source Functions must comply with all three parts of the Compliance Rules.

---

<sup>5</sup> See Adopter Agreement § 1.6.

The DTCP Robustness Rules are set forth in Exhibit C to the Adopter Agreement. Exhibit C also includes at Exhibit C-1 a Robustness Checklist that restates many of the obligations of the Robustness Rules as a series of questions, for ease of use by engineers. It is an optional aid to Adopters in ensuring compliance with the Robustness Rules; the Checklist does not impose any additional or independent obligations on Adopters.

**D. Enforcement Provisions**

DTLA does not require certification testing for implementations of DTCP. Section 10.3 of the Adopter Agreement gives DTLA the right to request reasonable cooperation from Adopter in obtaining examples of Adopter products that incorporate DTCP and, under nondisclosure agreement, a service manual for the product. This provision was intended to promote resolution of questions concerning compliance or robustness.

**E. Approval Procedures for Downstream Technologies and Recording Methods**

DTLA created DTCP for the purpose of providing an interoperable platform for devices that transmit, receive and record protected digital content. With such interoperability in mind, DTLA provides in its licensing agreements for the use of digital output and recording protection technologies that may currently be identified by DTLA or may be approved by DTLA in the future.<sup>6</sup> DTCP has approved several technologies to output and store data that has been protected using DTCP, specifically:

- digital output protection technologies such as HDCP for the DVI and HDMI interfaces, and

---

<sup>6</sup> See Adopter Agreement, Exhibit B Part 1: Compliance Rules for Sink Functions, §§ 2.2.1 and 4.4. See also Content Participant Agreement § 3.7(a) and (b).

- recording protection technologies such as D-VHS for Digital VHS tape recorders; CPRM for DVD-R, DVD-RW and DVD-RAM recorders as well as SDcard flash memory cards; VCPS for +R and +RW recorders; CPS for BD-RE for Blu-Ray Disc recorders; and MG-R(SVR) for Memory Stick PRO / Hi-MD.

An additional request for technology approval currently is under review.

DTCP protects one transmission “link” in the chain of use and distribution in the home and personal network, and it is axiomatic that any chain is only as strong as its weakest link. Therefore, DTLA considers it essential that DTCP “hand off” content that has been protected with DTCP only to other technologies that provide protection at least as effective as DTCP. For that reason, the criteria used by DTLA to evaluate and approve downstream protection systems mirror the protective elements of the DTLA technology and license, particularly with respect to the provisions of Compliance Rules, Robustness Rules, and enforcement capabilities that are at least as stringent as those set forth in the DTCP license agreements.

The criteria by which DTLA evaluates requests for approval of digital transmission and recording protection methods are set forth in the document submitted herewith as Tab F, “Statement of DTLA Criteria for Reviewing Recording and Retransmission Protection Technologies.” attached at Tab \_\_. DTLA provides this document to any technology proprietor that requests approval of its technology by DTLA as an authorized digital output or digital recording protection technology. The proponent provides DTLA with non-confidential technical information concerning the operation of the technology, and the applicable licensing terms, sufficient to enable DTLA to evaluate whether the criteria have been satisfied. DTLA will accommodate requests by proponents to make presentations to DTLA, in person or telephonically, and may engage the proponent in follow-up correspondence so as to clarify the

proposal or obtain additional information necessary for an informed decision.

A determination by DTLA to approve a particular transmission or recording protection technology is a “DTLA Proposed Action” that is subject to change management review by Content Participants. Pursuant to paragraph 3.7 of the Content Participant Agreement, Content Participants may file a written objection to such approval within 15 business days of notification by DTLA, based on specific evidence that such approval will have a material and adverse impact on the integrity or security of DTCP, the operation of DTCP with respect to protection of content from unauthorized transmission, interception or copying, or the rights of Content Participants with respect to DTCP. Any such objections are to be resolved by arbitration before an independent arbitrator or panel from the American Arbitration Association.

DTLA has received several requests for approval from proponents of other protection technologies for digital transmissions and recording. DTLA has approved HDCP as an authorized digital output protection technology. DTLA has approved as digital recording protection technologies D-VHS for the DVHS digital tape recorder, CPRM for certain DVD recorders as well as SDcard flash memory cards, CPS for BD-RE for Blu-ray recorders, VCPS for +RW/+R recorders, and MG-R(SVR) for Memory Stick PRO and Hi-MD. Other recently-received requests currently are under consideration by DTLA. To date, DTLA has not refused a request for approval from any technology proponent.

**F. Change Provisions**

The DTCP Adopter Agreement permits limited changes to be made to the DTCP Specification in consultation with Adopters and, as required by the Content Participant Agreement, in consultation also with Content Participants. The relevant provisions are set forth

at section 3.3 of the Adopter Agreement and at section 3.7 of the Content Participant Agreement.

The essential elements of these provisions are summarized below:

1. DTLA will not make material changes to the Specification for DTCP, provided that DTLA may make limited changes to enable DTCP to be used over additional interfaces.
2. DTLA reserves the right to correct omissions or errors to the Specification, or to make changes that would clarify, but not materially amend, alter or expand the Specification.
3. Content Participants possess specified “change management” rights with respect to certain proposed amendments to the DTCP Specification and the terms of the DTCP Adopter and Content Participant Agreements. A Content Participant will receive advance notice of a DTLA Proposed Action, as defined in section 3.7 of the Content Participant Agreement, and will have 15 business days in which to file a written objection to such action setting forth specific reasons why such Content Participant believes the action will have a material and adverse effect on the integrity or security of DTCP, the operation of DTCP with respect to protection of content from unauthorized transmission, interception or copying, or the rights of Content Participants with respect to DTCP. Any objections are to be resolved by arbitration before an independent arbitrator or panel from the American Arbitration Association. Certain proposed actions, such as the mapping of DTCP to particular interfaces used on a home and personal network, have been deemed by the parties in advance to not be material or adverse.
4. Adopters participate in a Content Protection Implementers Forum (“CPIF”), and are provided with 30 days’ advance notice and opportunity to comment on proposed changes to the Specification and to the Compliance Rules. From time to time, DTLA may convene meetings of the CPIF to discuss proposed changes and permit open discussion among CPIF members and DTLA.

5. Adopters are required to implement any mandatory changes to the Specification within 18 months after notice that a proposed change has been adopted as final by DTLA.
6. Changes to the Compliance Rules become effective within 12 months of adoption.
7. Voluntary changes that add new features not previously addressed in the Specification (*e.g.*, the adoption of a new Specification adapting DTCP to an additional interface) or the Compliance Rules (*e.g.*, permitting a “move” of Copy One Generation content stored on a PVR to a different recordable medium) become effective upon adoption.
8. Changes to procedures for ordering DTCP certificates and cryptographic keys may be made upon 30 days’ prior written notice.
9. Changes to the Administration Fee or Per Certificate Fee for Adopters may be made upon 30 days’ prior notice; such changes to the Administration Fee will become effective beginning on the next Annual Payment Date for that Adopter. Notwithstanding, DTLA has committed in section 2.1 of the Adopter Agreement, that, where device key or per Adopter costs decrease, DTLA will take commercially reasonable efforts to reduce its fees. Similarly, under section 4.1 of the Content Participant Agreement, changes to the Administration Fee for Content Participants may be made annually upon 30 days’ prior notice, with any increases in fees to be commensurate with any increase in DTLA’s costs.<sup>7</sup>

**G. IPR Arrangements**

The Adopter Agreement and Content Participant Agreement follow an approach, commonly employed in licenses for digital video content protection technology, that narrowly

---

<sup>7</sup> DTLA has not increased its fees under either the Adopter Agreement, the first of which was executed in 1999, or the Content Participant Agreement, the first of which was executed in 2001.

defines the scope of “necessary” patent claims being licensed for the purpose of implementing the technical specification of that particular protection technology,<sup>8</sup> and requires in return that the licensee agree not to assert any of its “necessary” patent claims, within that scope, against any other licensee (here, the Adopters that implement the DTCP technology and the Content Participants that invoke its use). The owners of many technologies – and their scores of licensees – have deemed this approach an appropriate one for digital video copy protection and related technologies.<sup>9</sup>

DTLA elected to use this predominant model for content protection technology licenses because it is sensible and pro-competitive. Manufacturers compete based on product features, not content protection technologies. Content protection technologies are simply necessary infrastructure in the digital market-place, which can benefit consumers by providing incentives for release of digital content, but content protection technologies are not themselves digital product offerings for which consumers will pay higher prices. DTLA is not therefore charging the type of commercial royalty rates that the 5C Companies typically would charge for their intellectual property, but instead are offering DTCP with an eye to cost recovery. Thus,

---

<sup>8</sup> “Necessary Claims” in the DTCP agreements, in brief, are limited to those patent claims owned or controlled by the 5C Companies that must be infringed to make a product that complies with the protocols and cryptographic algorithms, packet formats and data structures disclosed in the DTCP Specification. The license grant further extends to all copyright and trade secret rights owned or controlled by the 5C Companies embodied in the Specification for DTCP. *See* Adopter Agreement §§ 1.22 and 5.2; Content Participant Agreement, definition of “Necessary Claims” at 7, and § 2.1.

<sup>9</sup> For example, licenses for CSS (for DVD video discs), CPPM (for prerecorded DVD audio discs), CPRM (for certain recordable DVD discs and for content stored on SD memory cards), HDCP (for the DVI and HDMI interfaces) and CPS for Blu-Ray RE (for recordable high capacity digital video discs), and the HDMI format, all utilize this same necessary claims/reciprocal covenants licensing model.

consumers and all licensees benefit from the lower costs enabled by the license model, including the reciprocal covenants. Nothing in the DTCP license prevents any Adopter or Content Participant from licensing its patents on whatever terms it wishes in connection with any technology developed by that licensee (including in a competing content protection technology), or has any other impact outside the scope of the “necessary claims” specifically associated with implementing DTCP.

DTLA is not a patent pool. The agreements address indemnification with respect to infringement of intellectual property rights of third parties in Section 9.2 of the Adopter Agreement, and Section 10.1 of the Content Participant Agreement. Limitations on liability of DTLA to Adopter or Content Participant are set forth in Section 9.3 of the Adopter Agreement and Section 10.2 of the Content Participant Agreement.

**H. Warranty Provisions**

The agreements provide disclaimers of warranties in Section 9.2 of the Adopter Agreement, and Section 10.1 of the Content Participant Agreement. Limitations on liability of DTLA to Adopter or Content Participant are set forth in Section 9.3 of the Adopter Agreement and Section 10.2 of the Content Participant Agreement.

**I. Term**

The term of the Adopter Agreement is 10 years, subject to the provisions of Section 8 thereof. Terms and conditions relating to the term of the Content Participant Agreement are set forth in Section 8 thereof.

**J. Patent List**

DTLA does not provide a list of known essential patents. First, a patent disclosure is not necessary or appropriate for a license to a Specification that implicates rights based on patent,

trade secret and copyright. Second, patent disclosure is unnecessary in a license agreement that relies upon the “Necessary Claims” formulation. The DTCP license approach assures Adopters and Content Participants that they have obtained all rights possessed by DTLA and the Founders in Necessary Claims. This approach avoids concerns from licensees that the list may be under-inclusive or, conversely, concerns on behalf of the DTLA Founders that the list may be over-inclusive (i.e., may include non-essential patents). Third, requiring disclosure of patents creates unnecessary expenses, such as hiring outside counsel to perform independent evaluations of “essentiality,” which expenses would have to be compensated by increased administrative fees.

**K. Revocation**

DTLA has specified the circumstances under which revocation may be imposed, namely, where (a) a Device Key and corresponding Device Certificate have been cloned such that the same key and certificate are found in more than one device or product; (b) a Device Key and/or Device Certificate have been lost, stolen, intercepted, misdirected or made public or disclosed; or (c) revocation is required by court order or other government authority. *See* Adopter Agreement § 4.2. Revocation cannot be ordered for any other noncompliance with or breach of an Adopter Agreement. *Id.* Moreover, revocation for reasons described in clauses (a) and (b) can only occur with the consent of the affected Adopter or pursuant to a determination in an independent arbitration, in accordance with detailed processes with procedural safeguards set forth in the Adopter Agreement, Procedural Appendix § 14, and Content Participant Agreement § 6. Notwithstanding, as a further safeguard, DTLA designed its system such that a revocation that proved to be erroneous could be reversed by issuance of an updated SRM. DTLA notes that, to date, no revocations have been either requested or performed.

**L. Applicable Encoding Rules**

The DTLA Content Participant Agreement, at Sections 5.1(a), (b), (d) and (e) and 5.3, sets forth the applicable encoding rules for the use of DTCP. These rules also are set forth in the IP Statement.

## **II. TECHNICAL DESCRIPTION OF DTCP AND DTCP-IP**

The following sections describe the general technical characteristics of DTCP and specific and supplemental protection elements of DTCP-IP, in accordance with the numbered Sections of the CableLabs Submission document.

### **A. Section 3.2 -- Security Overview**

The Digital Transmission Content Protection Specification defines a cryptographic protocol for protecting audio/video entertainment content from unauthorized copying, intercepting, and tampering as it traverses digital interconnects. Only legitimate entertainment content delivered to a source device via another approved copy protection system (such as a conditional access System) will be protected by this copy protection system.

The operation of DTCP is set forth fully in the Specifications for use of DTCP over the various transports to which DTCP has been mapped. DTCP Volume 1.(V1), DTCP Volume 2 and DTCP Volume 1 Supplement E (V1SE) "Mapping DTCP to Internet Protocol" (IP) together describe DTCP-IP implementation. General DTCP protections are detailed in DTCP V1 whereas DTCP V1SE contains modification/additions to DTCP V1 that are necessary to map DTCP to IP. Informational versions of these Specifications for DTCP (which exclude only those aspects that reflect confidential and trade secret information) are available from the DTLA website, <http://www.dtcp.com>.

In overview, the DTCP system addresses four fundamental layers of content protection:

- **Authentication and Key Exchange**
- **Content Encryption**
- **Copy Control Information**
- **System Renewability**

## 1. Authentication and Key Exchange (AKE)

Before sharing protected information, a connected device must first authenticate the other connected device; that is, that each device indicates its implementation of and compliance with DTCP. The authentication process occurs when devices are connected and/or activated along a digital network, and typically completes within a timeframe that is imperceptible to the user. Specification V1 includes two authentication levels: Full Authentication and Restricted Authentication. However, the Specification V1SE mapping for DTCP-IP permits only the use of the Full Authentication procedure. For non-IP mapping, full Authentication can be used with all content protected by the system, but must be used for copy-never content.

Both Full and Restricted Authentication involve the calculation of three types of keys:

- an **authentication key**, established during the authentication process, used to protect the exchange keys
- an **exchange key**, used to set up and protect content streams
- a **content key**, used to encrypt the content being exchanged

DTCP-IP augments the Authenticated Key Exchange (AKE) by including a 7 millisecond Round Trip Time (RTT) check procedure. This procedure is referred to as RTT-AKE in section 8.5 “Additional Localization via RTT” of DTCP V1SE. In addition, the DTCP V1SE requires that the Time To Live datagram packet be set to not more than 3.

## 2. Content Encryption

Following authentication, content is transmitted from a source device to a DTCP-compliant sink along a secure authenticated channel in encrypted form. The content cipher, that is, the algorithm used to encrypt the digital content itself, must be robust enough to protect the content yet efficient enough to implement in either hardware or software in PCs and CE devices.

To ensure interoperability, all devices must support the specific cipher specified as the baseline cipher. The channel cipher subsystem can also support additional optional ciphers, the use of which is negotiated during authentication. All ciphers are used in the converted cipher block chaining mode. Converted cipher block chaining provides greater security than ordinary cipher block chaining.

DTCP-IP requires use of the Advanced Encryption Standard with a 128 bit key length (AES-128) as the baseline cipher, as specified in section 4.20 of DTCP V1SE. AES-128 also is defined as an optional cipher that may be used in addition to the baseline M6 cipher for DTCP over other protocols.

In addition, DTCP-IP requires that WEP, WAP or successor algorithms be utilized for wireless transmissions of content protected by DTCP-IP.

