DTCP2 DIGITAL TRANSMISSION PROTECTION LICENSE AGREEMENT
Evaluation License Convertible to Product License

This DTCP2 DIGITAL TRANSMISSION PROTECTION LICENSE AGREEMENT, ("Agreement") is effective as of the latest date set out on the signature page hereof (the "Effective Date") by and between Digital Transmission Licensing Administrator, LLC, a Delaware limited liability company ("DTLA") and the "Adopter" which is named immediately below:

Name of Adopter:	
Description of Adopter's Business	
Location of Principal Office:	
Jurisdiction of Adopter's Formation:	
Year of Formation:	
Number of Employees:	
Amount of Capital:	

BACKGROUND

A. The Founders have developed a certain enhanced method for encryption, decryption, key exchange, authentication, and renewability for purposes of protecting certain digital content from unauthorized interception, retransmission and copying.

B. The Founders have licensed the method to DTLA for purposes of further licensing the system and administering such licenses.

C. Adopter wishes to receive a license, subject to the terms and conditions set forth in this Agreement for the purpose of developing and evaluating such method including, but not limited to, adherence to the Compliance Rules.

Therefore, DTLA and Adopter agree as follows:

AGREEMENT

1. DEFINITIONS.

In addition to terms defined elsewhere in this Agreement (including in the Exhibits hereto), the following terms shall have the following meanings. All definitions herein shall apply equally to their singular and plural forms, all pronouns shall apply without regard to gender, and all references to Sections and Exhibits shall be deemed to be references to Sections of, and Exhibits to, this Agreement unless the context shall otherwise require.

1.1 "**Activation"** means that the Adopter has executed the Activation Notice and has paid the fees referenced in Section 2.2, which are required to activate the Adopter's manufacturing license.

1.2 **"Adopter"** means the entity named at the beginning of this Agreement and includes its Affiliates.

1.3 "**Adopter ID**" has the meaning given in the DTCP2 Specification.

1.4 **"Affiliate"** means with respect to any person or entity, any other person or entity directly or indirectly controlling or controlled by or under direct or indirect common control with such person or entity. "Control" means the possession of beneficial ownership of more than 50% of the stock or other similar interest entitled to vote for election of the Board of Directors or similar managing authority.

1.5 **"Commercial Entertainment Content"** is defined in the Compliance Rules.

1.6 **"Common Device Key and Common Device Certificate"** means a common DTCP2 Device Key and common DTCP2 Device Certificate as contemplated in Section 2.2 of the Procedural Appendix.

1.7 **"Compliance Rules"** means both the requirements set out in Exhibit B and the Robustness Rules set out in Exhibit C, as such exhibits may be amended by DTLA from time to time pursuant to Section 3.3.

1.8 **"Compliant"** refers to a product that is in compliance with all applicable Compliance Rules and, in the case of a product that incorporates a common DTCP2 Device Key or common DTCP2 Device Certificate, is also in compliance with Section 2.2 of the Procedural Appendix.

1.9 **"Confidential Information"** means Proprietary Information that is either marked "confidential" or "proprietary" when disclosed in written form or indicated as "confidential" or "proprietary" when disclosed orally and confirmed in writing within thirty (30) days after such disclosure.

1.10 **"Content Participant"** means a company that has executed a Content Participant Agreement with DTLA, or with an entity authorized by DTLA to execute such agreements. DTLA will identify such companies periodically.

1.11 **"Content Participant Agreement"** means any Content Participant Agreement and any addendum thereto entered into by a provider of Commercial Entertainment Content and DTLA or any entity authorized by DTLA to execute a Content Participant Agreement.

1.12 **"DTCP1"** that certain method for encryption, decryption, key exchange, authentication and renewability for purposes of protecting certain digital content from unauthorized interception and copying which method is described in the DTCP1 Specification.

1.13 **"DTCP1 Adopter"** means an entity that licenses DTCP1 under a DTCP1 Adopter Agreement, for so long as such agreement between such entity and DTLA remains in effect.

1.14 **"DTCP1 Specification"** means the specification entitled "5C DTCP Digital Transmission Content Protection" release 1.0 and subsequent releases adopted by DTLA and licensed by DTLA under the "Digital Transmission Protection License Agreement" for DTCP1 (the "**DTCP1 Adopter Agreement**").

1.15 "**DTCP2**" means that certain method for encryption, decryption, key exchange, authentication and renewability for purposes of protecting certain digital content from unauthorized interception and copying which method is described in the DTCP2 Specification.

1.16 **"DTCP2 Adopter Agreement"** means this Agreement and any other DTCP2 Digital Transmission Protection License Agreement entered into by DTLA and any other adopter of DTCP2.

1.17 **"DTCP2 Associates"** means entities that have executed an agreement relating to the handling and redistribution of Licensed Components and who are designated as DTCP2 Associates by DTLA. DTLA will identify such entities periodically.

1.18 **"DTCP2 Device Certificate"** means a cryptographically encoded value that may be provided by DTLA or its designee under a DTCP2 Adopter Agreement and that authorizes a DTCP2 Licensed Product to exchange certain Commercial Entertainment Content.

1.19 **"DTCP2 Device Keys"** means cryptographic values that may be provided by DTLA or its designee under a DTCP2 Adopter Agreement for use in DTCP2 Licensed Products, and that includes the "DTCP2 Private Device Key" and the "DTCP2 Public Device Key" as identified in the DTCP2 Specification.

1.20 **"DTCP2 Specification"** means the specification entitled "5C DTCP2 Digital Transmission Content Protection" release 1.0 as may be amended from time to time pursuant to Section 3.3.

1.21 **"Fellow DTCP2 Adopters"** means the Founders and any other entity that has executed a DTCP2 Adopter Agreement and delivered it to DTLA or its designee.

1.22 **"Founders"** means Hitachi Maxell, Ltd., Intel Corporation, Panasonic Corporation, Sony Corporation, and Toshiba Corporation.

1.23 **"Generator"** means DTLA or an entity that has been retained by DTLA to generate DTCP2 Device Certificates and DTCP2 Device Keys for use by Fellow DTCP2 Adopters.

1.24 **"Highly Confidential Information"** means Proprietary Information that is marked "Highly Confidential Information" when disclosed in written form or is otherwise designated as such hereunder**.**

1.25 "**IKLC**" has the meaning given in Section 7.4.

1.26 "**Implementation**" means the portion of one or more Licensed Products that constitutes a unique combination of technology that embodies the applicable portions of the DTCP2 Specification with the means of compliance with the applicable Compliance Rules and Robustness Rules for such Licensed Products. By way of example only: (i) two Licensed Products that have different model numbers or enclosures, but internally implement DTCP2 (and comply with the Compliance Rules and Robustness Rules) in the same way have the same Implementation; (ii) two different Licensed Products in which Adopter uses chips, sourced from multiple vendors (where each vendor used its own design rather than a common design provided by Adopter), that implement DTCP2 in different ways have different Implementations.

1.27 **"Implementation ID"** has the meaning given in the DTCP2 Specification.

1.28 **"Interface"** means the protocols (including cryptographic algorithms), packet formats, and data structures disclosed in the DTCP2 Specification.

1.29 **"Licensed Component"** means a product, such as an integrated circuit, circuit board, or software module, that is designed to be assembled into a Licensed Product and that embodies a portion of the DTCP2 Specification (including, for avoidance of doubt, a product that incorporates a DTCP2 Device Key or DTCP2 Device Certificate), and that does not embody the entirety of the DTCP2 Specification or does not completely satisfy the Compliance Rules.

1.30 **"Licensed Components with Keying Material"** means a Licensed Component that contains Keying Material, other than an IKLC.

1.31 **"Licensed Product"** means a product, including a hardware device or software application, that:

1.31.1 Embodies the designs set out in the DTCP2 Specification,

1.31.2 Is Compliant, and

1.31.3 Is designed for the transmission and/or receipt of digital transmissions comprising Commercial Entertainment Content.

1.32 **"Necessary DTCP2 Claims"** means claims of a patent or patent application relating to the Interface that must be infringed in order to make a product that complies with the Interface, which are

owned or controlled by DTLA, any Founder, Adopter or any Fellow DTCP2 Adopter, any Content Participant or any of their respective Affiliates. "Necessary DTCP2 Claims" do not include any claims relating to semiconductor manufacturing technology; claims relating to aspects of any technology, standard or product that is not itself part of the DTCP2 Specification (including, by way of example, AACS, CSS, MPEG, and analog copy protection systems) even though such technology, standard or product may otherwise be mentioned or required by the DTCP2 Specification or Compliance Rules; claims with regard to which it would be possible to build a product in compliance with the Interface without infringing such claim (even if in the same patent as Necessary DTCP2 Claims); or claims which, if licensed, would require a payment of royalties by the licensor to unaffiliated third parties.

1.33 **"Procedural Appendix"** means that document of the same name attached hereto which is hereby incorporated into this Agreement by reference, as may be amended by DTLA from time to time.

1.34 **"Proprietary Information"** means any and all information relating to the DTCP2 Specification made available to Adopter directly by DTLA or its designees or representatives, or by any Fellow DTCP2 Adopter including, without limitation, specifications, software, hardware, firmware, documentation, designs, flow charts, technical data, outlines, blueprints, notes, drawings, prototypes, templates, systems, manuals, know-how, processes and methods of operation.