**B. Section 3.3: Video Transport -- Copy Control Information**

DTCP-IP is content agnostic. DTCP-IP provides protection to general HTTP and RTP transports of commercial entertainment content.

Content owners may specify whether and to what extent their content may be duplicated and redistributed, subject to the Encoding Rules described below. The content protection system must therefore support transmission of encrypted data between devices, using **Copy Control Information (“CCI”)**. If source and sink devices have conflicting capabilities, they must follow the most restrictive CCI method(s) available, which is determined by the source device. DTCP is capable of securely communicating copy control information (CCI) between devices in two methods that are defined by the specification:

- The **Encryption Mode Indicator (“EMI”)** provides an easily-accessible yet cryptographically-linked indicator of CCI. EMI is sent in the clear but is

cryptographically bound to the content. The EMI indicates the mode of encryption applied to a stream. DTCP-IP uses the Extended-Encryption Mode Indicator (E-EMI) as specified in section 4.7 of DTCP V1SE. When multiple mechanisms are available, the most restrictive should be used.

- **Embedded CCI** is carried as part of the content stream. Many content formats including MPEG have fields allocated for carrying the CCI associated with the stream. The integrity of embedded CCI is ensured since tampering with the content stream results in erroneous decryption of the content. Only devices capable of processing the content itself can process this form of CCI.

With respect to the values of the CCI settings:

- Content that is never to be copied (*e.g.*, content from prerecorded media with a Copy Generation Management System (“CGMS”) value of 11, such as a DVD Movie) can only be exchanged between devices that have successfully completed full authentication.
- Content that can be copied one-generation (*e.g.*, content with a CGMS value of 10, such as a pay TV program) can be exchanged between devices using either full or restricted authentication.
- For content marked no-more-copies, future exchanges are marked to indicate that a single-generation copy has already been made. This content can be exchanged between devices using either full or restricted authentication.
- Content also may be marked “Encryption Plus Nonassertion” (“EPN”), which applies DTCP protection, so as to protect against unauthorized

redistribution outside of compliant devices along the authenticated network, yet permits the content to be freely copied in a protected form.

In accordance with FCC regulations, digital terrestrial broadcast television content marked with the Broadcast Flag is to be set to EPN.

- Copy Never content other than from prerecorded media may be retained (such as on a PVR) for no less than 90 minutes.
- Copies of content (other than content marked copy never) stored on a non-removable storage medium (*e.g.*, a PVR) can be “moved” to a removable storage medium (*e.g.*, a DVD-R disc or D-VHS cassette tape).
- No authentication or encryption is required to protect a digital terrestrial broadcast transmission that has not been marked with a Broadcast Flag and, so, programming received via such a transmission can be copied and redistributed freely.

Source devices will choose the right encryption mode based on embedded CCI and set the EMI accordingly. Sink devices will choose the right decryption mode by examining the EMI.

If the EMI bits are tampered with, the encryption and decryption modes will not match, resulting in erroneous decryption of the content.

EMI and Embedded CCI are to be encoded by or at the direction of the content owner in accordance with Encoding Rules set forth in the Content Participant Agreement, and in an “IP Statement” that facilitates the use of DTCP by non-Content Participants.

**C. Section 3.4: Content Protection Profiles**

Not applicable to DTCP.

**D. Section 3.5: Key Exchange Algorithms**

In addition to the general description provided in section A above, details regarding authentication, as requested in Section 3.5, are described for DTCP generally in DTCP V1 and for DTCP-IP in V1SE.

**E. Section 3.6: Security Interfaces**

Not applicable to DTCP.

**F. Section 3.7: Security Processing**

Detailed rules describing how the keys and secrets are to be protected during cryptographic calculation, and how CCI, image constraint and other parameters are protected throughout the system are set forth in the Adopter Agreement at Exhibit C, Robustness Rules.

**G. Section 3.8: Certificate Management**

Each DTLA Licensed Product is given a certificate which is signed by the DTLA. The Device Certificate is used during the Authentication and Key Exchange (AKE) procedure to ensure that connected devices can transport commercial entertainment content. Each certificate contains a Device Identifier. Further information is set forth in Section 4 and Section 7 of DTCP V1.

Device Certificates and Device Keys are generated by a Key Generation Facility. DTLA Founders obtain information on a periodic basis concerning the total number of keys generated by the facility, but do not request potentially competitively sensitive information, such as the number of certificates and keys ordered by particular Adopters. Moreover, DTLA does not know what types of devices will use these keys, or what DTCP protocol will be used.

**H. Section 3.9: Revocation/Renewability**

DTLA generates System Renewability Messages (SRM) that contain Certificate

Revocation List which in turn contain Device Identifiers that have been revoked. System renewability ensures the long term integrity of the system and provides the capability for revoking unauthorized devices. The revocation process invalidates the Device Certificate associated with a particular device when the device ID incorporated in such certificate is included in the certificate revocation list in the SRM, and renders such device unable to exchange content with another device via DTCP. More specifically, the DTCP source function during AKE aborts the AKE procedure if a Device Identifier in the certificate received from the sink functions is listed in the CRL. Details regarding SRMs are described in both DTCP V1 and V1SE.

Devices that support full authentication can receive and process System Renewability Messages (“SRMs”). These SRMs are generated by the DTLA and provided to its Content Participants for delivery via content.

SRMs can be delivered to DTCP-enabled sink devices from several sources, including:

- Prerecorded content source devices such as DVD players should be able to update an SRM from prerecorded content media (such as a DVD disc). In addition, prerecorded content should carry a system renewability message current as of the time the content is mastered. Such devices should also be able to update an SRM from another compliant device with a newer SRM.
- Devices such as digital set-top boxes (“STBs”) serving as digital cable receivers or DBS digital broadcast satellite receivers are a real-time delivery source of copyrighted content. They should be able to update an SRM from a content stream or from another compliant device with a newer SRM.

- Devices such as digital televisions are a receiver of copyrighted content. These devices should be able to update an SRM from another compliant device with a newer SRM.

**I. Section 3.10: Points of Attack/Potential Weaknesses**

DTLA knows of no specific points of attack or weaknesses.

**J. Section 3.11: Commercial Use**

DTLA does not collect information from Adopters concerning their commercial uses.

However, DTLA is aware that DTCP has been in commercial use since approximately 1999.

Currently, DTCP is implemented in a broad range of products including cable set top boxes, HD televisions and monitors, DVD recorders, D-VHS recorders and PVRs, as well as semiconductor IC chipsets that implement DTCP. DTCP-IP has been available for use since approximately September 2004. DTLA is aware that products using DTCP-IP such as wireless media adapters and video recorders have been announced or have come to market.

**K. Section 3.12: Contact Information**

For questions concerning technical aspects of DTCP-IP, please contact Michael Andre, michael.andre@intel.com, (503) 712-1211.

For questions concerning licensing or other non-technical aspects of DTCP-IP, please contact Seth Greenstein, sgreenstein@mwe.com, (202) 756-8088.

**Conclusion**

DTCP is a well-established, tested technology that provides effective protection against unauthorized redistribution of commercial audiovisual content. DTCP is used and approved by content owners for protecting all video content, and has been licensed for use by more than 120 companies. DTCP over 1394 has been approved for use in cable set-top boxes pursuant to the DFAST and CHILA license agreements, and DTCP generically (including DTCP-IP) has been

approved for use in the PHILA. DTCP is interoperable with other interface and recording technologies. Licenses are available to Adopters and Content Participants on a reasonable and nondiscriminatory basis, and any content owner may avail itself of the basic protections of DTCP without a license, pursuant to the IP Statement.

DTCP-IP further will promote home networking and flexibility for consumers, by enabling wireless as well as wired networking using the IP protocol. DTCP-IP is a robust implementation of DTCP that builds upon the solid DTCP technology with additional protections to ensure localization of protected content within home and personal networks.

For these reasons, DTLA respectfully submits that DTCP-IP merits approval by CableLabs as an authorized digital output protection technology in the DFAST and CHILA licenses.

Respectfully submitted,

Michael B. Ayers  
President  
Digital Transmission Licensing Administrator, LLC  
michael.ayers@tais.toshiba.com  
(949) 461-4714

Seth D. Greenstein  
Chair, DTLA Policy Committee  
McDermott, Will & Emery  
(202) 756-8088  
sgreenstein@mwe.com

Michael Andre  
Chair, DTLA Technical Working Group  
Intel Corporation  
(503) 712.1211  
michael.andre@intel.com

Attachments:

1. Adopter Agreement
2. Content Participant Agreement
3. DTCP Volume 1 V1.4 (Informational Version)
4. DTCP Volume 1 Supplement E V1.1 (Informational Version)
5. IP Statement

# **EXHIBIT 4**

Motion Picture Association of America, Inc.  
15503 Ventura Boulevard  
Encino, CA 91436

Digital Transmission Licensing Administrator, LLC  
c/o License Management International, LLC  
225B Cochrane Circle  
Morgan Hill, CA 95037

July 11, 2005

Via Electronic Mail and First Class Mail

Jud Cary, Esq.  
Deputy General Counsel  
Cable Television Laboratories, Inc.  
858 Coal Creek Circle  
Louisville, CO 80027-9750

Dear Jud:

With respect to CableLabs' consideration of the Request by DTLA for Approval of DTCP-IP as a New Digital Output Protection Technology, and with reference to the May 27, 2005, letter from MPAA to Jud Cary of CableLabs, the MPAA and DTLA wish to provide the following clarifications and supplementary comments.

1. MPAA supports the DTLA's Request for Approval, and urges CableLabs promptly to approve DTCP-IP as an authorized digital output protection technology. Implementation of DTCP-IP will promote localized networking for the home and personal environment, which will mutually benefit cable subscribers and content owners. We therefore ask CableLabs to complete its approval of DTCP-IP at the earliest possible time.
2. DTLA supports the MPAA proposal asking CableLabs to promptly provide a means for signaling the EPN state in DTCP. The EPN state provides greater flexibility to content owners and consumers for enjoyment of cable-delivered non-broadcast digital basic tier programming services, which both DTLA and MPAA consider to be extremely important. The ability to signal EPN also will be essential to the proper implementation and operation of DTCP with respect to broadcast digital basic tier programming as regulations pertaining to the "Broadcast Flag" come into force in the United States.
3. With respect to points 2 and 3 in the May 27 MPAA letter, DTLA has informed MPAA that DTLA continues to make progress in its efforts to establish additional localization techniques for the protocols supported by DTCP, pursuant to the DTLA "Work Plan for

Localizing Transmissions.” MPAA and DTLA look forward to working with CableLabs so that localization means for IEEE 1394, and other protocols to which DTCP has been or will be mapped, can be applied to future devices manufactured pursuant to DFAST, PHILA and CHILA licenses. Furthermore, MPAA supports CableLabs’ approval of other “localized” forms of DTCP.

4. With respect to point 4 in the May 27 MPAA letter, DTLA has clarified that the current Compliance and Robustness Rules applicable to the “Move” function in the DTCP Adopter Agreement also apply to any Move function permitted via DTCP-IP. With such understanding, MPAA believes that DTLA has addressed point 4 of our letter. DTLA further has explained that, to the extent practicable, DTLA is continuing work on defining a more uniform protocol for performing the Move function over DTCP-IP, so as to promote greater device interoperability.

5. DTLA has clarified, and MPAA agrees, that the format and procedure for facilitating the delivery of SRMs over cable systems should be established by CableLabs and the cable systems themselves. DTLA concurs with MPAA that the revocation of lost, stolen, or cloned DTCP device certificates enabled by delivery of SRMs remains an important element of the security provided to content owners by DTCP. DTLA and MPAA therefore urge CableLabs to develop an OpenCable specification and to promote the implementation of the specification necessary to ensure delivery of SRMs via cable systems. DTLA would be pleased to provide CableLabs upon request with information that could assist in this endeavor.

Thank you in advance for your efforts to help facilitate the implementation by CableLabs’ licensees of the protections and benefits offered by DTCP. We look forward to your prompt approval of DTCP-IP, and to working cooperatively with you to address the issues discussed in the MPAA May 27 letter.

Very truly yours,

Brad Hunt  
Sr. VP, Chief Technology Officer  
Motion Picture Association of America, Inc.

Michael Ayers  
President  
Digital Transmission Licensing Administrator, LLC

# **EXHIBIT 5**





1. The PCI Express Interconnect Bus Should Be Considered a “User Accessible Bus” and The Interface Between Discrete Decryption Engines and Discrete Video Decoders Must Be Protected.

The Computer Companies claim that it would be difficult for one to access cable content on the PCI Express interconnect bus. However, they do not assert that it is an unachievable task given sufficient development time and resources. Specifically, the Computer Companies have not claimed, and cannot claim, that it would be impossible to manufacture a tool to gain access to Controlled Content that travels in the clear over a PCI Express interconnect bus. Indeed, one could imagine a PCI Express Card, developed and sold legitimately as a PCI Express bus analyzer. This card could be used in combination with a downloaded software application to easily access in-the-clear Controlled Content moving across the PCI Express bus. The possibility that such a tool could be developed to access Controlled Content supports CableLabs’ position that the PCI Express is a “user accessible bus.”

There is an additional harm to content providers if Controlled Content is not protected while moving across the PCI Express bus. If, as suggested by the Computer Companies, there were no such protection applied to Controlled Content moving over this bus, then one could argue that there is no “technological measure” being applied as defined under the Digital Millennium Copyright Act, 17 U.S.C. §§ 1201-1205 (2005) (the “DMCA”) and that the DMCA protections would be unavailable. *See* 17 U.S.C. §1201. Therefore, the MPAA believes that the DCAS license agreement should not be amended to eliminate the categorization of the PCI Express interconnect bus as a user-accessible bus.

Likewise, Controlled Content traveling across a PCI Express bus between a discrete DCAS decryption engine and a discrete video decoder residing in the software player application must be encrypted, or otherwise protected,<sup>1</sup> from being accessed in the clear. Without such a “technological measure,” content providers may be deprived of the protections afforded under the DMCA. While the MPAA supports enabling general-purpose computers as secure, cable navigation devices through their incorporation of the DCAS technology, the MPAA disagrees with the Computer Companies’ position to eliminate the current DCAS license requirement that the interface between discrete decryption engines and discrete video decoders be encrypted.

2. An Effective Downloadable Conditional Access System Must Have a Hardware Root of Trust.

DCAS can only operate effectively in the form of authenticated software loaded and executed within a DCAS Secure Microprocessor Chip since the system relies upon a hardware “root of trust” within the specialized microprocessor Chip. DCAS cannot provide the same level of security if it were to be implemented in the form of a software application that was downloaded and executed on a general purpose computer, as suggested in the comments filed by Dell, H-P, Intel and Sony Electronics, Inc. In fact, if DCAS were implemented as a downloadable software application with a software “root of trust,” it would greatly expose the security of the system to software attacks, which could be developed and easily distributed over the Internet.

---

<sup>1</sup> Although encryption is well-recognized as a secure means of protecting a stream of Controlled Content, the MPAA and its member companies would be amenable to discussing other effective technological measures to protect Controlled Content.

The MPAA restates its support of the goal of Dell, H-P, Intel and Sony Electronics, Inc. in enabling the general purpose computer as a cable navigation platform to enhance the competitive marketplace for navigation devices. However, the MPAA does not see the need to eliminate the security afforded by the DCAS Secure Microprocessor and its hardware “root of trust” as necessary to achieve this goal.

3. DCAS Should Support Secure Home Networking of Cable-Delivered Content.

The MPAA has supported technological innovations that enable secure home networking because they provide benefits to both cable subscribers and content providers. In that vein, the MPAA supports the position reflected in the comments filed by Dell, H-P, Intel and Sony Electronics, Inc. that DCAS should recognize and support secure home networking.

To this end, the MPAA has worked with CableLabs to gain its support for additional protection technologies to enable secure home networking of cable-delivered content. For example, on July 11, 2005, the MPAA filed a joint letter of support with the Digital Transmission Licensing Administrator, LLC (“DTLA”) to CableLabs to support the approval of DTCP over IP as an authorized digital output protection technology. This was done in conjunction with gaining CableLabs’ support for implementing a Redistribution Control Trigger (“RCT”) bit that would signal when redistribution control is asserted over Controlled Content where no numeric copy control is being asserted. Since the RCT bit was implemented in the DCAS License, the MPAA and its member companies support the approval of DTCP over IP as an authorized output technology under the DCAS License.