1.35 "**Robust Inactive Product**" means a product or component that (i) does not contain a DTCP2 Device Key, (ii) is designed not to have its DTCP2 functions be activated except by an Update, and (iii) is no less secure from circumvention (including but not limited to modification and/or compromise of Confidential Information or Highly Confidential Information) than Licensed Products are required to be hereunder. By way of example, a product or component consisting of software object code manufactured by Adopter shall be deemed a Robust Inactive Product if (x) if the portions implementing DTCP2 (including any portion of DTCP2) are encrypted using a commercially reasonable strength of encryption and the keys necessary to decrypt and use such portions are not made available to any person or entity other than Adopter and (y) the product or component does not contain a DTCP2 Device Key.

1.36 **"Robust Licensed Component"** means a Licensed Component that is designed to be modified via an Update to become, or designed to be incorporated via an Update into, a Licensed Product and that (i) complies with all applicable Robustness Rules and all other applicable Compliance Rules, (ii) is designed in such a way that unless such Robust Licensed Component is modified to become, or is incorporated into, a Licensed Product by means of Update, such Robust Licensed Component shall not be able to transmit via any digital output any content using DTCP2 or any components thereof, or decrypt or encrypt any content using DTCP2, and (iii) shall upon distribution of such Robust Licensed Component and at such time as such Robust Licensed Component (as distributed) is modified to become, or is incorporated into, a Licensed Product, be no less secure from interception of DTCP2 Device Keys, DTCP2 Device Certificates and Decrypted DT Data, and from circumvention (including but not limited to modification and/or compromise of Confidential Information or Highly Confidential Information) than Licensed Products are required to be hereunder. By way of example, Licensed Components consisting of software object code shall be deemed Robust Licensed Components if the object code is encrypted using a commercially

reasonable strength of encryption and the keys necessary to decrypt and use such code are made available only to Fellow DTCP2 Adopters, DTCP2 Associates and Have Made Parties, or such Licensed Components are capable of being Updated and the DTCP2 functions are only activated when contained in a Licensed Product (i.e., the resultant product meets all of the requirements that a Licensed Product was required to meet at the time the Licensed Components were distributed).

1.37 **"Robustness Rules"** means the requirements set out in Exhibit C, as such exhibit may be amended by DTLA from time to time pursuant to Section 3.3.

1.38 **An "Update"** means, with respect to a Licensed Product or Robust Licensed Component or a Robust Inactive Product distributed by a Fellow DTCP2 Adopter (a "Distributed Adopter Product"), the distribution by a Fellow DTCP2 Adopter of a Licensed Product or Robust Licensed Component (the " Adopter Update") to modify or replace such Distributed Adopter Product (including but not limited to modifications that activate the DTCP2 functions in such Distributed Adopter Product, or replace the DTCP2 Device Certificate or DTCP2 Device Key or the Implementation ID in such Distributed Adopter Product), such that (i) the resultant product (i.e., the Distributed Adopter Product as modified or replaced by the Adopter Update) shall be a Licensed Product or Robust Licensed Component (i.e., shall comply with all of the requirements that Licensed Products or Robust Licensed Components, as the case may be, were required to meet at the time the Distributed Adopter Product was distributed) and (ii) upon distribution of the Adopter Update, and upon modification or replacement of the Distributed Adopter Product, such Adopter Update and Distributed Adopter Product shall be no less secure from interception of DTCP2 Device Keys, DTCP2 Device Certificates and Decrypted DT Data and from circumvention (including but not limited to modification and/or compromise of Confidential Information or Highly Confidential Information) than Licensed Products are required to be hereunder. By way of example but not limitation, an Update may take place by means of an on-line download of a Robust Licensed Component or the distribution of CD-ROM containing a Robust Licensed Component to end-users. For clarification, a "Distributed Adopter Product" and "Update" with respect thereto may be distributed at the same or different times.

2. FEES.

2.1 **Administration and Disclosure Fee**. Within thirty (30) days of the Effective Date, Adopter shall pay DTLA a nonrefundable sum in the amount of the Annual Administration Fee set out in the Procedural Appendix (the "Annual Administration Fee"). Adopter shall not be entitled to any refund thereof for any reason. Adopter shall pay DTLA the "Per DTCP2 Certificate Fees" set out on the Procedural Appendix in accordance with the procedures for ordering DTCP2 Device Certificates and DTCP2 Device Keys or Common DTCP2 Device Certificates and Common DTCP2 Device Keys specified in the Procedural Appendix. Upon each anniversary of the Effective Date, or such other date as specified in the Procedural Appendix (the "Annual Payment Date"), Adopter shall pay DTLA the Annual Administration Fee for the following year (or, in the final year of the Term, such portion of the Annual Administration Fee as is specified in the Procedural Appendix). DTLA may, upon at least thirty (30) days' notice to Adopter, modify the Annual Administration Fee and Per Certificate Fees payable for the period beginning on the next Annual Payment Date, provided that any increase in such fees shall not exceed an amount commensurate with any increase in DTLA's costs (including but not limited to the cost of inflation). Without limiting the foregoing, where costs per DTCP2

Device Key or per Fellow DTCP2 Adopter decrease, DTLA shall use commercially reasonable efforts to reduce the Per Certificate Fee or Annual Administration Fee, respectively.

2.2 **Activation.** At any time after Adopter has paid the Annual Administration Fee for the initial year, or any subsequent year, of the Term for the "Small Adopter" or "Large Adopter" category (as selected by Adopter with reference to the Fee Schedule set forth in the Procedural Appendix), Adopter may execute the Activation Notice attached hereto as Exhibit D in accordance with the procedures set out in Exhibit D. Prior to Activation, Adopter is not licensed to distribute any products or components hereunder, and the provisions of Sections 6.2, 6.3, 6.4, 7.1, 7.2, 7.3, 7.4, 7.5, and 7.6 shall only be applicable after Activation. Any Evaluation Fee (as set out in the Procedural Appendix) which Adopter has paid hereunder for the year in which Adopter elects Activation shall be credited as provided in such Activation Notice against the Annual Administration Fee for such year payable upon Activation.

2.3 **DTCP2 Device Certificate and DTCP2 Device Keys.** DTCP2 Device Certificates and DTCP2 Device Keys are necessary to manufacture Licensed Products. These are generated under the direction of DTLA and, except in the case that Adopter elects to use a Common DTCP2 Device Certificate and Common DTCP2 Device Key for certain devices as described in the Procedural Appendix and Compliance Rules, are generated uniquely per device. Without limiting any other provision of this Agreement, Adopter may not use the same DTCP2 Device Key or DTCP2 Device Certificate in more than one individual unit or copy of any product or component except for the use of Common DTCP2 Device Keys and Common DTCP2 Device Certificates in accordance with Section 2.2 of the Procedural Appendix. Following Activation, DTCP2 Device Keys and DTCP2 Device Certificates shall be made available according to the fee schedule set out in the Procedural Appendix, as updated from time to time in accordance with the terms of this Agreement. Prior to Activation, facsimile DTCP2 Device Certificates and facsimile DTCP2 Device Keys shall be issued to Adopter for development purposes. Adopter is cautioned that such facsimile cryptographic materials will not inter-operate with commercial devices. Without limiting any other provision of the Agreement, Adopter may replace or cause the replacement of DTCP2 Device Certificates and DTCP2 Device Keys by Update.

2.4 **Implementation IDs.** DTLA shall make available to Adopter an Adopter ID to be used in an Implementation ID that uniquely identifies the particular Implementation in Adopter's Licensed Products. DTLA shall issue to Adopter facsimile Adopter IDs that Adopter may use for development purposes. Adopter is cautioned that such facsimile materials will not interoperate with commercial devices. Following Activation, Adopter IDs shall be made available in accordance with the Procedural Appendix.

3. DTCP2 SPECIFICATION; COMPLIANCE RULES; USERS GROUP.

3.1 **Delivery**. Upon Adopter's execution hereof and DTLA's receipt of the applicable fee(s), DTLA shall cause to be distributed to Adopter the relevant portions of Proprietary Information and/or the DTCP2 Specification that Adopter has not previously received.

3.2 **Acknowledgement.** Adopter agrees to provide copies of the DTCP2 Specification, Compliance Rules and Robustness Verification List to those persons having supervisory

responsibility for the design and manufacture of Licensed Products and Licensed Components for and on behalf of Adopter, in such manner and at such times as to promote Adopter's compliance with all applicable terms thereof.