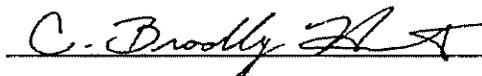
## CONCLUSION

The MPAA supports the development of the DCAS technology and its implementation in a wide range of cable navigation platforms, including general-purpose computers. However, the MPAA does not see the logic or the need to lower the security requirements for computer-based platforms in order for them to successfully compete in the navigation device marketplace. The MPAA also supports secure home networking of cable-delivered content and strongly urges CableLabs to amend the DCAS License to support the approval of DTCP over IP as an authorized digital output protection technology.

Respectfully submitted,

THE MOTION PICTURE ASSOCIATION OF AMERICA, INC.

By:



C. Bradley Hunt  
Executive Vice President and  
Chief Technology Officer  
Motion Picture Association of America, Inc.  
15503 Ventura Boulevard  
Encino, California 91436  
(818) 995-6600

# **EXHIBIT 6**

**CableLabs®**

Cable Television Laboratories, Inc.

March 5, 2006

Mr. Seth D. Greenstein  
CONSTANTINE | CANNON, P.C.  
1627 Eye Street, N.W.  
Washington, D.C. 20006

**Re: Approval of DTCP-IP under DFAST License, for UDCP Products**

Dear Seth:

CableLabs is prepared to grant provisional approval to DTCP-IP for receipt of Cable Content from UDCPs. As with the previously approved Content Protection systems for use over IP digital outputs (e.g., Windows Media DRM), Cable Content may be mapped to DTCP-IP over the DRI interface, and into Licensed Cable Products downstream from the DRI interface subject to certain conditions. An Exhibit to be included with the DTCP Adopters Agreement would require that Licensed Cable Products provide for detection and correct response to copy control and content protection information so that it is correctly mapped from the cable network to the DTCP content protection system; assure that the license obligations applicable to use of the DFAST Technology are satisfied by the Licensed Cable Product and downstream devices which receive Cable Content via DTCP; meet the compliance and robustness rules applicable to Cable Content, and be subject to an adopters compliance letter setting forth effective remedies and enforcement means for breaches. A separate letter from DTLA would provide assurances that the DTCP change process would not be used to reduce the security for Cable Content and will be used to remain at a substantially equivalent level of robustness and compliance in comparison to the DFAST agreement to which DTCP would be added.

The provisional approval shall be effective, and the ability to use DTCP-IP for receipt of Cable Content is dependent, upon DTLA promulgating a document specifying the applicable rights mapping requirements for Cable Content being converted from DFAST protection to DTCP-IP, and providing adequate assurances that Licensed Cable Products that receive such Cable Content can satisfy the license requirements applicable to Licensed Cable Products licensed to use the DFAST Technology and can meet the requirements comparable to those which are applicable to previously approved IP digital outputs. The provisional nature of this approval is convertible to full approval upon the satisfaction of these commitments no later than June 30, 2006.

With respect to your email of 2 March, our requirement to address both content protection and transport are clearly set forth in our guidelines. We do not require a new transport to be invented; existing transports can be specified so long as they meet our criteria to display cable content. And, in fact, we note that DTLA appears to also require a transport to be approved (see e.g., DTCP on USB-IP).

---

858 Coal Creek Circle  
Louisville, Colorado 80027-9750  
Phone: 303.661.9100  
Fax: 303.661.9199  
<http://www.cablelabs.com>

**CableLabs®**

Cable Television Laboratories, Inc.

With respect to the DRI specification itself, it is a public specification. Any and all 5C members are invited to comment on the specification, with or without a Contribution Agreement or NDA in place. We have been proceeding under the assumption that Michael Andre has been representing DTLA. That said, we have also had input from Sony. No 5C company has been denied any avenue of input. If any 5C company has any comments, please let us know.

If you would like to arrange a call to discuss this provisional approval, the licensing, and other arrangements, please contact me. We would also like to continue to work on approval of DTCP-IP for use on OCUR type devices under the CHILA/OpenCable agreement.

Sincerely,



Michael E. Davis  
Project Director  
OpenCable Business Relations

---

858 Coal Creek Circle  
Louisville, Colorado 80027-9750  
Phone: 303.661.9100  
Fax: 303.661.9199  
<http://www.cablelabs.com>

## Exhibit to DTCP Adopters Agreement

March 2, 2006

*DTCP Adopters Agreement shall be amended by terms and a supplement that shall apply these additional terms and conditions to Licensed Products that are designed for the transmission and/or receipt of digital transmissions comprising Cable Content from UDCP type products.*

### **EXHIBIT X, PART 1: RULES FOR LICENSED CABLE PRODUCTS**

#### **1. INTRODUCTION**

- 1.1. Applicability. This Part 1 of this Exhibit X is applicable to Licensed Cable Products. Licensed Products that do *not* receive Cable Content are not required to implement these additional requirements.
- 1.2. Proper use of the DRI includes both technical and licensing aspects, to ensure that the overall system robustly maintains the security of Cable Content protected by DTCP after it is passed from the DRI.
- 1.3. Licensed Cable Products employing the DRI shall not compromise or interfere with the integrity and security of Cable Content.
- 1.4. The DRI interface addresses certain transport and service issues specific to Cable Content and its presentation. These rules detail the requirements for receiving and maintaining the security of Cable Content from the DRI, and protected by DTCP.
- 1.5. This Exhibit requires that Licensed Cable Products
  - 1.5.1. provide for detection and correct response to copy control and content protection information such that it is correctly mapped from the cable network to the DTCP content protection system;
  - 1.5.2. assure that the license obligations applicable to use of the DFAST Technology are satisfied by the Licensed Cable Product and downstream devices which receive Cable Content via DTCP; and
  - 1.5.3. meet the compliance and robustness rules applicable to Cable Content and be subject to a compliance letter setting forth effective remedies and enforcement means for breaches.

#### **2. DEFINITIONS**

- 2.1. "Cable Content" means unidirectional cable content that has been transmitted from a cable headend or otherwise over the cable system to a unidirectional digital cable product (UDCP) licensed to use DFAST Technology, and through the DRI. Once marked Cable Content, such content shall remain Cable Content, and be treated as such, in Licensed Cable Products, and all downstream devices.
- 2.2. "Cable Operator" means any cable operator that CableLabs identifies on its <www.cablelabs.com> website as a member and any other cable operator that provides CableCARDS to customers in connection with the provision of cable services in North America.

- 2.3. "Content Protection System" means the DTCP content protection system used with the DRI.
- 2.4. "Licensed Cable Product" means a product, including a hardware Licensed Cable Product or software application, which is a Licensed Product and is designed for the transmission and/or receipt of digital transmissions comprising Cable Content.
- 2.5. "DRI" means the Digital Receiver Interface output specification [OC-SP-DRI-I02-060210], and subsequent versions thereof approved for output from products using DFAST Technology.
- 2.6. DFAST Technology means the patents and licensed know-how licensed under the DFAST Technology License Agreement for Unidirectional Digital Cable Products.

### **3. Mapping and Rights**

- 3.1. Licensed Cable Products **MUST** adhere to the mapping requirements identified in Exhibit A and provide for detection and correct response to copy control and content protection information, as defined in Exhibit A;
- 3.2. Licensed Cable Products **MAY**
  - 3.2.1. Stream Cable Content to networked Licensed Cable Products for display (but not for storage) in both HD and SD.
  - 3.2.2. Move SD Cable Content to another Licensed Cable Product compliant with this Exhibit, pursuant to and in accordance with Section 3 of Part 1 and Section 3 of Part 2 of Exhibit B.
  - 3.2.3. Securely move Copy Freely SD Cable Content to a portable Licensed Cable Product otherwise compliant with this Exhibit, where such portable Licensed Cable Product is subject to the proximity limits when obtaining Cable Content.
  - 3.2.4. Burn Copy Freely Cable Content to a DVD in both SD and HD.
  - 3.2.5. Map, store or record, Cable Content to approved outputs under the DFAST Agreement or via DRI to other Licensed Cable Products, so long as such mapping is conformant to this Exhibit and Exhibit A.
  - 3.2.6. All other use of Cable Content is prohibited unless and until this Exhibit is amended with the written consent of Cable Television Laboratories, Inc.
- 3.3. Cable Content **MUST** be marked as "Cable Content" by the Content Protection System, and maintain such marking from the DRI to the Licensed Cable Product and to any downstream Licensed Cable Products.
- 3.4. Licensed Cable Products **MUST** implement the proximity control mechanism of DTCP [confirm ref in DCTP, or need to specify] to limit all Cable Content to the home network.
- 3.5. Licensed Cable Products **SHALL** prohibit the output of Cable Content through a VGA interface in accordance with a schedule to be mutually agreed upon by the consumer electronics, information technology, and content industries

### **4. License Requirements**

- 4.1. Licensed Cable Products must assure that the license obligations applicable to use of the DFAST Technology are satisfied by the Licensed Cable Product which receives Cable Content via DRI and by all downstream Licensed Cable Products which receive such Cable Content via DTCP. These supplemental requirements are required only for Cable

Content accessed from the DRI, or Cable Content that is passed to other Licensed Cable Products downstream.

- 4.2. Specifications -- Licensed Cable Products that access Cable Content via the DRI using a DTCP protection method MUST be compliant with the DRI Specification and with this Exhibit.
- 4.3. MMI -- Licensed Cable Product SHALL ensure that MMI resources will be rendered on network connected displays in an equivalent manner as provided in OpenCable Host Licensed Cable Product 2.0 Specification (OC-SP-HOST2.0-CFR-I06-050708) and successor versions. [details to follow]
- 4.4. EAS -- Licensed Cable Product SHALL respond to emergency alerts that are transmitted in compliance with ANSI/SCTE 54 2003 (formerly DVS 241): “Digital Video Service Multiplex and Transport System Standard for Cable Television” (incorporated by reference, see § 15.38) and ensure that live EAS will be rendered on network connected displays in an equivalent manner as provided in OpenCable Host Licensed Cable Product 2.0 Specification (OC-SP-HOST2.0-CFR-I06-050708) and successor versions. [details to follow].
- 4.5. Channel Mapping, Closed Captioning, Content Advisory, and Language Identification – Similar to sections 4.2.1 and 4.2.2, channel mapping, closed captioning, content advisory/V-Chip, and language identification need to be addressed in an equivalent manner as provided in OpenCable Host Licensed Cable Product 2.0 Specification (OC-SP-HOST2.0-CFR-I06-050708) and successor versions. [details to follow]]
- 4.6. Licensed Cable Product MUST implement the latest versions (2.0 or later) of UPnP QoS Policy Holder Service, UPnP QoS Manager Service and UPnP QoS Device Service for QoS management of both live and recorded content.
- 4.7. Diagnostics and User Presentation
  - 4.7.1. At setup, Licensed Cable Product MUST employ a network performance test, and inform the user if issues are detected that will impede the delivery of Cable Content to the network Licensed Cable Product. See below for details.
  - 4.7.2. If the home network QoS is insufficient to deliver the Cable Content as intended, the Licensed Cable Product SHALL notify the user of such conditions and the network Licensed Cable Product shall employ transcoding, transrating, or equivalent stream optimization to meter the streamed Cable Content to the available QoS on the home network. The user shall have the option to 1) continue automatically optimizing the stream, or not, and 2) specify whether this notification is always displayed when stream optimization is being employed.
  - 4.7.3. Licensed Cable Product SHALL provide a user-accessible diagnostic screen that enables the user to monitor the network performance and its suitability for streaming Cable Content to the network Licensed Cable Product.
  - 4.7.4. Licensed Cable Product MUST be able to measure dropped packet rate for content being transmitted over DRI [[will provide details later]]
  - 4.7.5. Licensed Cable Product MUST be able to detect if the dropped packet rate exceeds a specified threshold [[see DRI spec, and we will provide details later]]
  - 4.7.6. Licensed Cable Product MUST be able to present options to the user if the threshold is exceeded, and execute the specified action. Guidelines for presentation as specified by CableLabs in the DRI Specification (stop

transmission, continue transmission, re-encode, etc.) [[see DRI spec, and we will provide details later, e.g., on threshold, guidelines for presentation, etc.]]

- 4.7.7. Licensed Cable Product MUST be able to present information to the user on the cause of the degradation. The device MUST use both packet loss and network FEC overflow in determining user feedback messages. The following messages MUST be implemented and displayed. [*exact language subject to approval*]
- No FEC overflow, packet loss threshold overflow: “*Your home network has insufficient bandwidth to display this video without errors.*”
  - FEC overflow, packet loss under threshold: “*The signal strength from your cable connection has been compromised. Please check the cable input connections to the main receiving device*”
  - FEC overflow, packet loss threshold overflow: “*Your home network has insufficient bandwidth to display this video without additional errors and the signal strength from your cable connection to the main receiving device may be insufficient.*”
- 4.8. DRI Connections to Licensed Cable Product and downstream networked Licensed Cable Products
- 4.8.1. Licensed Cable Product, and any downstream network Licensed Cable Products, SHALL employ technical measures, such as network monitoring, video packet prioritization, and user notification of network congestion, to promote a quality user experience when viewing streamed Cable Content.
- 4.8.2. Licensed Cable Product, and any downstream network devices, shall be capable of receiving, error resilient under a bit error rate of  $10^{-6}$ , a single stream (up to 38.8 Mbps). Regardless, downstream devices must measure packet loss and report errors to the user when they exceed a defined threshold. The user may then elect to continue playing the content with errors. (Defined above).
- 4.8.3. Licensed Cable Products, and any downstream network Licensed Cable Products that comply with this Exhibit, may connect via DRI to the following transports:
- 4.8.3.1 Licensed Cable Products that connect via WiFi SHALL comply with WiFi Multimedia QoS (referred to as “WMM”), which provides prioritized QoS capabilities, and shall support both 802.11 A & G or better.
  - 4.8.3.2 Licensed Cable Products that connect via Ethernet SHALL support transmitting and receiving packets containing Cable Content marked for priority using DSCP and/or 802.1p/q tags and shall support 100BaseT or better.
  - 4.8.3.3 Licensed Cable Products that connect via any Other Physical Interface SHALL support transmitting and receiving packets containing Cable Content marked for priority using DSCP and/or 802.1p/q tags, and shall use a network interface that has a PHY speed of capable of receiving, error resilient under a bit error rate of  $10^{-6}$ , a single stream (up to 38.8 Mbps). Other Physical Interfaces include UWB (ultra wideband), HomePlug AV, HomePNA, MoCA (Multimedia over Coax) and any new

physical interfaces with respect to which DRI Vendor has provided prior written notice to CableLabs and which meet the requirements listed above.

- 4.9. No feature or functionality of the Licensed Cable Product shall (a) technically disrupt, impede or impair the delivery of services to a cable customer; (b) cause physical harm to the network or the CableCARD; (c) facilitate theft of service or otherwise interfere with reasonable actions taken by cable operators to prevent theft of service; (d) jeopardize the security of any services offered over the cable system; or (e) interfere with or disable the ability of a cable operator to communicate with or disable a CableCARD or to disable services being transmitted through a CableCARD.
- 4.10. Graphics and Video Support for Licensed Cable Products that include display capability
  - 4.10.1. Licensed Cable Product MUST include an MPEG-2 decoder in compliance with Host 2.0
  - 4.10.2. Licensed Cable Product MUST include graphics support in compliance with Host 2.0

## **5. Compliance and Robustness Rules**

- 5.1. In addition to meeting the Compliance and Robustness Rules of this Adopter Agreement, each Licensed Cable Product shall:
  - 5.1.1. provide a level of protection consistent with the requirements of the Compliance and Robustness Rules set forth in the most current version license agreement for use of the DFAST Technology, including with respect to maintaining the protection of Cable Content through authorized digital, analog and high definition analog outputs, and prohibiting unauthorized retransmission of Cable Content over wide area networks and the Internet;
  - 5.1.2. assure that Cable Content may be output from DTCP only to outputs in the most current version license agreement for use of the DFAST Technology. For avoidance of doubt, the only digital outputs or content protection technologies for Cable Content are currently: 1394 with DTCP, DVI/HDMI with HDCP, WMDRM over DRI (with conditions), VCPS as a recording technology.
  - 5.1.3. provide for a means of security for the making of permissible copies in accordance with a Cablelabs DFAST approved recording technology;
  - 5.1.4. provide that removable recorded media will maintain the required level of protection when played back on an implementation other than the implementation upon which the recording was made in accordance with a CableLabs DFAST approved removable media recording technology;
  - 5.1.5. Licensed Cable Product SHALL NOT allow decrypted uncompressed Cable Content with a resolution greater than 520000 pixels per frame to be transmitted over a User Accessible Bus, in a Licensed Cable Product which does not comply with the following robustness requirements: The Licensed Cable Product shall be clearly designed such that when decrypted uncompressed video data with a resolution greater than a constrained image of 520000 pixels per frame is transmitted over a User Accessible Bus, such data is reasonably secure from unauthorized interception by using either Widely Available Tools or Specialized Tools, except with difficulty, other than Circumvention Devices.
  - 5.1.6. PCI Express is considered a user accessible bus for purposes of Cable Content.
  - 5.1.7. Access to Cable Content on a Cable Licensed Product shall be limited to applications of the Adopter of this Exhibit X on the Adopter's Licensed Cable Product.