3.3 **Changes.** The DTCP2 Specification and the Compliance Rules may be amended from time to time by DTLA only in accordance with this Section 3.3. Adopter shall be required to comply with all amendments (a) to the Compliance Rules and Section 2.2(i)(y) of the Procedural Appendix within twelve (12) months after notification of the changes has been sent as specified herein or, in extraordinary cases, within such shorter or longer period specified by DTLA and (b) to the DTCP2 Specification within eighteen (18) months after such notice. Changes in the Procedural Appendix, with the exception of changes to Section 2.2(i)(y), the Annual Administration Fees and Per Certificate Fees, shall be effective on no less than thirty (30) days' notice. Changes to the Annual Administration Fees or Per Certificate Fees shall be permitted only as set out in Section 2.1. In the case of individual units or copies of Robust Licensed Components, Robust Inactive Products or of Licensed Products that are capable of being Updated and are shipped by Adopter after the effective date of such amendment, the requirements of this Section 3.3 may be met by ensuring that the required changes are implemented in such Robust Licensed Components, Robust Inactive Products and Licensed Products through an Update by or at the direction of Adopter before the DTCP2 functions of such Licensed Products, Robust Inactive Products and Robust Licensed Components may be used for the first time. Notwithstanding the foregoing, in the event Adopter issues, after the effective date of any such amendment, an Update to a Licensed Product or Robust Licensed Component or Robust Inactive Product that was distributed prior to the effective date of such amendment, the Update and the Licensed Product or Robust Licensed Component or Robust Inactive Product as Updated shall not be required to comply with such amendment, provided that it (a) is not a Different Licensed Product, (b) complies with all applicable provisions of the DTCP2 Specification and Compliance Rules in effect at the time such Licensed Product or Robust Licensed Component or Robust Inactive Product was distributed, and (c) where applicable, complies with Section 3.5.

For purposes of this Section 3.3, a "Different Licensed Product" means, with respect to an Update applied to a Licensed Product, a resulting Licensed Product that is the same as a Licensed Product that (x) is separately marketed by Adopter under a new product name or a higher numerical designation to the left of the decimal point (e.g., the change from Version 1.0 to Version 2.0, but not to Version 1.9), and (y) either--

(i) enables DTCP2 protection of a service that would not have been protectable with DTCP2 by the Licensed Product prior to the Update, or

(ii) performs the DTCP2 functions by substantially different means and in a substantially different way than was performed by the Licensed Product prior to the Update.

3.3.1 DTLA shall not make any material changes to the DTCP2 Specification (including any changes that would expand the DTCP2 Specification to require new technical features, not included in version 1.0 of the DTCP2 Specification or such later version of the DTCP2 Specification as may be in effect as of the Effective Date, that would create compatibility problems with Licensed Products manufactured prior to such changes), provided, however, that DTLA may make such limited changes, if any, in the DTCP2

Specification as would permit DTCP2 to be used with protocols and/or transports other than those permitted in version 1.0 of the DTCP2 Specification. Without limiting the foregoing, DTLA reserves the right to correct any errors or omissions in the DTCP2 Specification or to make changes that would clarify, but not materially amend, alter or expand the DTCP2 Specification, from time to time.

3.3.2 Adopter shall manufacture all Licensed Products that implement revocation with the capacity to store, in accordance with the provisions of this Agreement, a revocation list of no less than 16 kilobyte (16 KB) as set forth in Section 8.1 of the DTCP2 Specification.

3.3.3 Except as DTLA, in consultation with owners of Commercial Entertainment Content, may conclude is necessary to ensure and maintain content protection, DTLA shall not make any revisions to the Compliance Rules that would materially increase the cost or complexity of implementations of Licensed Products. Without limiting the foregoing, DTLA shall provide the members of the CPIF (defined in Section 3.4) with at least thirty (30) days' notice of any material changes to the Compliance Rules.

3.4 **Content Protection Implementers Forum.** Adopter has the right to be a member of and to participate in a Content Protection Implementers Forum ("CPIF"), which DTLA shall convene, with which it may exchange views and information regarding DTCP2. Members of the CPIF will have the right to participate in interoperability tests for DTCP2 and review and comment on proposed revisions to the Compliance Rules set forth in a notice from DTLA pursuant to Section 3.3.3.

3.5 **Most Current Update.** At any time that Adopter activates the DTCP2 functions of a unit or copy of a Licensed Product via an Update or replaces a DTCP2 Device Key of a unit or copy of a Licensed Product via an Update, Adopter shall issue one or more Updates to such unit or copy as necessary so as to cause the resulting product to include the changes that would have resulted if the copy or unit had received all sequential Updates designed for, and capable of properly functioning with, such copy or unit since the time the copy or unit was first distributed, provided, that if Adopter has, at any time, made available two or more versions of any such sequential Updates on different business terms (e.g., a free version and a fee-based version), the foregoing requirement shall apply with respect to the version of the Update(s) selected by the user of such unit or copy.

3.6 **Limitation for Licensed Products with Common DTCP2 Device Key.** Adopter shall not first activate the DTCP2 functions of a unit or copy of a Licensed Product that uses a Common DTCP2 Device Key more than eight (8) years after the particular version or model of such Licensed Product first was distributed, provided that a unit or copy of a particular version or model of such Licensed Product for which the DTCP2 functions were first activated during such eight-year period may be reactivated via an Update as permitted under Section 2.2(i)(y) of the Procedural Appendix. In the event that Adopter reasonably concludes that a software application containing or consisting of a copy of Licensed Product that uses a common DTCP2 Device Key and whose DTCP2 functions were first activated during such eight (8)-year period on a particular device was subsequently re-installed on the same device, the activation or re-activation of the DTCP2 functions of such re-installed copy shall not be deemed to be a "first activation" for purposes of this Section 3.6. If a software application containing or consisting of a copy of a Licensed Product that uses a Common

DTCP2 Device Key and whose DTCP2 functions were first activated during such eight (8)-year period on a particular device is subsequently installed and activated via an Update on a different device, such activation of the DTCP2 functions of such copy installed on the different device shall be deemed to be a "first activation" for purposes of this Section 3.6, subject to the reasonableness standard of the preceding sentence.

4. ELECTION OF RENEWABILITY OR THIRD PARTY CERTIFICATION

4.1 **Generally.** Before commercial distribution of a Licensed Product, Adopter shall ensure that the Implementation in such Licensed Product –

4.1.1 is Renewable (as set forth in Section 4.2), or

4.1.2 has passed a Third Party Review (as set forth in Section 4.3), or

4.1.3 for a Licensed Product that is Partially Renewable (as set forth in Section 4.2), has passed a Third Party Review for at least all non-Renewable portions (as set forth in Section 4.3).

4.2 **Renewability.** An Implementation is "Renewable" where the portions of such Implementation that both (i) are implemented in other than physical hardware, and (ii) constitute Primary L1 Core Functions (defined in Exhibit C Part 1 Section 3.5.1) and/or DTCP2 Core Functions (defined in Exhibit C Part 2 Section 3.5) are in each case designed to be replaced by an Update. An Implementation is "Partially Renewable" if a portion but not the entirety of the Implementation that is both implemented in other than physical hardware and constitutes Primary L1 Core Functions and/or DTCP2 Core Functions is designed to be replaced by an Update. "Physical hardware" means an implementation in a physical device, including a component, that does not include instructions or data other than such instructions or data that are permanently embedded in such device or component.

4.2.1 If Adopter elects to make an Implementation Renewable or Partially Renewable and elects not to submit the entire Implementation to Third Party Review, it shall renew by Update at least the renewable portion of such Implementation that has been found to satisfy the Revocation Criteria in Section 5.2.5(b) or (c), if all of the following criteria in Sections 4.2.1.1 through 4.2.1.3 are met:

4.2.1.1 DTLA issues to Adopter, within 12 months after such Implementation is first commercially distributed in any major world market, a notice of revocation in accordance with the Procedural Appendix Section 5.1 asserting Adopter's product is materially not Compliant;

4.2.1.2 It is both technically feasible and commercially reasonable to cure the noncompliance with an Update, and,

4.2.1.3 Adopter can include the Update with an upgrade of non-DTCP2 features of the product, scheduled for distribution within a reasonable time following a Constructive Revocation Determination or the date that an arbitrator determines that Adopter's product is materially non-Compliant.

4.2.2 For clarification, the Implementation after renewal as described in Section 4.2.1 is a new Implementation and therefore, if such Implementation incorporates an Implementation ID pursuant to Section 5.1.1, it must have a new Implementation ID.

4.3 **Third Party Review.**

4.3.1 Where Adopter elects to submit its Implementation to Third Party Review (defined below) pursuant to Section 4.1, Adopter shall submit to a Third Party Robustness Authority (defined in Procedural Appendix Section 4) information sufficient to enable such facility to determine that the Robustness Verification List accurately describes the compliance of the Implementation with the Robustness Rules (such review, a "Third Party Review"). In the event the Third Party Robustness Authority makes a determination that the Robustness Verification List does not accurately describe compliance of the Implementation with the Robustness Rules, Adopter's Implementation shall not be deemed to have passed the Third Party Review. DTLA will provide instructions to Third Party Robustness Authorities requiring that such a determination shall be provided in the form of a report issued to Adopter, which report shall be retained by Adopter and the applicable Third Party Robustness Authority and shall be made available to DTLA or Third Party Beneficiaries in the event of an allegation that one or more of Adopter's purported Licensed Products are not compliant with the Robustness Rules. Once an Implementation has passed Third Party Review, other products of Adopter may use the same Implementation without requiring re-submission to Third Party Review. If such Implementation is Partially Renewable, the Third Party Review may, at Adopter's election, be limited to the portions of the Implementation that are not Renewable. For clarification, Adopter may choose to obtain Third Party Review for a Renewable Implementation.