5.1.8. **[[Additional amendments to be determined]]**

**5.2. Third Party Beneficiaries.**

5.2.1. CableLabs and Cable Operators are third party beneficiaries of the DTCP Adopters Agreement, and this Exhibit X, with respect to Cable Content.

## **DRI Adopters Compliance Letter**

For

**Model:** \_\_\_\_\_ (“Licensed Cable Product”)

***This Compliance Letter warrants the correct design and distribution of a Licensed Cable Product that incorporates features capable of being used with cable television services received from a DRI connection. This letter is intended to address certain (but not all) hardware and testing requirements necessary to the manufacture, marketing and distribution of such Licensed Cable Product. Failure to meet these requirements could result in a breach of the DTCP Adopter Agreement as well as a breach of this Compliance Letter. Company agrees that CableLabs and Cable Operators are third party beneficiaries of the DTCP Adopters Agreement, and Exhibit X to DTCP Adopters Agreement, with respect to Cable Content.***

Company, via the corporate officer identified below, hereby promises, represents and warrants to CableLabs and Cable Operators that:

1. The Licensed Cable Product has complied with the Exhibit X to DTCP Adopters Agreement - DRI License Requirements.
2. The Licensed Cable Product identified above has passed the Licensed Cable Product Tests provided by DTLA for DRI Adopters [to be supplied by CableLabs to DTLA] , and DRI Adopter has participated in a DRI Plug Fest.
3. Access to Cable Content on a Cable Licensed Product is limited to applications of the adopter of Exhibit X to DTCP Adopters Agreement on the Adopter’s Licensed Cable Product.
4. The Licensed Cable Product identified above will at the time of manufacture include support for applicable regulatory requirements imposed by the Federal Communications Commission (“FCC”) for Licensed Cable Products receiving and displaying cable programming (including broadcast programming retransmitted over a cable system) that are in effect as of the date of manufacture of the Licensed Cable Product. These include response to emergency alerts, channel mapping, closed captioning, content advisory/V-Chip, and language identification.
5. The Licensed Cable Product identified above, shall protect Cable Content in accordance with Exhibit A, without change or modification in the protection provided to the content or the rights granted in the content by or to the cable operator as received via the DRI.
6. The Licensed Cable Product identified above shall at the time of manufacture be compliant with this Agreement and as manufactured and distributed, no feature or functionality of the Licensed Cable Product shall (a) technically disrupt, impede or impair the delivery of services to a cable customer; (b) cause physical harm to the network or the CableCARD; (c) facilitate theft of service or otherwise interfere with reasonable actions taken by cable operators to prevent theft of service; (d) jeopardize the security of any services offered over

the cable system; or (e) interfere with or disable the ability of a cable operator to communicate with or disable a CableCARD or to disable services being transmitted through a CableCARD. Further, Company shall not shall not intentionally provide, promote or distribute subsequent modifications, upgrades, downloads, modules, or plug-ins to the Licensed Cable Product that defeat this requirement.

7. In no event shall Company's breach of this Compliance Letter give rise to liability to CableLabs or any Cable Operator, nor shall CableLabs or a Cable Operator be liable to Company, for consequential, incidental, special, indirect, punitive, or exemplary damages of any kind, including without limitation loss of profit, savings, or revenue, or the claims of third parties, whether or not advised of the possibility of such loss, however caused and on any theory of liability, arising out of this Compliance Letter or based on the making, using, selling or importing of any Licensed Cable Product. In no event shall either Company or CableLabs be liable to the other (or a Cable Operator) under any circumstances under this Compliance Letter for any amount that exceeds \$1,000,000 per instance of breach. As used herein, "instance" shall be defined as a breach attributable directly or indirectly to one cause (including a series of similar problems related to a single cause) and may, for example, affect multiple models or Licensed Cable Products sharing a common chassis. The foregoing limitation of liability shall not apply in the case of Company's failure to meet applicable regulatory requirements imposed by the FCC as provided in Section 4 of this Compliance Letter.
  
8. The foregoing limitation of liability in no way limits or otherwise affects the rights of CableLabs or a Cable Operator to seek injunctive relief against Company for a breach of this Compliance Letter. Company acknowledges that material breach of any obligation under this Compliance Letter will cause CableLabs, and/or the Cable Operators, to suffer immediate and irreparable harm and damage for which money alone cannot fully compensate. Company therefore agrees that upon such material breach, CableLabs shall be entitled to entry of a temporary restraining order, preliminary injunction, permanent injunction or other injunctive relief, without posting any bond or other security, compelling Company to comply with such obligations as deemed proper by a court of competent jurisdiction, provided, however, that neither CableLabs nor a Cable Operator may seek injunctive relief unless such party has first provided Company with notice. This paragraph shall not be construed as an election of any remedy, or as a waiver of any right available to either party under this agreement or the law, including the right to seek damages, nor shall this paragraph be construed to limit the rights or remedies available under applicable law for any violation of any provision of this Agreement.

Note: Company shall maintain records indicating such compliance and testing, and shall make such records available to CableLabs on reasonable request.

Corporate Officer: _____	Project Manager: _____
Title: _____	Title: _____
Phone: _____	Phone: _____
Fax: _____	Fax: _____
	E-Mail: _____

E-Mail: _____	Address: _____
Address: _____	_____
Signature: _____	Signature: _____
Date: _____	Date: _____

Quality Assurance: _____
Title _____
–
Phone: _____
Fax: _____
E-Mail: _____
Address: _____
<b>Signature:</b> _____
Date: _____

## DTLA Side Letter

In connection with CableLabs consideration of approval of DTCP-IP as a content protection technology for use in conjunction with the DFAST Technology, DTLA represents, warrants and agrees as follows:

- **DTLA accepts Conditional Technical Approval of DTCP-IP** over DRI, pending agreement to Exhibit X to the DTCP Adopters Agreement.
- **Test Suite.** DTLA must make available to Licensed Cable Product adopters a published test plan to ensure that DRI requirements herein are implemented correctly. (to be provided by Cablelabs)
- **IP Statement.** DTLA, its Founders, and Content Participants, hereby acknowledge that transcoding copy protection states that are not prohibited by FCC encoding rules satisfies the quitclaim conditions to the IP Statement. No subsequent change by DTCP shall trigger a right of action.
- **DTCP on 1394.** DTLA shall amend the DTCP Compliance and Robustness Rules to conform to Exhibit A hereto.
- **Changes in DTCP.** DTLA commits, that future changes to the technology specification(s), or amendments to the DTCP Adopters Agreement, including side letters, Exhibits, or waivers, will ensure against reductions in security for Cable Content, and not diminish the protections afforded to Cable Content. Any technical or legal changes that are material and substantial in nature, must be submitted to CableLabs for approval. Material changes shall include, but are not limited to: (1) mapping to a new transport or media; (2) changes in the encoding or treatment of Controlled Content; (3) changes that may have a material and adverse effect on the integrity or security of the technology; (4) changes in the cryptographic method used, except where the algorithm is unchanged and only the key length is expanded; (5) changes in the scope of redistribution; and (6) any fundamental change in the nature of the technology.
- **Changes to DFAST Compliance and Robustness Rules.** CableLabs shall provide to DTLA written notice in a commercially reasonable time frame, not to exceed 60 days, prior to any changes in the Compliance or Robustness Rules that are imposed on Licensees of the DFAST Technology (“DFAST C&R Changes”). DFAST C&R Changes may affect either functionality or security or both. To the extent that such DFAST C&R Changes would materially affect the functionality of devices subject to DFAST C&R Changes, or would reduce or cure an unreasonable risk of unauthorized access, copying, or distribution of Cable Content received from the DRI, DTLA shall use best efforts to implement such DFAST C&R Changes in the DTLA Compliance & Robustness Rules applicable to Licensed Cable Products in a substantially equivalent manner, and to make such changes applicable to such Licensed Cable Product within no less time than would be required of Licensees of the DFAST Technology. In the event that DTLA is otherwise in compliance with this Agreement, including the obligation to use best efforts to implement such DFAST C&R Changes, and CableLabs reasonably determines that those best efforts have not resulted in a substantially equivalent level of robustness and compliance in comparison to such DFAST C&R Changes, then CableLabs shall have the right to withdraw approval of DTCP as an approved content protection technology or to

pursue other remedies available in law or equity, or any other remedies available under this Agreement.

- Remedies and enforcement [more definition to be provided later]. DTLA acknowledges that DTCP as drafted has defined a role for content providers but not for distributors. Because Cable Operators are aggregators and the source of Cable Content, DTLA hereby agrees that:
  - Cable Operators and CableLabs are third party beneficiaries under the Adopters Agreement and Exhibit X;
  - Cable Operators and Cablelabs be afforded status and rights substantially equivalent to any Major AV Content Participant. At a minimum, such rights shall assure:
    - a right of revocation or for renewability in appropriate circumstances;
    - legal recourse is potentially available in case of circumvention of the technology by persons other than licensees;
    - effective remedies and enforcement means are available, potentially including legal recourse on the part of persons other than the licensor, for breaches of the license agreement and associated compliance and robustness requirements;
    - participation in the process and criteria for approving outputs
    - participation in the process to manage changes to DTCP or its licensing terms so that they do not diminish the protections afforded to Cable Content
  - DTLA agrees to provide assistance to CableLabs with any regulatory action required of CableLabs or any CableLabs' member with respect to the support by Licensed Cable Products for applicable regulatory requirements imposed by the Federal Communications Commission.
- Reserved Right. CableLabs reserves the right to rescind this approval in circumstances where there has been: (i) a significant compromise to the technology; or (ii) a change to the specification or license terms; that would have a material and adverse effect on the ability of the technology to robustly maintain the security of Cable Content protected by DTCP after it is passed to the technology or would materially and adversely compromise or interfere with the integrity and security of Cable Content.

## Exhibit A - DRI CONTENT PROTECTION REQUIREMENTS (normative)

- When paired with a CableCARD, the DRI Transceiver (DRIT, e.g., a DRI “source” device) SHALL output content received on the Cable Input ONLY on the DRI and consistent with the tables below. The DRI Receiver is referred to as the DRIR (e.g., a DRI “sink” device).
- The Content Protection System (e.g., DRM) SHALL specify usage rights (enforced pursuant to the applicable Content Protection System compliance rules) to permit content output only as shown in the tables below.

Content Type key: A = Analog; D = Digital; S, 0, 1, 2, 3, RCI and N summarize the values in the successive content control columns; X = ignore or don't care.

Analog TV Signals on DRIT Cable Input							DRM License and Encryption on DRI	Internal DRIR Retention Limit (min.)	Downstream Distribution from DRIR of DRM-Protected Cable Content		Output of Content by Devices Downstream of DRIT									
#	Content Type	CA Scrambled	Macrovision Encoding on Video Signal	APS <sup>1</sup>	CGMS-A <sup>1</sup>	RCD <sup>1</sup>			To Display Only Devices (no persistent storage)*	To External Storage Devices**	Analog Composite or Component Outputs				VGA <sup>4</sup> Max. Frame Resolution (pixels)	HDCP on DVI and HDMI	1394 / DTCP			VCPS Output Allowed (NP=not Protected)
											Macrovision Encoding on 480 line Video Signals	CEA-608-C and IEC 61880, or CEA-805-C encoding <sup>3</sup>	Image Constraint <sup>3</sup>	APS <sup>2</sup>			CGMS-A <sup>2</sup>	RC <sup>2</sup>	DTCP Encryption?	
1	A S	1	X	X	X	X			Not supported by the DRIT device											
2	A 300	0	AGC + 4 CS	X	X	X	Yes	90	Yes	No	AGC+ 4 CS	1,1	no	520k	Yes	Yes	1	1,1	No	
3	A 200		AGC + 2 CS								1,0									
4	A 100		AGC								0,1									
5	A 30		1,1								1									
6	A 20		1,0	1																
7	A 10		0,1	1																
8	A 03		1,1	1																
9	A 01		0,1	1																
10	A 02		1,0	1																
11	A RCI		0,0 or none	1																
12	A N		0,0 or none	0 or none																

Input of Digital TV on DRITCable Input							DRM License and Encryption on DRI	Internal DRIR Retention Limit (min.)	Downstream Distribution of DRM-Protected Cable Content	Output of Content by Devices Downstream of DRIT											
#	Content Type	CA-Scram-Bled <sup>6</sup>	CCI Value <sup>7</sup>						Display Only Devices (persistent storage not allowed)*	To External Storage Devices**	Analog Composite and Component Outputs					VGA <sup>10</sup>	HDCP on DVI or HDMI	1394/DTCP			VCPS Output Allowed
			ENR***	CIT	APS	EMI					Macrovision Encoding on All 480 Line Video Signals	CEA-608-B and IEC 61880, or CEA-805-C encoding <sup>8</sup>	Image Constraints <sup>9</sup>	Max. Frame Resolution (pixels)	DTCP Encryption?			EPN	EMI		
										AGC	APS	CGMS-A	RC								
1	D1 33			0	1,1			Yes		AGC+ 4 CS	1,1			No	520k	Yes	Yes	1	1,1	No	
2	D1 C33			1						AGC+ 2 CS	1,0										520k
3	D1 23			0	1,0							1,1									No
4	D1 C23	1	X	1		1,1	Yes			90				1							520k
5	D1 13			0	0,1																No
6	D1 C13			1								0,1									520k
7	D1 03			0	0,0																No
8	D1 C03			1								0,0									520k
9	D1 31			0	1,1			No		AGC+ 4 CS	1,1			No	520k	Yes	Yes	1	0,1	No	
10	D1 C31			1						AGC+ 2 CS	1,0										520k
11	D1 21			0	1,0							1,1									No
12	D1 C21	1	X	1		0,1	Yes			90				1							520k
13	D1 11			0	0,1																No
14	D1 C11			1								0,1									520k
15	D1 01			0	0,0																No
16	D1 C01			1								0,0									520k
17	D1 32			0	1,1			Yes	None	AGC+ 4 CS	1,1			No	520k	Yes	Yes	1	1,0	Protected	
18	D1 C32			1						AGC+ 2 CS	1,0										520k
19	D1 22			0	1,0							1,1									No
20	D1 C22	1	X	1		1,0	Yes			None				1							520k
21	D1 12			0	0,1																No
22	D1 C12			1								0,1									520k
23	D1 02			0	0,0																No
24	D1 C02			1								0,0									520k
25	D1 E30			0	1,1			Yes	None	AGC+ 4 CS	1,1	1,1		No	520k	Yes	Yes	0	0,0	Protected	
26	D1 EC30			1						AGC+ 2 CS	1,0	1,1									520k
27	D1 E20			0	1,0							1,1									No
28	D1 EC20	1	0 (Signaled)	1		0,0	Yes			None				1							520k
29	D1 E10			0	0,1								1,1								No
30	D1 EC10			1								0,1									520k
31	D1 E00			0	0,0								0,0								No
32	D1 EC00			1								0,0									520k
33	D1 30	1	1 (Not Signaled)	0	1,1	0,0	Yes	None	Yes				0	No	520k	Yes	No	1	0,0	Not Protected	
34	D1 C30			1							1,1			520k							
35	D1 20			0	1,0						1,1			No							
36	D1 C20			1						0,1				520k							
37	D1 10			0	0,1						1,1			no							



---

<sup>10</sup> VGA outputs as defined in CHILA. Content output over VGA can be output or displayed using video processing techniques such as line doubling or sharpening to improve the perceived quality of the image.

<sup>11</sup> If SCTE 21 data is present and includes values for APS, CGMS-A, or RC, the DRIT SHALL permit the output of content only according to the values shown in the inset tables.

\* Display Only Devices, which are downstream rendering devices that are not permitted under applicable compliance rules to persistently store Cable Content, shall be subject to agreed upon proximity limits.

\*\* External Storage Devices, which are downstream devices on which Cable Content can be stored (where permitted under applicable compliance rules) and played back, shall be subject to agreed upon proximity limits (when obtaining content) and limited to Standard Definition.

\*\*\* ENR is Encryption Not Required

# **EXHIBIT 7**



Digital Transmission  
Licensing Administrator

March 14, 2006

VIA EMAIL, CERTIFIED MAIL  
AND FACSIMILE (303) 661-9199

Michael E. Davis  
Project Director, OpenCable Business Relations  
CableLabs  
858 Coal Creek Circle  
Louisville, CO 80027-9750

Dear Michael:

The Digital Transmission Licensing Administrator, LLC (“DTLA”) responds below to the letter of March 5, 2006, from CableLabs, together with the proposed Exhibit X and Side Letter. DTLA thanks CableLabs for its willingness to grant “provisional approval” to DTCP-IP. This willingness to grant such approval recognizes that DTCP-IP provides robust technological protection for Controlled Content. Therefore, we believe that further discussions between DTLA and CableLabs should focus on the scope of additional obligations so as to ensure that Controlled Content when presented to an output protected by DTCP-IP will properly trigger the protections of DTCP-IP.

We are concerned about the set of obligations proposed by CableLabs in Exhibit X and the Side Letter as a condition to the approval of the DTCP-IP content protection system. In particular, DTLA’s licenses do not cover or dictate the elements of any of the underlying protocols over which DTCP may operate, and do not impose any requirements with respect to the operation of services across those protocols. Any such requirements lie beyond the scope of content protection technology, and so cannot be encompassed within a license for DTCP.

The only obligations that DTLA imposes in its Adopter Agreements is to ensure that the proper levels of DTCP protection are triggered by the content to be protected when delivered to the DTCP-IP output. We propose in the attachment to this letter a simple streamlined alternative that would achieve the goal of protecting “Controlled Content” by proposing the authorizing clauses and defining the “associated obligations” to be included in the CableLabs DFAST, CHILA and DCAS agreements. This document

Michael E. Davis

March 14, 2006

Page 2

satisfies the requirement in your March 5 letter that DTLA should promulgate a document specifying the applicable rights mapping requirements for Controlled Content to be protected using DTCP-IP.

We respond to your letter below, first, by explaining in more detail the approach we propose and, second, by addressing some of the specific points in your letter and your attachments.

#### Background to our Proposed Approach

In other contexts in which DTCP-IP has received approval from third parties for use with respect to protected content from particular sources, the approvals have been accompanied by a set of "Associated Obligations." These Associated Obligations specify the particular settings required in the Source Function so as to trigger correctly the specified level of protection via DTCP-IP. Associated Obligations therefore are to be included in the licenses for the technologies that provide the source content. For example, the DVD CCA approval of DTCP-IP for protecting CSS-encrypted content output from DVD Video discs included such associated obligations in the Procedural Specifications for CSS. Similarly, the FCC approval of DTCP-IP for protection of Marked Content and Unscreened Content in the Broadcast Flag proceeding included associated obligations governing the proper presentation of information so as to trigger the "EPN" setting in DTCP-IP. Such associated obligations also appears to have covered all that was necessary in our prior discussions with CableLabs concerning the approval of DTCP over 1394. And, similarly, when DTLA and its Content Participants in the past have approved the output of DT Data to other protection systems, we similarly have assured the manner in which the CCI and EMI for DTCP should be mapped to the other system.

In the DFAST context, if the Controlled Content presents to the DTCP-IP output the correct E-EMI and CCI settings, then DTCP will ensure that the content remains protected thereafter on home and personal networks in accordance with those settings. Because these obligations attach upstream from the DTCP-IP output, they properly belong as requirements for DFAST, CHILA, and DCAS rather than in the DTCP Adopter Agreement. If these OpenCable license agreements condition the use of DTCP-IP upon presenting to the DTCP-IP output the specified E-EMI and CCI settings as set forth in the attached Associated Obligations, these settings will trigger the correct levels of protection as required by the encoding applied to the content via the content owner and cable operator.

The attachment hereto proposes the two necessary elements for implementation of DTCP-IP in products covered by the DFAST, CHILA and DCAS licenses ("Digital Cable Products"). The first is to state in these OpenCable license agreements that DTCP-IP has been approved as a digital output protection technology, and to require that a Digital Cable Product with a DTCP-IP output must follow the requirements in the DTCP Specification for a "Format-cognizant real-time-delivery content source/decoding device." The second is to set forth the appropriate settings for the E-EMI and CCI to be

presented to the DTCP-IP output, as applicable to each of the four protected states enabled by DTCP as well as to the state in which no protection is being applied via DTCP. These are the only obligations that need to be implemented in order to properly trigger the use of DTCP-IP at the DTCP-IP output. From that point forward, devices downstream that implement DTCP will protect the content in accordance with the requirements of the DTLA Adopter Agreement, including its Compliance Rules and Robustness Rules.

#### DTLA Response to the March 5 CableLabs Proposal and Letter

The specific elements of your proposed Exhibit X and the Side Letter relating to quality of service, consumer notification, and so forth, constitute “upstream” obligations from DTCP-IP that should be addressed in the OpenCable license agreements. Such obligations are outside the scope of the DTLA Adopter Agreement because they do not pertain directly either to DTCP itself or to the downstream protection of content that once had been protected using DTCP. Such obligations have nothing to do with content protection and so are not germane to the very limited content protection subject matter covered by DTCP.

In no other context has DTLA been asked to address the types of issues that CableLabs asks of DTLA Adopters in your letter of March 5, 2006. Any Adopter that wishes to implement DTCP over 1394, IP, USB, MOST, Op-iLink, IDB 1394, and so forth, bears the responsibility of ensuring that its products adequately implement these protocols in a manner that enables the transport of the protected audio and audiovisual content. Issues relating to quality of service, bandwidth, and so forth, are the responsibility of the manufacturer – not of the licensor of a content protection technology that may be used to protect content traversing those interfaces.

We have endeavored in our past discussions with you to make this point. We consistently have noted that it should not be the responsibility of a proponent of a content protection technology to design the video transport layer. As we have noted, the video transport standard selected for DTCP-IP does not affect the level of security provided by DTCP-IP to Controlled Content, and the level of security provided in the DTCP-IP specification will not change, regardless of the video transport standard adopted.

Notwithstanding, and hoping to accelerate CableLabs approval of DTCP-IP, several DTLA member companies contributed substantial efforts to help CableLabs choose the applicable video transport layer over IP. As we noted in our correspondence with you, such efforts are beyond the charter of DTLA and so could not fairly be characterized as a DTLA effort. Moreover, because at least one of the DTLA member companies has not signed a Contribution Agreement with CableLabs, we were informed that CableLabs would not permit nonsignatory companies to participate in this process, and such nonsignatories specifically were excluded by CableLabs from key meetings to discuss potential solutions. (In that respect, your March 5 letter is inaccurate. The DRI Specification itself may be a public document; but at the time of that December 6

Michael E. Davis

March 14, 2006

Page 4

meeting there was no agreement to use DRI as the solution, and CableLabs would not permit any nonsignatories to attend that meeting. Thus, our statement stands that CableLabs has excluded certain DTLA member companies from any meaningful participation in this project.)

In spite of the various changes of direction by CableLabs, Intel recently submitted to CableLabs a proposal that satisfied your request based the video transport layer according to the DLNA Home Network version 1.5 (HNv1.5) guidelines. These guidelines are being adopted as a robust, secure and interoperable standard in inter-industry discussions. From the perspective of DTLA member companies, use of such inter-industry standards provides significant benefits to the marketplace by more readily integrating digital cable devices into the overall home and personal network environment. You therefore can understand the dismay that CableLabs apparently ignored the Intel suggestion in favor of the proprietary DRI interface.

Notwithstanding, now that CableLabs is ready to adopt an IP video transport, CableLabs cannot offer this as a reason to delay or condition approval of DTCP-IP upon the ability of DTCP-IP Adopters to follow specific QoS and man-machine interface standards designed by CableLabs in any device that in some manner may receive content first delivered to the home over a cable system. Any concerns regarding quality of service, delivery of error messages over the MMI, or compliance with a video transport standard for IP may affect the performance of the IP connection itself, which may be of concern to manufacturers. But, they do not affect the security provided by the DTCP-IP digital output protection technology. Therefore, they do not provide CableLabs with a justification to delay approval of DTCP-IP under either the terms of the OpenCable license agreements or the requirements set forth by the Federal Communications Commission ("FCC") upon its approval of the DFAST license for unidirectional digital cable ready devices.

Specifically, section 2.4.4 of Exhibit B of the DFAST license states that "CableLabs shall not withhold approval of any such output or content protection technology that provides effective protection to Controlled Content against unauthorized interception, retransmission and copying." Although the FCC recognized in its Second Report and Order of October 2, 2003, "the fundamental interest of the cable industry in ensuring that devices connecting to their distribution systems do not result in theft of service or harm to their networks," it expressed concern that "CableLabs' proposed role as the sole initial arbiter of outputs and associated content protection technologies to be used in unidirectional digital cable products could affect innovation and interoperability in a number of areas . . . ." None of the issues addressed in CableLabs's proposed "Exhibit X" or "DRI Adopters Compliance Letter" directly relates to either theft of service or harm to the cable network. Thus, CableLabs has articulated no legitimate rationale to further delay approval of DTCP-IP.

DTLA has demonstrated clearly and persuasively that DTCP-IP "provides effective protection to Controlled Content against unauthorized interception,

retransmission and copying” as the DFAST license requires. Nor does DTCP-IP preclude cable providers from “ensuring that devices connecting to their distribution systems do not result in theft of service or harm to their networks.”

Moreover, CableLabs’ own policy statement regarding approval of digital content protection technologies does not make the evaluation of video transport a mandatory condition of approval. Rather, the document states that “CableLabs will evaluate all proposals in a reasonable, objective, and non-discriminatory manner. *Depending on the specific output or technology submitted*, criteria for evaluation will include [video transport]: . . . .” Submission of New Digital Outputs and Content Protection Technologies, September 17, 2004, v. 1.4, at ¶ 4 (emphasis added). Now that CableLabs has settled on a video transport, CableLabs can no longer offer the absence of a video transport as a reason to withhold or further condition the approval of DTCP-IP.

The FCC has acknowledged that video transport standards are irrelevant to the level of security provided by an output protection technology. In approving DTCP-IP in the context of broadcast flag regulations, the FCC did not evaluate the robustness of the video transport standard or concern itself with issues of quality of service, notices to consumers, man-machine interface, out of band data, or any of the obligations that CableLabs has attempted to impose upon DTLA before approving DTCP-IP. CableLabs likewise should recognize the limited scope of concerns relating to content protection technology, and should not hold up approval of DTCP-IP.

As an aside, your letter asserts that “DTLA appears to also require a transport to be approved (see e.g., DTCP on USB-IP).” We are unaware of either any circumstance in which DTLA requires a transport to be approved or of any application of DTCP or transport known as “DTCP on USB-IP.” We further note that in the recent discussions with our Content Participants leading to the promulgation of the May 2005 Adopter Agreement, DTLA and our Content Participants specifically discussed the question of whether PCI Express should be classified as a “User Accessible Bus.” The parties examined the question and determined that it should not be so classified. For that reason, even though certain changes were made to the User Accessible Bus provisions in the May 2005 Adopter Agreement, PCI Express specifically was not added to the list of User Accessible Buses.

Finally, any further delay or attachments of conditions to approval of DTCP-IP runs contrary to the promise by CableLabs to approve digital output protection technologies that have the support of four MPA member studios. Section 2.4 of the DFAST license provides: “in the event that CableLabs is advised that four (4) member studios of the Motion Picture Association approve a digital output or content protection technology that provides effective protection to Controlled Content against unauthorized interception, retransmission or copying, such output or content protection technology shall be deemed approved by CableLabs pursuant to this Section 2.4.4, and upon receipt of notice by CableLabs of such approval by the four studios, CableLabs shall amend these Compliance Rules to include such output and/or content protection technology.”

Michael E. Davis

March 14, 2006

Page 6

Notably, this promise does not include the right to condition its approval on any matters, no less on matters such as QoS that are unrelated to content protection. On July 11, 2005, the MPAA sent a letter to CableLabs expressing support for approval of DTCP-IP. That support recently was reiterated by the MPAA in its February 6, 2006, Comments to the FCC in CS Docket 97-80, in which they state that “the MPAA and its member companies support the approval of DTCP over IP as an authorized output technology under the DCAS License,” and that MPAA “strongly urges CableLabs to amend the DCAS License to support the approval of DTCP over IP... .” Comments at 5, 6. In addition, as CableLabs is aware, DTCP-IP has been approved as an authorized digital output protection technology by DVD-CCA for Copy Never content from DVD Video Discs that have been encrypted using CSS, and by AACS-LA for all protected content, including from high definition optical discs. This strong showing of support from the motion picture industry further demonstrates that CableLabs has an obligation under its own license agreements to grant immediate and unconditional approval for DTCP-IP in all CableLabs license agreements.

As we have informed you, CableLabs’s decision to continually delay or condition approval of DTCP-IP pending resolution of issues unrelated to content protection is prejudicing DTLA’s ability to provide its Adopters with competitive marketplace content protection solutions. Any further conditions or delay can only lend credence to the FCC’s concern about CableLabs’ “role as the sole initial arbiter of outputs and associated content protection technologies.” DTLA and its member companies therefore request that CableLabs abide by its licensing and regulatory obligations and immediately approve DTCP-IP as a digital output technology under the DFAST, CHILA and DCAS license agreements.

We look forward to your prompt response and to prompt full approval of DTCP-IP by CableLabs.

Sincerely,

/s/

\_\_\_\_\_  
Michael B. Ayers

President

Digital Transmission Licensing Administrator, LLC

## **Obligations for Controlled Content Output over DTCP-IP**

The following sets forth suggested amendments to the OpenCable technology license agreements for products that would implement DTCP-IP. These suggested amendments are intended to provide the set of information necessary to enable a Digital Cable Product to map correctly to the content protection states supported by DTCP-IP.

Capitalized terms used below that are not used in the OpenCable technology license agreements shall have the meaning set forth in the DTCP Specification and DTCP Adopter Agreement.

### 1. Suggested Amendment to CableLabs Compliance Rules

#### a. For DFAST License

- i. Add as Exhibit B, Compliance Rules, Section 2.4.3 the following:

If a Unidirectional Digital Cable Product includes any form of output using the Internet Protocol, such Unidirectional Digital Cable Product may output Controlled Content, and pass Controlled Content to such output in digital form where such output is protected by DTCP-IP. A Unidirectional Digital Cable Product, when passing Controlled Content to such output protected by DTCP-IP, is to follow requirements for a “Format-cognizant real-time-delivery content source/decoding device” as set forth in the “Digital Transmission Content Protection Specification” as such specification may be amended from time to time.

- ii. Renumber current paragraph 2.4.3 and subsequent paragraphs accordingly.

- iii. Change “2.4.4” in the text of renumbered 2.4.4 and 2.4.5 to read “2.4.5”.