4.3.2 DTLA shall make available to Adopters a list of approved third party facilities.

5. REVOCATION.

5.1 **Generally.** The DTCP2 Specification includes means by which the DTCP2 Device Certificates or Implementation IDs of certain devices may be invalidated, rendering such devices with invalidated DTCP2 Device Certificates or Implementation IDs unable to exchange data via DTCP2 with Licensed Products (generally, "Revocation" or "Revoked"). Adopter shall elect one of the following alternatives in each of its Licensed Products to accurately identify the Implementation used in such Licensed Product:

5.1.1 An Implementation ID;

5.1.2 Unique Device Certificates incorporated into Licensed Products using the same Implementation in a substantially contiguous manner (*i.e.*, by consistent provisioning of sequentially-numbered Unique Device Certificates, consistent with guidelines to be promulgated by DTLA); or,

5.1.3 A Common Device Certificate.

For clarification, (a) Adopter shall incorporate an Implementation ID in Licensed Products that use Unique Device Certificates where such certificates are not provisioned in such products in a substantially contiguous manner as described in Section 5.1.2; (b) the same Implementation ID shall not be used in different Implementations; and, (c) Adopter may, but is not required to, incorporate an Implementation ID into Licensed Products described in Section 5.1.2 or 5.1.3. Failure to comply with the requirements of this Section 5.1 shall be deemed a material breach of the Agreement.

5.2 **Revocation.** DTLA may revoke a DTCP2 Device Certificate or Implementation ID when it is required to do so pursuant to Section 5.2.3 or it has otherwise been determined, pursuant to the procedures set forth in the Procedural Appendix, that one or more of the DTCP2 Revocation Criteria have been satisfied or as provided in the last sentence of Section 5.5. The "DTCP2 Revocation Criteria" mean the criteria set forth in Sections 5.2.1, 5.2.2, 5.2.3, 5.2.4 or 5.2.5:

5.2.1 (a) a DTCP2 Device Key and corresponding DTCP2 Device Certificate (other than a Common DTCP2 Device Key and Common DTCP2 Device Certificate) have been cloned such that the same DTCP2 Device Key and corresponding DTCP2 Device Certificate are found in more than one device or product or (b) a Common DTCP2 Device Key and corresponding Common DTCP2 Device Certificate are found in any product or component that is not manufactured by a Fellow DTCP2 Adopter or is not authorized by the Fellow DTCP2 Adopter that ordered such Common DTCP2 Device Key.

5.2.2 a DTCP2 Device Key and corresponding DTCP2 Device Certificate have been lost, stolen, intercepted or otherwise misdirected, or made public or disclosed in violation of a DTCP2 Adopter Agreement;

5.2.3 DTLA is required to revoke a DTCP2 Device Certificate by the National Security Agency, court order, or other competent government authority;

5.2.4 a DTCP2 Device Key with a corresponding DTCP2 Device Certificate or Implementation ID is used in a non-Compliant product purported to be a Licensed Product that was not produced by or on behalf of a Fellow DTCP2 Adopter;

5.2.5 a DTCP2 Device Key with a corresponding DTCP2 Device Certificate or Implementation ID is used in a product purported to be a Licensed Product, in each case that is materially not Compliant and is made or distributed by a Fellow DTCP2 Adopter, and—

(a) such Fellow DTCP2 Adopter has voluntarily committed to remedy such noncompliance through a renewability method (such as by Update) following a Constructive Revocation Determination or a determination by an arbitrator that such product is materially not Compliant;

(b) such material noncompliance is causing, or is likely to cause, a material and adverse effect on the integrity or security of DTCP2, or the operation of DTCP2 with respect to protecting Commercial Audiovisual Content from any output, transmission, interception or copying, in each case that is unauthorized, where such material and adverse effect results in or is likely to result in commercially significant harm to

Content Participants; or,

(c) such product has been deliberately designed to allow unauthorized unprotected output or unauthorized copying of Decrypted DT Data. For purposes of this criterion, public promotion by or, on behalf of, or in collaboration with Adopter of noncompliant output or noncompliant copying features, such as in advertising, use instructions, or on websites, shall be deemed deliberate.

DTLA shall not commence Revocation under Section 5.2.5(a) until after a reasonable time, no sooner than ninety (90) days but no later than one hundred and fifty (150) days following the arbitrator's determination.

5.2.6 Notwithstanding any Revocation decision issued by an arbitrator in accordance with Section 5.2.4 and 5.2.5 and Section 3 of the Procedural Appendix, DTLA, in consultation with and taking into account in good faith all comments received from Content Participants, retains discretion not to Revoke based on factors such as potential harm to end users, reputational impact, and other factors affecting the interests of DTLA, Fellow DTCP2 Adopters, or its Content Participants.

5.2.7 An Implementation that has passed Third Party Review shall not be subject to Revocation based on the criteria in Section 5.2.5(b), provided that if only a portion of the Implementation has passed Third Party Review (i.e., where the other portions are Renewable but have not been submitted to Third Party Review), a Device Certificate or Implementation ID in a product with such Implementation may be Revoked only if the material non-Compliance is in the portion of the Implementation that has not passed Third Party Review.

5.2.8 In the circumstance in which the Section 5.2.5(b) criteria are met and DTLA issues to Adopter a Revocation Notice—

(A) if Adopter can Update its Implementation as provided above in Section 4.2.1, then DTLA shall commence Revocation no sooner than 90 days following (i) the arbitrator's determination that the criteria set forth in Section 5.2.5(b) is met, or (ii) a Constructive Revocation Determination; and

(B) if Adopter cannot Update its Implementation as provided above in Section 4.2.1, then DTLA may commence Revocation without such delay following a Constructive Revocation Determination or following such determination by the arbitrator.

5.3 **General**. Without limiting the foregoing, DTLA shall not Revoke a DTCP2 Device Certificate or Implementation ID based on Adopter's general implementation of the DTCP2 Specification in a model or product line that is not Compliant or otherwise based on Adopter's breach of this Agreement, except (a) that if Adopter has caused any of the circumstances described in Sections 5.2.1, 5.2.2, 5.2.4, or 5.2.5., the DTCP2 Device Certificate or Implementation ID of any device or product in which such a DTCP2 Device Key has been included may be Revoked or (b) as expressly set forth in Section 5.2.5.

5.4 **Procedure.** Except as set forth in this Section 5.4, the procedures set out in the Procedural Appendix shall govern Revocation and any rescission or cancellation thereof. Such procedures provide for notice and review of DTLA decisions and/or actions regarding Revocation where requested. At any time commencing forty-eight (48) months following the issuance to a Fellow DTCP2 Adopter of a Common DTCP2 Device Certificate, such Common DTCP2 Device Certificate may be Revoked without notice.

5.5 **Remedies**. Except as otherwise expressly provided in this Section 5.5, Adopter's sole recourse with respect to Revocation shall be the objection and arbitration procedures set out in the Procedural Appendix. The Founders, Generator and Eligible Content Participants (defined below) shall each have no liability whatsoever with respect to any Revocation. Without limiting the foregoing, DTLA and the Founders shall not have any liability with respect to any Revocation, and no compensation shall be made to Adopter, except that if DTLA determines that a Revocation was performed in error by DTLA, DTLA, at the request of Adopter shall, at DTLA's discretion, (a) rescind the Revocation through substantially the same means as were used to effect the Revocation, or (b) provide for compensation to Adopter (or Adopter's affected customers) for each of its affected devices in an amount equal to the least of (i) the fair market value of each device, (ii) the cost of reworking each device to incorporate a new DTCP2 Device Certificate and DTCP2 Device Keys or Implementation ID, (iii) $25 per device, or, (c) in the case of Revocation of a Common DTCP2 Device Certificate, provide Adopter without charge with a new Common DTCP2 Device Key and Common DTCP2 Device Certificate at the same level of Unit Option or Blanket Option of the Revoked Common DTCP2 Device Certificate, or (d) provide for an alternative method of remedial action that DTLA determines appropriate to the particular circumstances of the Revocation.

6. LICENSES.

6.1 **Development**. Adopter may possess and use the DTCP2 Specification for development of Licensed Products or Licensed Components. Any distribution or disclosure of the DTCP2 Specification or of any product made with the use of the DTCP2 Specification must be in compliance with the other terms hereof.

6.2 **License**. Subject to the other provisions hereof, including payment of all fees required, DTLA grants to Adopter (including its Affiliates) a nonexclusive, nontransferable, nonsublicenseable, worldwide sublicense under the Necessary DTCP2 Claims of the Founders, as well as under any trade secrets or copyrights embodied in the DTCP2 Specification to make, have made, use, import, offer to sell and sell Licensed Products and Licensed Components; provided that such sublicense shall not extend to features of a product that are not required to comply with the DTCP2 Specification or for which there exists a noninfringing alternative, and further does not extend to Adopter if Adopter is in violation of Section 6.3 below.

6.3 **Reciprocal Non-Assertion Agreement**.

6.3.1 Adopter, on behalf of itself and its Affiliates, promises not to assert or maintain against DTLA or Fellow DTCP2 Adopters and Affiliates thereof, and accepts Fellow DTCP2 Adopters' promise not to assert or maintain, any claim of infringement under its or their respective Necessary DTCP2 Claims, as well as under any trade secrets or copyrights

embodied in the DTCP2 Specification for (a) with respect to Fellow DTCP2 Adopters, the making, having made, use, import, offering to sell and sale of Licensed Products and Licensed Components and (b) with respect to the Founders and DTLA, the use and licensing of DTCP2; provided that in each case such promise shall not extend to features of a product that are not required to comply with the DTCP2 Specification or for which there exists a noninfringing alternative, and further does not extend to any person or entity that is asserting, or whose Affiliate is asserting, a Necessary DTCP2 Claim against Adopter if Adopter (x) is not willfully in material breach of its obligations under the Compliance Rules or Confidentiality Agreement , or (y) is not otherwise in material breach of the Compliance Rules or Confidentiality Agreement, which breach has not been cured or is not capable of cure within thirty (30) days of Adopter's receipt of notice thereof.

6.3.2 Adopter, on behalf of itself and its Affiliates, further promises not to assert or maintain against DTLA or against DTCP1 Adopters that execute a "Non-Assertion Addendum" to the DTCP1 Adopter Agreement in the form available on the DTLA website and Affiliates thereof, any claim of infringement under its or their respective Necessary DTCP2 Claims, as well as under any trade secrets or copyrights embodied in the DTCP2 Specification for (a) with respect to such DTCP1 Adopter and its Affiliates, the making, having made, use, import, offering to sell and sale of products that fall within the definition of "Licensed Products" or "Licensed Components" under the DTCP1 Adopter Agreement, and (b) with respect to the Founders and DTLA, the use and licensing of DTCP1; provided that in each case such promise shall not extend to features of a product that are not required to comply with the DTCP1 Specification or for which there exists a noninfringing alternative, and further does not extend to any person or entity that is asserting, or whose Affiliate is asserting, in violation of the Non-Assertion Addendum to the DTCP1 Adopter Agreement, a patent claim that falls within the definition of "Necessary Claim" under the DTCP1 Adopter Agreement against Adopter if Adopter (x) is not willfully in material breach of its obligations under the Compliance Rules or Confidentiality Agreement, or (y) is not otherwise in material breach of the Compliance Rules or Confidentiality Agreement, which breach has not been cured or is not capable of cure within thirty (30) days of Adopter's receipt of notice thereof.

6.4 **Content Participant Non Assertion**. Adopter, on behalf of itself and its Affiliates, promises not to assert or maintain against Content Participants and Affiliates thereof any claim of infringement under its or their respective Necessary DTCP2 Claims, as well as under any trade secrets or copyrights embodied in the DTCP2 Specification for Content Participants' using or causing the use of DTCP2 to protect Commercial Entertainment Content in compliance with their Content Participant Agreements; and accepts Content Participants' promises not to assert or maintain any claim of infringement under their respective Necessary DTCP2 Claims, as well as under any trade secrets or copyrights embodied in the DTCP2 Specification for the making, having made, use, import, offering to sell and sale of Licensed Products and Licensed Components; provided that each such promise shall not extend to features of a product that are not required to comply with the DTCP2 Specification or for which there exists a noninfringing alternative, and further does not extend to any person or entity that is asserting, or whose Affiliate is asserting, Necessary DTCP2 Claims against Adopter if Adopter (x) is not willfully in material breach of its obligations under the Compliance Rules or Confidentiality Agreement, or (y)) is not otherwise in material breach of the

Compliance Rules or Confidentiality Agreement, which breach has not been cured or is not capable of cure within thirty (30) days of Adopter's receipt of notice thereof.

6.5 **Scope of Use**. This license, and the promises of non-assertion extended or accepted pursuant to Sections 6.3.1 and 6.4, shall, in each case, extend only to Licensed Products and to Licensed Components, only for transmission of content that, when received by the applicable Licensed Component or Licensed Product, was protected using a Commercially Adopted Access Control Method (as defined in the Compliance Rules) or otherwise constitutes Commercial Entertainment Content, and under a DTCP2 Device Certificate issued by or under the authority of DTLA following Activation. No license is granted, express or implied, and no promises of non-assertion extended or accepted pursuant to Sections 6.3 and 6.4, for (a) aspects of any technology, standard or product that is not itself part of the DTCP2 Specification (including, by way of example, AACS, CSS, MPEG, and analog copy protection systems) even though such technology, standard or product may be otherwise mentioned or required by the DTCP2 Specification or Compliance Rules or (b) implementation of any portion of the DTCP2 Specification other than for enabling the implementation of DTCP2 in Licensed Products.

6.6 **Proper Use.** The licenses granted herein are subject to and conditioned on the requirements that Adopter shall not produce or sell devices or software (a) under color of this Agreement, or (b) using Confidential and Highly Confidential Information, where such devices or software are designed to circumvent the requirements or effectiveness of the DTCP2 Specification.

6.7 **Have Made Parties.** If Adopter provides Licensed Components to, or has Licensed Components produced by, its Have Made Party (as defined in Section 7.2.1), Adopter shall contractually prohibit such Have Made Party from selling, distributing or furnishing such Licensed Components to any third person or entity other than Adopter.

7. DISTRIBUTION OF PRODUCTS AND MANAGEMENT OF DTCP2 KEYING MATERIAL IN LICENSED COMPONENTS.

7.1 **Licensed Products.** Licensed Products may be furnished, distributed, sold or disposed of in any commercially reasonable manner.

7.2 Licensed Components without Keying Material.

7.2.1 Licensed Components without a DTCP2 Device Key and corresponding DTCP2 Device Certificate (collectively, “Keying Material”) may not be furnished, distributed, or sold by Adopter to any person or entity other than to Fellow DTCP2 Adopters, DTCP2 Associates or any person or entity that is providing services to Adopter pursuant to the right under Section 6.2 to “have made” Licensed Products or Licensed Components (a “Have Made Party”).

Adopter may not install (or have installed) Keying Material into a product other than a Licensed Component or Licensed Product, in each case produced by Adopter or its Have Made Party, which may include a Licensed Product that contains a Licensed Component without Keying Material produced by a Fellow DTCP2 Adopter.

7.3 **Licensed Components with Keying Material.**

7.3.1 Licensed Components with Keying Material may not be furnished, distributed, or sold by Adopter to any person or entity (other than its Have Made Party) except that if Adopter produces (or has produced by its Have Made Party) a Licensed Component with Keying Material, Adopter may sell such Licensed Component to a Fellow DTCP2 Adopter solely for incorporation by such Fellow DTCP2 Adopter (or its Have Made Party) into a Licensed Product produced by or on behalf of (by its Have Made Party) such Fellow DTCP2 Adopter if:

(a)(i) such Fellow DTCP2 Adopter places the order with DTLA for Keying Material to be incorporated into such Licensed Component and (ii) such Fellow DTCP2 Adopter sends, or directs DTLA to send, the Keying Material to Adopter; or,

(b) If Adopter is an Approved Licensed Component Adopter, Adopter may furnish, distribute and sell such Licensed Component with Keying Material to a Fellow DTCP2 Adopter for incorporation by such Fellow DTCP2 Adopter (or its Have Made Party) into a Licensed Product produced by or on behalf of such Fellow DTCP2 Adopter. An "Approved Licensed Component Adopter" means a Fellow DTCP2 Adopter that has been approved as such by DTLA based on a demonstration of its bona fide capability to securely sell Licensed Components, and upon satisfaction of objective criteria established by DTLA that demonstrate the reliability and integrity of such Adopter with respect to the handling and sales of Licensed Components and DTLA Confidential Information.

7.3.2 If Adopter is incorporating into its Licensed Product a Licensed Component with Keying Material produced by another Fellow DTCP2 Adopter, Adopter shall ensure that either (a) such other Fellow DTCP2 Adopter is an Approved Licensed Component Adopter or (b) the DTCP2 Device Certificate in the Licensed Component received from such other Fellow DTCP2 Adopter corresponds to the Keying Material ordered from DTLA by Adopter.

7.4 **Licensed Components with Inactive Keying Material.**

7.4.1 Licensed Components (excluding Robust Licensed Components) that, when sold, contain non-operational DTCP2 Device Certificates ("IKLC") may only be distributed by Adopter to (a) Adopter's Have Made Party and (b) Fellow DTCP2 Adopters, provided that the Keying Material in such IKLC shall be rendered operational only by activation by or under the control of Adopter at the request of such Fellow DTCP2 Adopter. Such activation may be performed by secure communication to activate a specific unit, or by providing to such Fellow DTCP2 Adopter an activation tool that is uniquely cryptographically identified only to such Fellow DTCP2 Adopter.

7.4.2 If Adopter receives an IKLC from a Fellow DTCP2 Adopter, Adopter shall only request activation or use the provided activation tool to activate the Keying Material in such IKLC at the time Adopter produces the Licensed Product incorporating such IKLC.

7.5 **Maintenance, Disclosure, and Audit of Keying Material Records.**

7.5.1 If Adopter provides Licensed Components with Keying Material or IKLCs to Fellow DTCP2 Adopters, Adopter shall maintain complete and accurate records of the DTCP2 Device Certificates supplied to each Fellow DTCP2 Adopter.