#### b. For CHILA License

- i. Amend Exhibit B, Compliance Rules, Section 2.4.1 to read as follows:

2.4.1 DTCP. Licensed Product may output Controlled Content, and pass Controlled Content to an output protected by DTCP, in digital form as follows:

2.4.1.1 Over IEEE 1394 interfaces as specified by the OpenCable Specifications, where such output is protected by DTCP. Licensed Product must support DTCP “Full Authentication,” and may additionally support DTCP “Restricted Authentication.” If required by the applicable license for DTCP,

content that is *not* Controlled Content shall be output on the IEEE 1394 output without DTCP protection.

2.4.1.2 Over IP interfaces, in the manner specified by the OpenCable Specifications, where such output is protected by DTCP-IP. Licensed Product must support DTCP “Full Authentication,” and may additionally support DTCP “Restricted Authentication.” If required by the applicable license for DTCP, content that is *not* Controlled Content shall be output on the IP interface without DTCP protection. A Licensed Product, when passing Controlled Content to such output protected by DTCP-IP, is to follow requirements for a “Format-cognizant real-time-delivery content source/decoding device” as set forth in the “Digital Transmission Content Protection Specification” as such specification may be amended from time to time.

ii. Add the following to Exhibit B, Compliance Rules:

2.4.3.2 DTCP-IP. Content may be output over the DRI protected by DTCP-IP in accordance with the OCUR-HMS Content Protection Requirements, where connected to a device that runs Microsoft Windows Media Center Edition (a “MCE HMS”) and such MCE HMS complies with (1) the OEM Compliance Letter between CableLabs and the MCE HMS manufacturer, such compliant devices posted at [www.opencable.com](http://www.opencable.com), and (2) the Redacted Agreement between Microsoft and CableLabs dated Dec 12, 2005.

c. For DCAS Host License Agreement

Amend Exhibit C, Compliance Rules, to add section 2.4.2 as follows:

2.4.2 **IP with DTCP.** Licensed Product may output Controlled Content, and pass Controlled Content to an output, in digital form over IP interfaces in the manner specified by the DCAS Specifications, only if such output is protected by DTCP. The DTCP source function in the Licensed Product must support DTCP “Full Authentication,” and may additionally support DTCP “Restricted Authentication.” In addition, the DTCP source function is required to: (a) process all validly received DTCP System Renewability Messages (“SRM”); (b) convey downstream all validly received System Renewability Messages supported by DTCP through its IP interface with DTCP output; and (c) map the copy control information (CCI) to the DTCP Encryption Mode Indicator (EMI), DTCP Analog Protection System (APS) signaling, DTCP Image Constraint Token (ICT), and DTCP Encryption Plus Non-assertion (EPN) signaling as defined in the DCAS Specifications. Capitalized terms used in this Section, but not otherwise defined in this Exhibit C or the Agreement, shall have the meaning set forth in the DTCP specification or the DTCP

Adopter Agreement. If required by the applicable license for DTCP, content that is *not* Controlled Content shall be output on the IP output without DTCP protection. A Licensed Product, when passing Controlled Content to such output protected by DTCP-IP, is to follow requirements for a “Format-cognizant real-time-delivery content source/decoding device” as set forth in the “Digital Transmission Content Protection Specification” as such specification may be amended from time to time.

Renumber remaining sections accordingly.

*[Remainder of page intentionally left blank]*

2. Suggested Associated Obligations for OpenCable License Agreements

A product licensed under the DFAST, CHILA or DCAS agreements (hereinafter “Digital Cable Product”), shall implement the following Associated Obligations when passing content to an output protected with DTCP-IP:

DTCP Encoding	Associated Obligations <sup>1</sup>															
Copy Freely	<p>When passing content that is not Controlled Content to an output protected by DTCP, a Digital Cable Product shall</p> <p>(a) not be required to carry any DTCP System Renewability Messages delivered in association with such content (in a manner to be defined) to the DTCP Source Function, and</p> <p>(b) set the following fields of the DTCP Descriptor to the indicated binary values:</p> <table data-bbox="625 951 1339 1129"> <tr> <td>APS:</td> <td>00</td> <td>(copy-free),</td> </tr> <tr> <td>DTCP_CCI:</td> <td>00</td> <td>(copy-free),</td> </tr> <tr> <td>EPN:</td> <td>1</td> <td>(EPN not asserted),</td> </tr> <tr> <td>Image_Constraint-Token:</td> <td>1</td> <td>(no constraint),</td> </tr> <tr> <td>Retention_State:</td> <td>000</td> <td>(forever), and</td> </tr> </table> <p>(c) set the E-EMI Value to 0000 (copy-free).</p>	APS:	00	(copy-free),	DTCP_CCI:	00	(copy-free),	EPN:	1	(EPN not asserted),	Image_Constraint-Token:	1	(no constraint),	Retention_State:	000	(forever), and
APS:	00	(copy-free),														
DTCP_CCI:	00	(copy-free),														
EPN:	1	(EPN not asserted),														
Image_Constraint-Token:	1	(no constraint),														
Retention_State:	000	(forever), and														
Copy Control Not Asserted – Redistribution Controlled	<p>When passing Controlled Content marked as Copy Control Not Asserted – Redistribution Controlled to an output protected by DTCP-IP, a Digital Cable Product shall</p> <p>(a) carry any DTCP System Renewability Messages delivered in association with such content (in a manner to be defined) to the DTCP Source Function, and</p>															

<sup>1</sup> Where more than one value is permitted for a particular binary field, the value shall be set in accordance with the authorization of the entity authorized to set the encoding for that specific content. In the absence of specific authorization, where a default value is specified, the default value shall be used.

	<p>(b) set the following fields of the DTCP Descriptor to the indicated binary values:</p> <table border="0"> <tr> <td>APS:</td> <td>00</td> <td>(copy-free),</td> </tr> <tr> <td>DTCP_CCI:</td> <td>00</td> <td>(copy-free),</td> </tr> <tr> <td>EPN:</td> <td>0</td> <td>(EPN-asserted),</td> </tr> <tr> <td>Image_Constraint-Token:</td> <td>1</td> <td>(no constraint),</td> </tr> <tr> <td>Retention_State:</td> <td>000</td> <td>(forever), and</td> </tr> </table> <p>(c) set the E-EMI Value to 0010 (copy-free/EPN asserted).</p>	APS:	00	(copy-free),	DTCP_CCI:	00	(copy-free),	EPN:	0	(EPN-asserted),	Image_Constraint-Token:	1	(no constraint),	Retention_State:	000	(forever), and												
APS:	00	(copy-free),																										
DTCP_CCI:	00	(copy-free),																										
EPN:	0	(EPN-asserted),																										
Image_Constraint-Token:	1	(no constraint),																										
Retention_State:	000	(forever), and																										
Copy One Generation	<p>When passing Controlled Content marked as “Copy One Generation” to an output protected by DTCP-IP, a Digital Cable Product shall</p> <p>(a) carry any DTCP System Renewability Messages delivered in association with such content (in a manner to be defined) to the DTCP Source Function, and</p> <p>(b) set the following fields of the DTCP Descriptor to the indicated binary values:</p> <table border="0"> <tr> <td>APS:</td> <td>00</td> <td>(APS not asserted)</td> </tr> <tr> <td></td> <td>01</td> <td>(APS on – AGC only)</td> </tr> <tr> <td></td> <td>10</td> <td>(APS on – AGC + 2L Colorstripe)</td> </tr> <tr> <td></td> <td>11</td> <td>(APS on – AGC + 4L Colorstripe)</td> </tr> <tr> <td>DTCP_CCI:</td> <td>10</td> <td>(copy one generation),</td> </tr> <tr> <td>EPN:</td> <td>1</td> <td>(EPN not asserted),</td> </tr> <tr> <td>Image_Constraint-Token:</td> <td>1</td> <td>(no constraint - default)</td> </tr> <tr> <td></td> <td>0</td> <td>(constrained),</td> </tr> <tr> <td>Retention_State:</td> <td>000</td> <td>(forever), and</td> </tr> </table> <p>(c) set the E-EMI Value to 1010 (copy-one-generation/format cognizant).</p>	APS:	00	(APS not asserted)		01	(APS on – AGC only)		10	(APS on – AGC + 2L Colorstripe)		11	(APS on – AGC + 4L Colorstripe)	DTCP_CCI:	10	(copy one generation),	EPN:	1	(EPN not asserted),	Image_Constraint-Token:	1	(no constraint - default)		0	(constrained),	Retention_State:	000	(forever), and
APS:	00	(APS not asserted)																										
	01	(APS on – AGC only)																										
	10	(APS on – AGC + 2L Colorstripe)																										
	11	(APS on – AGC + 4L Colorstripe)																										
DTCP_CCI:	10	(copy one generation),																										
EPN:	1	(EPN not asserted),																										
Image_Constraint-Token:	1	(no constraint - default)																										
	0	(constrained),																										
Retention_State:	000	(forever), and																										
Copy Never	<p>When passing Controlled Content marked as “Copy Never” to an output protected by DTCP-IP, a Digital Cable Product shall</p> <p>(a) carry any DTCP System Renewability Messages delivered in association with such content (in a manner to be defined, e.g. by ATSC) to the DTCP Source Function, and</p>																											



	10	(APS on – AGC + 2L Colorstripe)
	11	(APS on – AGC + 4L Colorstripe)
DTCP_CCI:	01	(no more copies),
EPN:	1	(EPN not asserted),
Image_Constraint-Token:	1	(no constraint - default)
	0	(constrained),
Retention_State:	000	(forever),
and		
(c) set the EMI Value to 0100 (no-more-copies).		

# **EXHIBIT 8**

March 29, 2006

Mr. Seth D. Greenstein  
CONSTANTINE | CANNON, P.C.  
1627 Eye Street, N.W.  
Washington, D.C. 20006

**Re: Approval of DTCP-IP under DFAST License for UDCP Products**

Dear Seth:

Thank you for your letter of March 14, 2006 concerning CableLabs' willingness to grant conditional approval of DTCP-IP for use in unidirectional digital cable products (UDCPs). Although there seems to be some misunderstandings between us, and some disagreements, I believe that a key suggestion in your response can provide a vehicle for CableLabs to grant approval in a way that addresses both your resistance to amending the DTCP Adopters Agreement and CableLabs' need to protect legitimate cable industry requirements for the delivery of cable services.

First, let me get our disagreements and misunderstandings out of the way. Much of your response is devoted to arguing that CableLabs may not take into account anything more than what the FCC took into account in approving DTCP-IP for broadcast flag purposes. You will recall that the FCC rejected DTLA's request that DTCP should be approved for all transports and media, noting that significant issues can arise when a content protection technology is mapped to another connector. DTLA asked the FCC to supplant the approval role currently assigned to CableLabs in "plug and play," and to make broadcast flag approval tantamount to "plug and play" approval. The FCC declined.<sup>1</sup>

Likewise, while I understand that DTCP-IP has been approved for other platforms in which the content provider can directly control the timing and content made available for output (e.g., AACS, CSS), DTLA is requesting approval of an output for all cable content available on a UDCP, independent of any specific implementation and subject to a licensing regime which DTLA is reluctant to amend. As a competitive service provider, the cable industry and its content suppliers have a legitimate right to expect that cable services will be rendered properly when delivered through a CableCARD-enabled device. This should help explain why we require

---

<sup>1</sup> "We are mindful that the digital broadcast content protection lens through which we are viewing these technologies focuses on a small subset of their capabilities. In light of this fact, our analysis and review of the above-referenced certifications must maintain a similar perspective. We are reviewing these technologies solely for their suitability in protecting digital broadcast television content as a part of the redistribution control system we established in the Broadcast Flag Order. To the extent that certain of these technologies may be intended for use in unidirectional digital cable ready products to protect pay television programming, initial approval determinations are made by CableLabs..." *Digital Output Protection Technology and Recording Method Certifications*, FCC 04-193 ¶64.

## CableLabs®

Cable Television Laboratories, Inc.

that DTCP-IP devices remain capable of presenting the MMI-interface necessary for a CableCARD to initialize, meet certain video transport requirements (including EAS, Closed Captioning, Content Advisory/v-chip, Language Selection, etc), address QoS issues for delivery of Cable Content or provide certain notices to the consumer,<sup>2</sup> and can live up to the existing DFAST license requirements that they not “technically disrupt, impede or impair the delivery of services to a cable customer.”<sup>3</sup> These and similar requirements, such as minimum working requirements for the delivery of cable content to networked screens, were agreed to by Microsoft for a comparable IP output. These issues are not analogous to other approvals or uses of DTCP where the content provider has direct control over the flow, or lack thereof, of content to the medium (e.g., an HD-DVD) or the Internet (e.g., MovieLink, CinemaNow) and delivery of service issues are not a direct, real time, issue (e.g., burning of DVDs).

Part of CableLabs role is to make certain that outputs and content protection technologies satisfy such requirements. You are correct that our guidelines do not appear to make video transport mandatory for every content protection submission. What you may not appreciate is that we are called upon to evaluate many technologies, so our guidelines for reviewing output and copy protection submissions necessarily “depend on the specific output or technology submitted,” as we say in the posted guidelines. CableLabs “evaluates all proposals in a reasonable, objective and non-discriminatory manner.” For example, on March 20, 2006, we approved a secure recording technology from EnCentrus. In December, 2005, we approved Windows Media DRM. These two submissions were quite different, and CableLabs completed the separate reviews based on the specific technology submitted. In the EnCentrus case, the technology enables the secure recording of certain Cable Content on internal or external hard drives, so “video transport” questions were not at issue. In the WMDRM case, video transport issues were a significant issue. Our review and approval process resulted in two new CableLabs specifications to ensure that WMDRM will securely receive and use Cable Content, as well as a number of changes to the WMDRM licensing obligations that flow to WMDRM adopters. A careful review of the proposal we sent to you in early March will reveal almost identical provisions as those included in the license between CableLabs and Microsoft for WMDRM-enabled devices capable of receiving Cable Content.<sup>4</sup>

I also need to take issue with a misunderstanding you have about the process we followed with you. At no time did CableLabs ever exclude any DTLA member from participating in the technical working group that was formed during the course of our DTCP-IP review. All of the members of DTLA have signed the OpenCable Contribution Agreement, and two of your members (Intel and Sony) participated in the working group meeting here at CableLabs on December 6, 2005. Although we did not extend a formal written invitation to all DTLA

---

<sup>2</sup> To quote the 1394 Trade Association, of which many of the Founders of DTLA are also members: “ ‘QoS’ cannot be an afterthought, or an upgrade– it must be in all products...” FCC *ex parte* filed March 27, 2006 by 1394 trade Association. We agree.

<sup>3</sup> See DFAST Technology License Agreement, section 2.2.

<sup>4</sup> Although you suggest that MPAA’s statement supporting the approval DTCP-IP automatically qualifies DTCP-IP for use under DFAST, we do not consider that statement to satisfy the requirements of the DFAST license.

members, we did advise Mr. Andre that he was free to invite technical experts that he believed would be able to contribute to the work. At all times, CableLabs treated Mr. Andre as the representative and agent of DTLA.<sup>5</sup>

We also take issue with your characterization of our process as one of unfair delay, irrelevant conditions, and prejudicial to your interests. I am only one of the many professionals who have devoted considerable energy to trying to approve a submission that was made without even addressing video transport of cable content. It would have been simpler in many respects to approve an output submitted directly by an implementer, so that all issues could be evaluated in a very specific context. But as you know, we have been working with you to permit the approval of a generic IP content protection technology independent of a specific implementation, in order to accommodate the business model of your Adopter Agreement. DFAST specifically expects us to evaluate “the license terms governing the secure implementation of the technology.” We did not “approve” the effectiveness of the WMDRM technology in a vacuum that ignored the associated licensing regime. Microsoft modified its licenses and its robustness and compliance rules to work with cable content. CableLabs should not be expected to approve DTCP-IP without comparable adjustments. That is the reason we thought that supplementing the Adopter Agreement with a set of associated obligations that attach to cable content would be the most appropriate and expeditious approach, and the one that seemed most promising for promoting interoperability. But, as you made clear, DTLA has declined to take that approach.