7.5.2 When placing orders for Keying Material to be incorporated in Licensed Components to be supplied by Adopter to a Fellow DTCP2 Adopter, Adopter shall inform DTLA at the time of the order that the keys are intended for use in either Licensed Components with Keying Material or IKLCs. With each subsequent order, or if Adopter has not placed a subsequent order for Keying Material within six (6) months after a previous order, Adopter shall also submit to DTLA a report, signed by an employee of Adopter having supervisory responsibility for the maintenance of such records, disclosing—

(a) each Fellow DTCP2 Adopter that purchased Licensed Components with Keying Material or IKLCs from Adopter during the period since the last report;

(b) which DTCP2 Device Certificates have been supplied to each such Fellow DTCP2 Adopter during such period; and,

(c) the disposition during such period of all other DTCP2 Device Certificates that Adopter acquired from DTLA.

7.5.3 Failure to maintain accurate records and to submit a complete and accurate signed report under this Section 7.5 shall be deemed a material breach of this Agreement. Adopter acknowledges that, in addition to the remedies set forth in Section 9.1.2 of this Agreement, DTLA reserves all rights and discretion to refuse to provide Adopter with additional DTCP2 Keying Material until and unless such breach is cured.

7.5.4 DTLA shall have the right, at reasonable times and intervals, to have audited Adopter's books and records to ascertain the accuracy and completeness of the reports submitted by Adopter under this Section 7.5. Such audit shall be performed by an independent auditor who shall be a Certified Public Accountant from a major accounting firm. The auditor shall only disclose those matters that are subject to a right to audit under this Agreement to DTLA, which may disclose such matters to Eligible Content Participants. Such disclosures and the results of the audit shall be deemed confidential, and shall be used only for purposes of enforcing Adopter's obligations under this Agreement. Auditor fees and costs shall be borne by DTLA except that, in a case where the audit discloses a failure to maintain accurate records or repeated material breaches, all fees and costs of the audit shall be paid by Adopter.

7.6 **Robust Licensed Components.** Notwithstanding the restrictions applicable to Licensed Components in Section 7.2-7.5**,** Robust Licensed Components may be disposed of in any commercially reasonable manner.

8. CONFIDENTIALITY.

8.1 **Treatment.** Adopter shall comply with the terms of Exhibit A ("the Confidentiality Agreement"). The portions of the DTCP2 Specification marked "Confidential" are to be treated as

Confidential Information under the Confidentiality Agreement, and the materials designated by DTLA as "Highly Confidential" shall be treated as specified by the Confidentiality Agreement.

8.2 **Compliance with Laws, Export**. Adopter will comply with all applicable rules and regulations of the United States, Japan and other countries and jurisdictions, including those relating to the export or re-export of commodities, software and technical data insofar as they relate to the activities under this Agreement. Adopter agrees that commodities, software and technical data provided under this Agreement are subject to restrictions under the export control laws and regulations of the United States, Japan and other countries and jurisdictions, as applicable, including but not limited to the U.S. Export Administration Act and the U.S. Export Administration Regulations and the Japanese Foreign Exchange and Foreign Trade Law, and shall obtain any approval required under such laws and regulations whenever it is necessary for such export or re-export.

9. TERM/TERMINATION.

9.1 **Termination**. This Agreement shall be effective upon the Effective Date and shall continue until the tenth anniversary of the Effective Date (the "Term") unless sooner terminated in accordance with any of the following events:

9.1.1 **Termination by Adopter**. Adopter shall have the right to terminate this Agreement at any time upon ninety (90) days' prior written notice to DTLA.

9.1.2 **Breach Capable of Cure.** In the event that either party (i) materially breaches any of its obligations hereunder, which breach is not cured within thirty (30) days after written notice is given to the breaching party specifying the breach or (ii) repeatedly breaches any of its obligations hereunder and fails to cure and cease committing such repeated breaches within thirty (30) days after being given written notice specifying the breaches, then the party not in breach may, by giving written notice thereof to the breaching party, terminate this Agreement, upon the expiration of a thirty (30)-day period beginning on the date of such notice of termination. Notwithstanding the foregoing, DTLA shall not terminate this Agreement for reason that a Robust Inactive Product manufactured or distributed by Adopter would not comply with the Compliance Rules if its DTCP2 functions were activated, provided that, no later than thirty (30) days after receiving notice of breach from DTLA, Adopter prevents activation of the DTCP2 functions of such Robust Inactive Product until such time, if any, that an Update is applied to such Robust Inactive Product that causes it to be a Licensed Product in accordance with the terms of Section 3.3.

9.1.3 **Breach Not Capable of Cure.** In the event of a material breach that is not capable of cure under the provisions of Section 9.1.2, the party not in breach may, by giving written notice of termination to the breaching party, terminate this Agreement. Such termination shall be effective upon receipt of such notice of termination.

9.2 **Effect of Termination.** Upon termination or expiration of this Agreement, Adopter shall immediately cease use of DTCP2 Device Certificates and DTCP2 Device Keys. Within thirty (30) days after termination or expiration of this Agreement, Adopter shall return such DTCP2 Device Certificates and DTCP2 Device Keys and shall as directed by DTLA: (i) return all other Proprietary Information to DTLA; or (ii) destroy all Proprietary Information in its possession, retaining no copies

thereof, and certify such destruction in writing to DTLA. Within thirty (30) days after termination or expiration of this Agreement, Adopter shall discontinue all manufacture, sale, or distribution of Licensed Products and Licensed Components. Notwithstanding the foregoing, in the event that Adopter, prior to the date of such termination or expiration, manufactures, distributes or sells to persons or entities Robust Inactive Products, Adopter shall have the right to continue to manufacture, distribute and sell the same version of such Robust Inactive Products after such termination or expiration for a period of up to two (2) years, or such longer period as DTLA may, in extraordinary circumstances, approve in writing, provided that the DTCP2 functions in any such Robust Inactive Products sold or distributed after the date of such termination shall not be activated.

9.3 **Survival**. Following termination of this Agreement for any reason, the following Sections shall survive: 1, 5, 6.3 and 6.4 (both with respect to the DTCP2 Specification in effect as of the date of termination), 8, 9.2, this Section 9.3, 10, 11, and 12.

10. DISCLAIMER AND LIMITATION OF LIABILITY.

10.1 **Generally.** The following terms limit the ability of the Adopter to recover any damages from DTLA or the Founders in excess of fees actually paid to DTLA by Adopter. These provisions are an essential part of the bargain, without which DTLA would not be willing to enter into this Agreement, nor would the Founders be willing to license their Necessary DTCP2 Claims to DTLA.

10.2 **Disclaimer.** ALL INFORMATION, MATERIALS, KEYS, AND CERTIFICATES ARE PROVIDED "AS IS." DTLA AND THE FOUNDERS AND GENERATOR MAKE NO REPRESENTATIONS OR WARRANTIES, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, AND EXPRESSLY DISCLAIM IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND ANY EQUIVALENTS UNDER THE LAWS OF ANY JURISDICTION THAT MIGHT ARISE FROM ANY ACTIVITIES OR INFORMATION DISCLOSURES RELATING TO THIS AGREEMENT. DTLA, THE FOUNDERS AND GENERATOR FURTHER DISCLAIM ANY WARRANTY THAT ANY IMPLEMENTATION OF THE DTCP2 SPECIFICATION, IN WHOLE OR IN PART, WILL BE FREE FROM INFRINGEMENT OF ANY THIRD PARTY INTELLECTUAL PROPERTY OR PROPRIETARY RIGHTS.

10.3 **Limitation of Liability**. NEITHER DTLA NOR THE FOUNDERS NOR GENERATOR NOR ANY DIRECTOR, OFFICER, AGENT, MEMBERS, REPRESENTATIVES, EQUIVALENT CORPORATE OFFICIAL, OR EMPLOYEE OF ANY OF THEM ACTING IN THEIR CAPACITIES AS SUCH (COLLECTIVELY, THE "AFFECTED PARTIES") SHALL BE LIABLE TO ADOPTER FOR ANY DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL OR PUNITIVE DAMAGES ARISING OUT OF ANY CAUSE OF ACTION RELATING TO THIS AGREEMENT, OR BASED ON MAKING, USING, SELLING OR IMPORTING ANY PRODUCTS OF ADOPTER THAT IMPLEMENT PROPRIETARY INFORMATION OR DTCP, WHETHER UNDER THEORY OF CONTRACT, TORT, INDEMNITY, PRODUCT LIABILITY OR OTHERWISE. TO THE EXTENT THAT ANY COURT OF COMPETENT JURISDICTION RENDERS JUDGMENT AGAINST DTLA NOTWITHSTANDING THE ABOVE LIMITATION, THE AFFECTED PARTIES' AGGREGATE LIABILITY TO ADOPTER IN CONNECTION WITH THIS AGREEMENT SHALL IN NO EVENT EXCEED THE AMOUNTS OF MONEY

RECEIVED BY DTLA FROM ADOPTER UNDER THIS AGREEMENT IN ANY ONE YEAR PERIOD.