So, let me move on to what I hope are areas of agreement and a potential means for CableLabs to grant approval in a way that addresses both your resistance to amending the DTCP Adopters Agreement and CableLabs’ need to protect legitimate cable industry requirements for the delivery of cable service. Our March 5, 2006 proposal for modifying the DTLA Adopters License addressed the issues that must be taken into account for any device receiving Cable Content via DTCP-IP, and we believe that the general approach of our proposal was not inconsistent with DTLA’s established practice of “mapping” DTCP to various transports such as USB, MOST, BlueTooth, and 1394. In addition, we believe that the approach we proposed would be the most “consumer friendly,” as this approach enables relative interoperability between any UDCP manufacturer’s products and any DTLA Adopter’s products.

It is clear from your March 14, 2006 response that DTLA is far more comfortable to applying such requirements from the *source* license: DFAST. Your explanation of how DTLA has previously approached “associated obligations” for products with source functions was helpful, and provides a starting point for products built under the DFAST Technology License. We believe we can also reach agreement from your proposed framework.

---

<sup>5</sup> Only in a brief email exchange on January 12, 2006, on which you were copied, did any party suggest that there might be an issue that was Intel-specific and not related to DTLA. This issue is one which we hope to pursue directly with Intel.

The approach we are suggesting today takes you up on the suggestion to place obligations directly on a DTCP source implementer to assure the obligations associated with cable content are met by DTCP-IP sources and sinks. We are prepared to modify the DFAST Technology License in a manner as attached here titled "Exhibit B-1. Video Transport Requirements for IP Outputs." This exhibit to the DFAST license relieves the need to change the DTLA Adopter's Agreement, per DTLA's request, and imposes certain obligations on the UDCP manufacturer (the DTCP-IP source) to ensure that connected downstream DTCP-IP devices meet applicable requirements before delivering any Cable Content.<sup>6</sup>

As you'll see, the attached exhibit does not specifying "how" the UDCP manufacturer ensures compliance of the downstream device – this is left to the implementer.<sup>7</sup> It does require adherence to the DRI mapping table. That table is written to map more granular settings than your proposed table; and is intended to apply to multiple IP platforms.<sup>8</sup> Overall, this proposal meets your stated objective: approval of DTCP-IP would be conditioned on the UDCP manufacturer abiding by the terms and conditions of the DFAST license, and not on changes in the DTCP Adopters Agreement.

---

<sup>6</sup> As you know, we have been working on approval of DTCP-IP under the DFAST Technology License, not for bi-directional products built under CHILA or the DCAS Host License Agreement, both of which you raised in your March 14, 2006 letter. More advanced two-way cable products will implement the OpenCable Application Platform (OCAP) middleware specification and will therefore be capable of receiving advanced cable services and applications, and to meet higher standards. Two-way connectivity and OCAP also provide a means to more elegantly address the issues at hand.

<sup>7</sup> If DTLA wishes to promote greater interoperability for DTCP-IP products, it could consider an amendment to the Adopters Agreement as previously suggested or a cable-specific amendment to the "Format-cognizant real-time-delivery content source/decoding device" as set forth in the "Digital Transmission Content Protection Specification." Or, manufacturers may propose more uniform or standardized solutions. But, in the meantime, DCTP-IP would be approved for use by UDCP manufacturers.

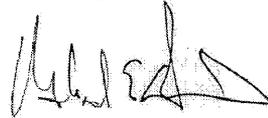
<sup>8</sup> By contrast, the table you suggested in your letter does not include enough granularity in some respects, and also includes business models not yet supported by UDCPs (e.g., retention state of 1 week) which cannot be signaled.

## CableLabs®

Cable Television Laboratories, Inc.

Seth, as stated above, CableLabs is prepared to finalize the approval of DTCP-IP, with the conditions and obligations being placed on the UDCP manufacturer through the DFAST Technology License. (There are a few selected assurances CableLabs would obtain directly from DTLA, to match the arrangement with IP outputs protected by WMDRM—see enclosed outline of DTLA Side Letter terms at the bottom of the exhibit.) If DTLA concurs with this approach, we would like to begin working with you on a press release, or press releases that announce this significant milestone. We would suggest that we target a release for the week of April 9<sup>th</sup> during the National Cable & Telecommunications Association (NCTA) tradeshow in Atlanta.

Sincerely,



Michael E. Davis  
Project Director  
OpenCable Business Relations

**CONFIDENTIAL ATTACHMENTS  
TO THIS EXHIBIT  
HAVE BEEN FILED  
IN A SEPARATE ENVELOPE**

## ***DRIR Product Compliance Letter***

For

**Model:** \_\_\_\_\_ (“**DRIR Product**”)

This Compliance Letter warrants the correct design and distribution of a product that incorporates features capable of being used with cable television services received from a DRI connection (DRIR Product). This letter is intended to address certain (but not all) hardware and testing requirements necessary to the manufacture, marketing and distribution of such DRIR Product. Failure to meet these requirements could result in a breach of the DFAT Technology License Agreement, any corresponding Content Protection System (CPS) Adopter Agreement, as well as a breach of this Compliance Letter. Company agrees that CableLabs and Cable Operators are third party beneficiaries of the any corresponding CPS Adopters Agreement, with respect to Cable Content. As used herein, “Cable Content” means unidirectional cable content that has been transmitted from a cable headend or otherwise over the cable system to a unidirectional digital cable product (UDCP) licensed to use DFAST Technology, and through one or more DRI connectors.

Company, via the corporate officer identified below, hereby promises, represents and warrants to CableLabs and Cable Operators that:

1. Company had read and reviewed Exhibit B-1 of the DFAST Technology License Agreement, and hereby certifies that the DRIR Product identified above is in compliance therewith..
2. The DRIR Product identified above has passed the DRI Product Tests provided by CableLabs for DRI Adopters, and DRI Adopter has participated in a DRI Plug Fest.
3. Access to Cable Content on a DRIR Product is limited to applications of Company only; no third party applications have access to Cable Content.
4. In no event shall Company's breach of this Compliance Letter give rise to liability to CableLabs or any Cable Operator, nor shall CableLabs or a Cable Operator be liable to Company, for consequential, incidental, special, indirect, punitive, or exemplary damages of any kind, including without limitation loss of profit, savings, or revenue, or the claims of third parties, whether or not advised of the possibility of such loss, however caused and on any theory of liability, arising out of this Compliance Letter or based on the making, using, selling or importing of any DRIR Product. In no event shall either Company or CableLabs be liable to the other (or a Cable Operator) under any circumstances under this Compliance Letter for any amount that exceeds \$1,000,000 per instance of breach. As used herein, “instance” shall be defined as a breach attributable directly or indirectly to one cause (including a series of similar problems related to a single cause) and may, for example, affect multiple models or DRIR Products sharing a common chassis. The foregoing limitation of

liability shall not apply in the case of Company's failure to meet applicable regulatory requirements imposed by the FCC as provided in Section 4 of this Compliance Letter.

- The foregoing limitation of liability in no way limits or otherwise affects the rights of CableLabs or a Cable Operator to seek injunctive relief against Company for a breach of this Compliance Letter. Company acknowledges that material breach of any obligation under this Compliance Letter will cause CableLabs, and/or the Cable Operators, to suffer immediate and irreparable harm and damage for which money alone cannot fully compensate. Company therefore agrees that upon such material breach, CableLabs shall be entitled to entry of a temporary restraining order, preliminary injunction, permanent injunction or other injunctive relief, without posting any bond or other security, compelling Company to comply with such obligations as deemed proper by a court of competent jurisdiction, provided, however, that neither CableLabs nor a Cable Operator may seek injunctive relief unless such party has first provided Company with notice. This paragraph shall not be construed as an election of any remedy, or as a waiver of any right available to either party under this agreement or the law, including the right to seek damages, nor shall this paragraph be construed to limit the rights or remedies available under applicable law for any violation of any provision of this Agreement.

Note: Company shall maintain records indicating such compliance and testing, and shall make such records available to CableLabs on reasonable request.

Corporate Officer: _____	Project Manager: _____
Title: _____	Title: _____
Phone: _____	Phone: _____
Fax: _____	Fax: _____
E-Mail: _____	E-Mail: _____
Address: _____	Address: _____
_____	Signature: _____
Signature: _____	Date: _____
Date: _____	

Quality Assurance: _____
Title _____
_____
Phone: _____
Fax: _____
E-Mail: _____
Address: _____
<b>Signature:</b> _____
Date: _____

## DTLA Side Letter

- **IP Statement.** DTLA, its Founders, and Content Participants, hereby acknowledge that transcoding copy protection states that are not prohibited by FCC encoding rules satisfies the quitclaim conditions to the IP Statement. No subsequent change by DTCP shall trigger a right of action.
- **FCC Compliance.** DTLA agrees to provide assistance to CableLabs with any regulatory action required of CableLabs or any CableLabs' member with respect to applicable regulatory requirements imposed by the Federal Communications Commission in products that receive Cable Content and use DTCP-IP.
- **VGA.** DTLA agrees to amend its applicable Compliance and Robustness Rules to prohibit the output of Cable Content through a VGA interface in accordance with a schedule to be mutually agreed upon by the consumer electronics, information technology, and content industries.
- **Changes in DTCP.** DTLA commits, that future changes to the technology specification(s), or amendments to the DTCP Adopters Agreement, including side letters, Exhibits, or waivers, will ensure against reductions in security for Cable Content, and not diminish the protections afforded to Cable Content. Any technical or legal changes that are material and substantial in nature, must be submitted to CableLabs for approval. Material changes shall include, but are not limited to: (1) mapping to a new transport or media; (2) changes in the encoding or treatment of Controlled Content; (3) changes that may have a material and adverse effect on the integrity or security of the technology; (4) changes in the cryptographic method used, except where the algorithm is unchanged and only the key length is expanded; (5) changes in the scope of redistribution; and (6) any fundamental change in the nature of the technology.

## **EXHIBIT 9**

## Initial Questions on Exhibit B-1

DTLA appreciates the desire of CableLabs to grant approval to DTCP-IP. We set forth below an initial round of questions on your proposed Exhibit B-1. Based on your responses to these questions, we anticipate additional more detailed questions and comments.

1. We have several questions with respect to the definition of "Cable Content."
  - a. A small point, but the use of "unidirectional cable content" in the beginning of the definition renders it circular. Is the intention "audio and audiovisual content transmitted from a cable headend to a UDCP," as used in the DFAST License?
  - b. What is the meaning of "transmitted from a cable headend or otherwise over the cable system"? Are there circumstances in which content is transmitted "over the cable system" but not from "a cable headend"?
  - c. What is the security-related reason to define "Cable Content" only for use with IP? There is no such definition in the DFAST license for example with respect to 1394.
  - d. Similarly, what is the security-related reason that content is required to be "marked as Cable Content" only when used with IP, while the same content transmitted over 1394 is not required to be so marked?
2. Does CableLabs intend that DRI will be the only interface approved for transmitting Cable Content over IP from the first device in the home that receives content from the cable headend?
3. Does CableLabs intend that DRI will be the only interface approved for transmitting Cable Content over IP from *any* device? Or can content that originates from the cable headend be output by a downstream device using an IP-based interface other than DRI? For example, could a HDD or DVD Recorder that received and recorded content from a DRI product then output that recorded content using a different IP interface enabled with DTCP-IP? How does Exhibit B-1 affect the ability of a DTCP-IP enabled device to output content using a DTLA-approved protection technology, such as over an HDMI or DVI interface protected with HDCP?
4. Can DRI be used to output over an IP-based network content that does not originate from a cable headend?
5. How does a downstream device know whether a particular piece of audiovisual content is "Cable Content"? Will the content be "marked as cable content" when transmitted from cable headend? What currently available specification defines how to mark content as "Cable Content"? Does this mean that a downstream device cannot output "Cable Content" to an interface protocol that cannot mark the content as to its source in a persistent manner? Does this mean that content "marked as cable content" cannot be output at any point downstream to a device that can not detect

such marking, regardless of whether the device provides the protections otherwise required by the relevant CCI?

6. Does the current definition of "Cable Content" intend that such content will remain "Cable Content" even after being converted to analog form in a downstream device?
7. In the second part of the definition of "DRIR Product":
  - a. What does the phrase "designed for receipt of Cable Content" mean? Does it mean designed "solely" for the receipt of Cable Content?
  - b. Similarly, what is the intention of the phrase "however connected"? Is a wireless adapter that is capable of receiving content via DTCP-IP, but then outputs the content to the display device as analog output "designed for receipt of Cable Content"?
8. What is the definition of "User Accessible Bus" applicable to Exhibit B-1? Do the requirements of section 3.5 differ from the requirements imposed upon a User Accessible Bus under the DTLA Adopter Agreement; and if so, how? Are these requirements imposed by CableLabs only on IP interfaces or on all interfaces under the DFAST license?
9. What is the intended difference between 3.7(a) and (d)?
10. How does the DRIT Product know whether a manufacturer has provided a Compliance Letter to CableLabs?
11. What does "user presentation" mean? Do the user presentation requirements in 4.5 apply to devices that have LED displays of the type generally found on CE products? The content in this context is uni-directional content. If the problem occurs in the connection between the receiving device and the video monitor, how are these messages to be displayed?
12. Please explain the reasons why it is necessary or appropriate to impose user presentation requirements on downstream devices. The content in this context is uni-directional content. Would it not be sufficient to impose obligations on the DRIT to send an error message to the display if there is an error condition along the network?
13. Please confirm that the encoding for DTCP-IP set forth in Exhibit B-1 is exactly the same encoding as that provided for that content in the DTCP Content Participant Agreement.

# **EXHIBIT 10**

Dear Seth,

Based on the form and substance of the questions you posed on April 20, we conclude that DTLA member companies are still uncertain about the elements and scope of our digital output review process, as well as the product requirements applicable to the digital cable environment. We think a contextual backdrop is worth describing to help DTLA and its members better understand how the “ecosystem” of UDCP approved outputs works, and how DTCP-IP can fit within that ecosystem. We believe that our responses to your technical questions are included below, and we will make ourselves available to discuss all of these issues with you, at your request. In addition, we have a number of questions for DTLA which are also included below.

### **SCOPE OF CABLELABS’ REVIEW PROCESS**

First, we want to reiterate that the scope of our review for new digital outputs is not limited solely to security issues. In addition to security issues, our review process encompasses the submitter's technology licensing terms and obligations, as well as the ability of the submitted technology to deliver cable services. As a competitive distributor of content and services, cable and its content suppliers have a keen interest in ensuring that the service is rendered properly to the subscriber. Failure to render the cable service as intended results in a bad user experience, great difficulty in providing customer support, and a significant resource drain on cable operators faced with answering calls related to issues that could have been addressed in the initial implementation of the technology. Proper implementation of QoS, MMI, EAS, Closed Captioning, V-Chip, and language identification on devices that receive cable content are a few examples. Because of these service-related issues, the UDCP device must meet the obligations of the DFAST agreement, including proper rendering of cable services, in addition to meeting the requirements for content protection. These requirements must be addressed up-front in the approval of the output. Unlike other uses of content protection where the content provider has complete control over the content distribution and medium at the “point of sale” (e.g., AAC3, CSS, MovieLink, CinemaNow, etc.), cable is a “live” service that must address service delivery issues along with content protection issues. Our process for approval of other outputs has taken these cable service issues into account. Our proposal for approval of DTCP-IP is modeled on these other output approvals. Even in the case of OpenCable approval of DTCP over 1394, we addressed cable-specific implementation issues, up front, in adjunct specifications (see SCTE 26, CEA 775-B , CEA 931-B ).

Cable and its content suppliers are also particularly concerned about IP-based outputs. IP enables content, for which cable operators are contractually obligated to protect, to be exchanged among devices and over the Internet in a much more fluid and seamless fashion than other outputs. Because of this, it's necessary to define "Cable Content" as we have for IP outputs to ensure that content controls asserted by cable operators, including localization controls, are applied to all content appropriately and not just "Controlled Content" marked as Copy Once or Copy Never. We are applying the definition of Cable Content consistently to all new IP outputs being submitted for approval, but have not taken any steps to apply this broader definition to the 1394 output since localization is inherently part of that technology.

DTLA and its content participants have uniquely addressed similar copy protection and distribution issues for non-cable environments in the past by amending its specifications and agreement, as it did with the addition of the EPN bit and broadcast flag requirements. We see no

reason why DTLA cannot make similar adjustments in the case of CableCARD-enabled products that receive uni-directional cable content. (Unidirectional cable content is the one-way linear, non-interactive cable services that are available to UDCPs, not simply the audio and audiovisual content received by a UDCP.) Proximity, HDCP control, image constraint, and certain other copy protection/distribution limitations are included in our proposal, and are consistent with our approval of other IP-based solutions such as Microsoft's WMDRM and Real Network's Helix DRM. We see no reason why DTCP should be given preferential treatment; rather, we consider DTCP-IP to be part of a TV tuned to a cable service. To the extent that this raises issues other than strictly "security" issues, we are happy to work with DTLA to address them.

#### **AUTHORIZED OUTPUTS WITHIN THE UDCP ENVIRONMENT**

All devices within the cable ecosystem must be capable of properly acquiring, storing, processing, streaming, consuming, or outputting cable content, as applicable, while maintaining the integrity of a conditional access distribution network, and without disrupting, impeding or impairing the delivery of services to a cable customer. This includes the obligation of the product manufacturer to ensure that the product does not interfere with the delivery of the cable services (audio, video, data, etc.) as the cable operator intended those services to be delivered, as well as to ensure that the product does not put at risk, among other things, the conditional access system, copy protection (including re-distribution or localization) controls, entitlements, or content usage rules.

One purpose of the authorized output approval process is to ensure that all connected devices within the "ecosystem" respect the entitlements and usage rights assigned to the content by the cable network operator within a single cable customer's home or network. In this regard, we do not intend for UDCPs to operate as devices that "hand off" cable content as IP files that may disregard those entitlements and usage rights. Once content is received as "Cable Content," it is always considered cable content and can be used within a single subscriber's home or network, however connected. Although device interoperability within the UDCP ecosystem is highly desired and recommended, interoperability is not essential to gaining approval for a submitted technology.

DTLA seemed to dismiss cable service issues entirely in its proposal of March 14. DTLA has refused to make any changes to its Adopter Agreement, and the only requirement suggested for an upstream source device was to act as a "format-cognizant real-time-delivery content source/decoding device" (as defined by the DTCP Specification). If we read the DTCP Specification correctly, DTLA is actually proposing that the cable UDCP device completely ignore CCI states set by the cable operator in accordance with contractual MSO programming agreement obligations. Rather, the device is to look in the content stream for the DTCP CCI states. This arrangement would seem to promote a complete bypass to cable content protection, and a complete disregard for the legitimate service delivery obligations and concerns of the cable industry--obligations to both our content providers on one end and our subscribers on the other.

Because DTLA rejected our proposal to make changes in the DTCP Adopters Agreement to address cable concerns, we proceeded in accordance with DTLA's suggestion to make the changes in the "upstream" DFAST license. The "mapping" of content protection settings in our proposal is identical to other IP-based outputs that we've approved, and applies to all Cable Content delivered over IP. But, because the DTCP license does not account for cable concerns, it is necessary for the device with the CableCARD to identify and mark Cable Content using technical measures, and ensure that all connected devices maintain that marking. This is not

unlike DTLA's modification of the DTCP license to accommodate content marked with the broadcast flag. Nevertheless, the result, we believe, is exactly what DTLA asked for – DTCP-IP approval for devices licensed under DFAST—and is consistent with all other approvals over IP.

Our guidelines for output approvals envision that submissions are made by actual product implementers, not pure technology purveyors that may not be fully vested in ensuring that a quality video service is delivered intact to the subscriber who paid for it. We are working with DTLA to try to approve DTCP-IP in the abstract, but we have to think through all the implementations and implications, such as making sure that presentation requirements flow to all downstream devices. It is DTLA's rejection of any effort to adjust its license that leads us to place such obligations directly on the implementer.

Another fundamental purpose of the authorized output approval process for UDCPs is to enable protection of high value cable TV services distributed to a single home cable subscriber account. IP-based authorized outputs are particularly appealing as they enable such protected services to be delivered across a home or personal network. Within this ecosystem it is necessary for content to be marked as Cable Content to help achieve effective localization within the cable customer's home and personal network. For this reason, a DRIT device, or any device with a DRIT function, is prohibited from outputting Cable Content to a DRIR device if the DRIR device cannot detect and maintain the Cable Content marking. However, a DRIT device, or a device with a DRIT function may output Cable Content to display devices that fully consume the content, or other devices having authorized protected outputs as identified in the DFAST Technology License. If product manufacturers wish to have their devices receive high value content and services within this UDCP ecosystem of authorized IP outputs, they must undertake these obligations to protect content and services. It is expected that parties bring their devices up to the standard of the applicable license and platform, including marking the content as Cable Content -- that is part of the responsibility of equipment providers.

The CableLabs' digital output approval process enables any party to submit technologies as proposed authorized outputs for UDCPs. To further that purpose, we do not anticipate limiting any submitter to only DRI-based solutions. Because the submission from DTLA did not address any of the video transport issues as required by the applicable submission guidelines, CableLabs embarked on a cooperative and collaborative effort with you to create a suitable specification that would address such cable transport issues for DTCP-IP, as well as other IP-based content protection solutions. The result of this input from DTLA (and Intel directly) was a set of changes to the DRI specification, which CableLabs subsequently adopted and published. Although we do not intend to require DRI for all future IP-based content protection technologies, we believe that the DRI solution is a good solution for IP-based submissions, and lends itself to product interoperability. Similar to the SCTE-26 standard that applies to the DTCP-protected IEEE-1394 outputs, the DRI specification resolves most of the video transport issues that are critically important to the cable industry.

The "DRI Content Protection Requirements" table included in our Exhibit B-1 addresses how a DTCP-IP enable device could further output Cable Content downstream using such authorized outputs for UDCPs. As the table shows, a DRIT or DRIR device would be able to output Cable Content through *any* authorized digital output identified in the DFAST Technology License. This would include DTCP-IP over DRI, DTCP over 1394, HDCP over DVI or HDMI, several recording technologies, and any other output that we may approve for UDCPs in the future. The CableLabs authorized output approval process is not directly impacted or influenced by DTLA's approval process for outputs, just as DTLA's approval process is not impacted or

influenced by ours. Based on your previous communication to us, we understand that DTLA is reluctant to make changes to the DTCP specification change process, which would include the approval of new technologies, or licensing provisions to specifically address cable concerns. Responding to that message, we are now taking the approach that our two approval processes and licensing regimes must remain separate. That said, we believe there are synergies and interoperability benefits to be gained by continuing to cooperate with each other and monitor each other's progress and changes in the approval of new digital outputs, as we've done in the past.

Neither CableLabs nor the cable industry are opposed to the widespread adoption of DRI,. CableLabs has made the spec publicly available, and does not charge any fees or royalties to any implementer. Therefore, DRI may be used to output over an IP-based network content that does not originate from a cable headend.

I believe the above explanation addresses most of your questions and will help DTLA understand how DTCP-IP can fit in the UDCP "ecosystem," but a few of the remaining technical issues are addressed specifically below. In addition to our responses, we've included several reply questions to help us better understand how DTLA wants to proceed at this point. As we stated in our letter of March 29, CableLabs is prepared to finalize the approval of DTCP-IP with the conditions and obligations being placed on the UDCP through the proposed Exhibit B-1 to the DFAST Technology License. From our point of view, there are no remaining issues in this Exhibit that need to be resolved between CableLabs and DTLA prior to our final approval of DTCP-IP, but we are more than happy to continue discussions with you , at your request. Our goal is to work with DTLA to get DTCP-IP approved as soon as possible for use within the authorized output environment for UDCPs. We continue to think we can find a solution that works for both parties.

Sincerely,

Judson D. Cary  
Deputy General Counsel  
Cable Television Laboratories, Inc.

## Specific Responses to Technical Questions

**Question 1(a):** A small point, but the use of "unidirectional cable content" in the beginning of the definition renders it circular. Is the intention "audio and audiovisual content transmitted from a cable headend to a UDCP," as used in the DFAST License?

**Response to Question 1(a):** Refer to explanatory letter. "Cable Content" is the one-way linear, non-interactive channels that are available to a UDCP.

**Question 1(b):** What is the meaning of "transmitted from a cable headend or otherwise over the cable system"? Are there circumstances in which content is transmitted "over the cable system" but not from "a cable headend"?

**Response to Question 1(b):** Not yet, but we are trying to anticipate more modular or distributed approaches.

**Question 1(c):** What is the security-related reason to define "Cable Content" only for use with IP? There is no such definition in the DFAST license for example with respect to 1394.

**Response to Question 1(c):** Refer to explanatory letter.

**Question 1(d):** Similarly, what is the security-related reason that content is required to be "marked as Cable Content" only when used with IP, while the same content transmitted over 1394 is not required to be so marked?

**Response to Question 1(d):** Refer to explanatory letter.

**Question 2:** Does CableLabs intend that DRI will be the only interface approved for transmitting Cable Content over IP from the first device in the home that receives content from the cable headend?

**Response to Question 2:** Refer to explanatory letter.

**Question 3:** Does CableLabs intend that DRI will be the only interface approved for transmitting Cable Content over IP from *any* device? Or can content that originates from the cable headend be output by a downstream device using an IP-based interface other than DRI? For example, could a HDD or DVD Recorder that received and recorded content from a DRIT product then output that recorded content using a different IP interface enabled with DTCP-IP? How does Exhibit B-1 affect the ability of a DTCP-IP enabled device to output content using a DTLA-approved protection technology, such as over an HDMI or DVI interface protected with HDCP?

**Response to Question 3:** Refer to explanatory letter. Also refer to the DRI Content Protection Requirements table in Exhibit B-1.

**Question 4:** Can DRI be used to output over an IP-based network content that does not originate from a cable headend?

**Response to Question 4:** Yes.

**Question 5:** How does a downstream device know whether a particular piece of audiovisual content is "Cable Content"? Will the content be "marked as cable content" when transmitted from cable headend? What currently available specification defines how to mark content as "Cable Content"? Does this mean that a downstream device cannot output "Cable Content" to an interface protocol that cannot mark the content as to its source in a persistent manner? Does this mean that content "marked as cable content" cannot be output at any point downstream to a device that can not detect such marking, regardless of whether the device provides the protections otherwise required by the relevant CCI?

**Response to Question 5:** Refer to explanatory letter.

**Question 6:** Does the current definition of "Cable Content" intend that such content will remain "Cable Content" even after being converted to analog form in a downstream device?

**Response to Question 6:** The "DRI Content Protection Requirements" table in Exhibit B-1 addresses the mapping of Cable Content to analog outputs. We would not expect existing analog output protection technologies to change in order to respond to the Cable Content markings applicable to digital outputs.

**Question 7, subparts a and b:** In the second part of the definition of "DRIR Product":

**Question 7(a):** What does the phrase "designed for receipt of Cable Content" mean? Does it mean designed "solely" for the receipt of Cable Content?

**Response to Question 7(a):** No

**Question 7(b):** Similarly, what is the intention of the phrase "however connected"? Is a wireless adapter that is capable of receiving content via DTCP-IP, but then outputs the content to the display device as analog output "designed for receipt of Cable Content"?

**Response to Question 7(b)** Yes, if the wireless adapter is receiving Cable Content.

**Question 8:** What is the definition of "User Accessible Bus" applicable to Exhibit B-1? Do the requirements of section 3.5 differ from the requirements imposed upon a User Accessible Bus under the DTLA Adopter Agreement; and if so, how? Are these requirements imposed by CableLabs only on IP interfaces or on all interfaces under the DFAST license?

**Response to Question 8:** We presume you mean section 3.6 of Exhibit B-1. The User Accessible Bus (UAB) language in Section 3.6 of Exhibit B-1 is in addition to the UAB language in Exhibit C, Paragraph 2 of the DFAST Technology License. Both of these provisions would apply to DRIT and DRIR devices.

**Question 9:** What is the intended difference between 3.7(a) and (d)?

**Response to Question 9:** Refer to explanatory letter.

**Question 10:** How does the DRIT Product know whether a manufacturer has provided a Compliance Letter to CableLabs?

**Response to Question 10:** The manufacturer of the DRIT product is expected to establish procedures to assure that a Compliance Letter has been sent to CableLabs.

**Question 11:** What does "user presentation" mean? Do the user presentation requirements in 4.5 apply to devices that have LED displays of the type generally found on CE products? The content in this context is uni-directional content. If the problem occurs in the connection between the receiving device and the video monitor, how are these messages to be displayed?

**Response to Question 11:** As discussed above, implementers are expected to bring their devices up to the standard of the applicable license and platform. This includes the obligation for a DRIR device to notify the user of network problems that may be interfering with delivery of the cable service. The example you provide - a problem in the connection between the receiving device and the video monitor - is exactly the type of problem that our approval process intends to address. This problem would be considered a catastrophic failure within the cable environment, as such a problem would prevent proper authorization of the CableCARD and any cable services, as well as prevent cable delivery of EAS messages, content ratings, and closed captioning. If a technology submitter fails to address such service delivery problems for IP outputs, or any other type of output, approval of the technology for use in the cable environment becomes an intractable problem. To alleviate this intractability, CableLabs has developed the DRI specification and has made it available to submitters of IP-based content protection to address such cable concerns.

**Question 12:** Please explain the reasons why it is necessary or appropriate to impose user presentation requirements on downstream devices. The content in this context is uni-directional content. Would it not be sufficient to impose obligations on the DRIT to send an error message to the display if there is an error condition along the network?

**Response to Question 12:** Refer to explanatory letter.

**Question 13:** Please confirm that the encoding for DTCP-IP set forth in Exhibit B-1 is exactly the same encoding as that provided for that content in the DTCP Content Participant Agreement.

**Response to Question 13:** Our requirements for all IP-based outputs are described in Exhibit B-1, including the DRI Content Protection Requirements attached thereto. If there is anything in DTLA's content protection system that does not comply with these requirements, please let us know.

## Reply Questions from CableLabs to DTLA

1. We understand from your letter of March 14 that, *"In other contexts in which DTCP-IP has received approval from third parties for use with respect to protected content from particular sources, the approvals have been accompanied by a set of "Associated Obligations." These Associated Obligations specify the particular settings required in the Source Function so as to trigger correctly the specified level of protection via DTCP-IP. Associated Obligations therefore are to be included in the licenses for the technologies that provide the source content."*
  - a. Does DTLA find anything in the DRI Content Protection Requirements table in our Exhibit B-1 that fails to specify the particular settings required in the source function to correctly trigger the specified level of DTCP-IP protection?
  - b. If DTLA has accepted Associated Obligations on the source content license in other contexts, why cannot DTLA agree to such obligations in this case?
  - c. Does the DRI Content Protection Requirements table in our Exhibit B-1 specify any particular content protection settings that DTCP-IP is incapable of providing?
2. We also understand from your letter of March 14 that, *"DTLA's licenses do not cover or dictate the elements of any of the underlying protocols over which DTCP may operate, and do not impose any requirements with respect to the operation of services across those protocols. Any such requirements lie beyond the scope of content protection technology, and so cannot be encompassed within a license for DTCP."*
  - a. Do the members and content participants of DTLA agree that requirements related to cable services protected by DTCP lie within the scope of the licenses applicable to the devices receiving such content services?
  - b. How does DTLA and its members propose to address the "operation of services" across the protocol to meet the service expectation level of a typical cable subscriber (QoS, EAS, Closed Captioning, delivery of MMI, etc)? Cable, of course, has their individual subscriber agreements to live up to.
3. Is there any portion of our proposed Exhibit B-1 (including, among other things, QoS, Emergency Alert Messaging, Closed Captioning, and delivery of MMI messages) that DTLA would consider as *not* being an "upstream" obligation, as described in your letter of March 14?
4. Do the DTCP specifications address a format-cognizant real-time-delivery content source/decoding device that is equipped with a CableCARD, and is capable of receiving CCI messages and EMI settings via out-of-band signaling from the cable operator?
5. From our point of view, the only outstanding issues that need to be resolved prior to our approval of DTCP-IP are outlined in the revised "DTLA Side Letter" that we sent to you on April 7. Does DTLA have any specific questions or requested changes to the proposed terms of the side letter?