11. REMEDIES.

11.1 **Indemnification for Wrongful Acts of Adopter**. Adopter shall indemnify and hold DTLA, the Founders and Generator, and their officers, members, representatives, agents, directors, equivalent corporate officials, and employees, harmless from and against any and all any losses, claims, actions, suits, proceedings or litigation, and any losses, deficiencies, damages, liabilities, costs and expenses including without limitation, reasonable attorneys' fees and all related costs and expenses, to be paid or otherwise incurred in connection with the defense of any claim, action, suit, proceeding or litigation, that result from any material breach of any covenant, agreement, representation or warranty herein or negligent acts committed by Adopter.

11.2 **Records Audit and Inspection**. In addition to the rights provided in Section 7.5.4, DTLA shall have the right, at reasonable times and intervals, to have audited Adopter's books and records to ascertain the propriety of any payment hereunder. Such audit shall be undertaken at DTLA's sole expense, and the auditor, who shall be a Certified Public Accountant from a major accounting firm, shall only disclose those matters which DTLA has the right to know under this Agreement, and the results of the audit shall be deemed confidential.

11.3 **Device Inspection**. DTLA may acquire products distributed hereunder on the open market for examination. Adopter shall provide reasonable cooperation in affording DTLA an example of any product distributed hereunder if requested, and Adopter shall provide, once per model of product, and under the terms of a non-disclosure agreement equivalent to that document referred to by DTLA as the Evaluation NDA, the service manual for such product in order to assist in evaluation of it. Adopter may, at its option provide further information.

11.4 **Equitable Relief**. DTLA and Adopter agree and acknowledge that due to the unique nature of certain provisions hereof and the lasting effect of and harm from a breach of such provisions, including making available the means for widespread unauthorized copying of copyrighted content intended to be protected using the DTCP2 Specification, if Adopter breaches its obligations hereunder, money damages alone may not adequately compensate an injured party, and that injury to such party may be irreparable, and that specific performance or injunctive relief is an appropriate remedy to prevent further or threatened breaches hereof, provided, however, that injunctive relief shall not be available to prevent the distribution of a Robust Inactive Product that would not comply with the Compliance Rules if its DTCP2 functions were activated if, no later than thirty (30) days after receiving notice of breach from DTLA, Adopter prevents activation of the DTCP2 functions of such Robust Inactive Product until such time, if any, that an Update is applied to such Robust Inactive Product that causes it to be a Licensed Product in accordance with the terms of Section 3.3. Notwithstanding the preceding sentence, Adopter agrees that DTLA shall be entitled to seek injunctive relief to prevent further or threatened breaches of this Agreement if Adopter has engaged in a pattern of behavior involving the repeated release of non-compliant products or components for which Adopter received notice of the breach, whether or not Adopter corrected such repeated breaches following such notice.

11.5 **Damages Measure and Limitation.** The parties agree that it would be impossible to estimate the amount of damages in the event of certain breaches. In the event of a material breach by Adopter (1) of the Confidentiality Agreement, Adopter shall be liable for one million dollars; (2) that involves the manufacture or distribution of devices or software, including but not limited to an Update, that fail to protect DTCP2 Device Keys and DTCP2 Device Certificates as provided by the applicable Compliance Rules or as required by Section 7.2, 7.3, 7.4, or 7.6, or the requirements hereunder applicable to Updates, Adopter shall be liable in an amount equal to its profits on such devices or software, and in no event less than one million dollars nor more than eight million dollars; and (3) that involves any other provision of this Agreement, Adopter shall be liable in an amount equal to its profits on the affected devices or software, and in no event more than eight million dollars. Notwithstanding the foregoing, if Adopter has remedied a material breach described in clause (2) or (3) above in accordance with the requirements of Section 5.2.5(a) or in response to a breach under Section 5.2.5(b) of this Agreement, Adopter shall not be liable for an amount greater than fifty percent (50%) of its profits on the affected devices or software, and in no event more than four million dollars. The amounts payable by Adopter in accordance with this Section 11.5 shall be DTLA's exclusive monetary remedies available for any and all such breaches by Adopter, and such amounts shall be paid by Adopter in lieu of any and all other monetary damages to DTLA relating to such breaches. For purposes of this Section 11.5, a series of substantially related events shall constitute a single material breach. A breach shall be "material" only if it has resulted in or would be likely to result in commercially significant harm to other users of DTCP, including but not limited to Fellow DTCP2 Adopters and Content Participants, or constitute a threat to the integrity or security of DTCP. In addition, the following is a non-exclusive list of circumstances in which, standing alone, there is no material breach of the applicable provisions by Adopter: (1) if no Confidential Information or Highly Confidential Information was released to a third party not permitted hereunder to have such information or could reasonably have been expected to have been released to such third party as a result of the breach; (2) if Adopter maintains an internal program to assure compliance herewith (including a program to assure maintenance of inventory, samples, and confidentiality of information for purposes in addition to compliance with this Agreement), the breach was inadvertent or otherwise unintentional, and the breach did not have a material adverse effect on the integrity or security of DTCP2 or the function of DTCP2 to protect Commercial Entertainment Content; (3) if Adopter brought the breach to DTLA's attention in a timely manner as required by this Agreement and such breach did not have a material adverse effect on the integrity or security of DTCP2 or the function of DTCP2 to protect Commercial Entertainment Content.

11.6 **Third-Party-Beneficiary Rights.** Compliance of Adopter and other licensees with the terms hereof is essential to maintain the value, integrity, security and performance of DTCP2. As part of the consideration granted herein, upon Activation, Adopter agrees that each Content Participant that (i) distributes or transmits, or causes or authorizes the distribution or transmission of, its Commercial Entertainment Content in commercial quantities, or via mass distribution channels such as satellite or cable transmission, to the general public in a form that would, in the course of a transmission up to and including the display or other performance of such Commercial Entertainment Content, use a channel protected by DTCP2 ("Eligible Content") and (ii) at such time (x) is not willfully in material breach of any term or condition of its Content Participant Agreement, and (y) is not otherwise in material breach of any term or condition of its Content Participant Agreement, which breach has not been cured, or is not capable of cure, within thirty (30) days of Content Participant's receipt of notice thereof by DTLA or any Fellow DTCP2 Adopter (an "Eligible Content Participant"), shall be a

third-party beneficiary of this Agreement and shall be entitled, during such period that such Content Participant is an Eligible Content Participant, to bring a claim or action to enforce rights against Adopter in accordance with the procedures set out in the Procedural Appendix with respect to Adopter's implementation of DTCP2 in any product that receives or transmits data in a format in which Content Participant has made Eligible Content available. Such rights shall be limited to seeking injunctive relief against the manufacture, distribution, commercial use and sale of Adopter's products that are in material breach of the Compliance Rules, and against disclosure of Highly Confidential Information in breach of this Agreement that affects the integrity or security of DTCP2, except where such Adopter has willfully breached, or engaged in a pattern or practice of breaching, such obligations, as to which breach attorneys' fees and costs shall be awarded to each Eligible Content Participant that is a prevailing party. Notwithstanding the provisions of this Section 11.6, injunctive relief shall not be available to an Eligible Content Participant to prevent the distribution of a Robust Inactive Product that would not comply with the Compliance Rules if its DTCP2 functions were activated if, no later than thirty (30) days after receiving notice of breach from DTLA, Adopter prevents activation of the DTCP2 functions of such Robust Inactive Product until such time, if any, that an Update is applied to such Robust Inactive Product that causes it to be a Licensed Product. Notwithstanding the preceding sentence, Adopter agrees that an Eligible Content Participant shall be entitled to seek injunctive relief to prevent further or threatened breaches of this Agreement if Adopter has engaged in a pattern of behavior involving the repeated release of non-compliant products or components for which Adopter received notice of the breach, whether or not Adopter corrected such repeated breaches following such notice.

11.7 **Adopter Claims.** Following Activation, and while Adopter (i) is not willfully in material breach of any term or condition of this Agreement, and (ii) is not otherwise in material breach of any term or condition of this Agreement, which breach has not been cured, or is not capable of cure, within thirty (30) days of Adopter's receipt of notice thereof by DTLA, Adopter shall be a third-party beneficiary of each Content Participant Agreement and shall be entitled to bring a claim or action to enforce rights against a Content Participant, in accordance with the third-party-beneficiary procedures set out in the Procedural Appendix, with respect to such Content Participant's compliance with its obligations under Section 5 of its Content Participant Agreement; provided that such rights, pursuant to such Content Participant Agreement, shall be limited to seeking equitable relief, except where such Content Participant has willfully breached, or engaged in a pattern or practice of breaching, such obligations, as to which breach attorneys' fees and costs shall be awarded to each Adopter that is a prevailing party.

12. MISCELLANEOUS.

12.1 **Ownership**. All Proprietary Information and media containing Proprietary Information as provided by DTLA to Adopter shall remain the property of DTLA or its suppliers. Except as expressly provided herein, this Agreement does not give Adopter any license or other right to the Proprietary Information.

12.2 **Entire Agreement**. This Agreement, the exhibits hereto and the DTCP2 Specification constitute the entire Agreement between the parties hereto with respect to the subject matter hereof and supersede all prior oral, written or other agreements. Except as otherwise provided herein, this

Agreement may not be modified except by written agreement dated subsequent to the date of this Agreement and signed by both parties.

12.3 **Controlled Entities**. Adopter represents and warrants that it has, or will have, the authority to bind its Affiliates to the terms of this Agreement.

12.4 **Money.** All fees shall be paid to DTLA or to its order in United States dollars by wire transfer or such other means as DTLA may reasonably specify. If Adopter is required by law to make any withholding from fees due to DTLA, it may make such withholding but shall provide DTLA, at the time of payment, with evidence of such withholding adequate to permit DTLA or its assignee to claim relevant tax credits under applicable treaties.

12.5 **Assignment**. The licenses granted hereunder are personal to Adopter, and Adopter's rights under this Agreement shall not be assigned or otherwise transferred except (a) with the written approval of DTLA (which shall not be unreasonably withheld) or (b) to a corporation controlling, controlled by or under common control with Adopter or to the purchaser of all or substantially all of the outstanding capital stock or assets and obligations of Adopter or to the surviving entity in a merger, reorganization, or other business combination and where notice of such assignment has been provided in advance to DTLA and where the surviving or acquiring company agrees in writing to be bound by this Agreement. Subject to the limitations set forth in this Agreement, this Agreement will inure to the benefit of and be binding upon the parties, their successors and permitted assigns. DTLA may assign or transfer this Agreement to a party that agrees to assume DTLA's obligations hereunder, and will provide Adopter with written notice thereof.

12.6 **Presumptions**. In construing the terms of this Agreement, no presumption shall operate in either party's favor as a result of its counsel's role in drafting the terms or provisions hereof.

12.7 **Governing Law; Jurisdiction**. THIS AGREEMENT, AND ALL THIRD-PARTY-BENEFICIARY CLAIMS BROUGHT PURSUANT HERETO, SHALL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF NEW YORK APPLICABLE TO AGREEMENTS MADE AND TO BE PERFORMED ENTIRELY IN SUCH STATE AND WITH THE LAWS OF THE UNITED STATES AS WOULD BE CONSTRUED BY A COURT SITTING IN THE SOUTHERN DISTRICT OF NEW YORK.

12.7.1 IN CONNECTION WITH ANY LITIGATION BETWEEN THE PARTIES HERETO OR IN CONNECTION WITH ANY THIRD-PARTY-BENEFICIARY CLAIM BROUGHT HEREUNDER ARISING OUT OF OR RELATING TO THIS AGREEMENT, EACH PARTY IRREVOCABLY CONSENTS TO: (i) THE EXCLUSIVE JURISDICTION AND VENUE IN THE FEDERAL AND STATE COURTS LOCATED IN THE COUNTY OF NEW YORK, NEW YORK (EXCEPT THAT CLAIMS BROUGHT PURSUANT TO SECTION 11.6 OR 11.7 MAY BE BROUGHT IN A COURT SITTING IN LOS ANGELES COUNTY, CALIFORNIA); AND (ii) THE SERVICE OF PROCESS OF SAID COURTS IN ANY MATTER RELATING TO THIS AGREEMENT BY PERSONAL DELIVERY OR BY MAILING OF PROCESS BY REGISTERED OR CERTIFIED MAIL, POSTAGE PREPAID, AT THE ADDRESSES SPECIFIED IN THIS AGREEMENT, OR TO THE AGENT TO BE APPOINTED PURSUANT TO THE SECTION, BELOW;

12.7.2 ADOPTER SHALL APPOINT AN AGENT IN THE STATE OF NEW YORK FOR ACCEPTANCE OF SERVICE OF PROCESS PROVIDED FOR UNDER THIS AGREEMENT AND SHALL NOTIFY DTLA OF THE IDENTITY AND ADDRESS OF SUCH AGENT WITHIN THIRTY (30) DAYS AFTER THE EFFECTIVE DATE

12.7.3 ADOPTER WAIVES ANY OBJECTION TO THE JURISDICTION, PROCESS, AND VENUE OF ANY SUCH COURT, AND TO THE EFFECTIVENESS, EXECUTION, AND ENFORCEMENT OF ANY ORDER OR JUDGMENT (INCLUDING, BUT NOT LIMITED TO, A DEFAULT JUDGMENT) OF SUCH COURT PERTAINING TO THIS AGREEMENT, TO THE MAXIMUM EXTENT PERMITTED BY THE LAW OF THE PLACE WHERE ENFORCEMENT OR EXECUTION OF ANY SUCH ORDER OR JUDGMENT MAY BE SOUGHT AND BY THE LAW OF ANY PLACE WHOSE LAW MIGHT BE CLAIMED TO BE APPLICABLE REGARDING THE EFFECTIVENESS, ENFORCEMENT, OR EXECUTION OF SUCH ORDER OR JUDGMENT, INCLUDING PLACES OUTSIDE OF THE STATES OF NEW YORK AND CALIFORNIA AND OF THE UNITED STATES.

12.8 **Notice**. All notices to be provided pursuant to this Agreement shall be given in writing and shall be effective when either served by personal delivery or upon receipt via certified mail, return receipt requested, postage prepaid, overnight courier service or sent by facsimile transmission with hard copy confirmation sent by certified mail, in each case to the party at the addresses set out herein.

12.9 **Severability; Waiver**. Should any part of this Agreement judicially be declared to be invalid, unenforceable, or void by any court of competent jurisdiction, the parties agree that the part or parts of this Agreement so held to be invalid, unenforceable, or void shall be reformed by such court without further action by the parties hereto but only to the extent necessary to make such part or parts valid and enforceable. A waiver by either of the parties hereto of any of the covenants to be performed by the other party or any breach thereof shall not be effective unless made in writing and signed by the waiving party and shall not be construed to be a waiver of any succeeding breach thereof or of any covenant herein contained.

12.10 **Most Favored Status.** DTLA will make available to Adopter its substantive commitments or clarifications regarding the standard DTCP2 Adopter Agreement through notice on the DTLA website or otherwise. DTLA also commits that the benefit of any of its clarifications or interpretations of language in the standard DTCP2 Adopter Agreement will be extended to Adopter in accordance with this Section 12.10. Where DTLA agrees to make a change to a particular Fellow DTCP2 Adopter's standard DTCP2 Adopter Agreement, such change shall be reflected in the next regular revision of the standard DTCP2 Adopter Agreement and Adopter will be given the ability to upgrade to such revised DTCP2 Adopter Agreement. Prior to such time as it makes a revised or upgraded standard DTCP2 Adopter Agreement available to all Fellow DTCP2 Adopters that have executed a standard DTCP2 Adopter Agreement, where DTLA has agreed to include language in a particular Fellow DTCP2 Adopter's standard DTCP2 Adopter Agreement that is more favorable than that in the then-current version of the standard DTCP2 Adopter Agreement, DTLA will not enforce the language in Adopter's DTCP2 Adopter Agreement to the extent that such language is less favorable than that found in such Fellow Adopter's DTCP2 Adopter Agreement. For purposes of this Section 12.10, “standard Adopter Agreement” refers to a DTCP2 Adopter Agreement under which a Fellow DTCP2 Adopter receives a license with respect to activities that are the same as those

activities licensed hereunder, but does not include, by way of example and not limitation, any DTCP2 Adopter Agreement in which a Fellow DTCP2 Adopter is not licensed to manufacture Licensed Products.

IN WITNESS WHEREOF, the parties have executed this Agreement as of the date first above written.

DTLA:	**Adopter:**
By:_____	**By:**_____
Name:_____	**Name:**_____
Title:_____	**Title:**_____
Date:_____	**Date:**_____

Addresses for notices:

DTLA:	**Adopter:**
c/o License Management International, LLC	
380 Tennant Ave., Unit 4	
Morgan Hill, CA 95037-5478	

Procedural Appendix

Unless otherwise expressly stated in this Procedural Appendix, all section references in this Procedural Appendix are references to sections of this Procedural Appendix.

Fee Schedule

A. Annual Administration Fee

Adopter may select whichever category of license it prefers. Adopter is encouraged to select the category of license which it finds most financially efficient. Adopter may (i) downgrade its elected category not more than once per year upon providing DTLA thirty (30) days prior written notice, provided that, such Adopter shall not be entitled to any refund of the Annual Administration Fee paid for such period; or (ii) upgrade its elected category upon providing DTLA thirty (30) days prior written notice and the full Annual Administration Fee associated with such upgraded category. Future Annual Administration Fees owed by such Adopter shall be due on the anniversary of the effective date of Adopter's notice, provided that the Annual Administration Fee payable for the last year of the Term shall be pro-rated based on the number of months remaining in the Term.

Category	Annual Administrative Fee (US $)
Component Supplier Fee	$14,000
Evaluation Fee	$10,000
DTCP2 Adopter-Small	$14,000
DTCP2 Adopter-Large	$18,000

B. DTCP2 Certificate Fees

(i). Unique DTCP2 Device Certificates

An Adopter in the category of DTCP2 Adopter-Small or DTCP2 Adopter-Large may order DTCP2 Device Keys and DTCP2 Device Certificates as unique certificates (i.e., a different certificate for each device).

Category	Per Unique DTCP2 Certificate Fee (US $)
DTCP2 Adopter - Small	.07
DTCP2 Adopter - Large	.06

Shipping and Handling - $200.00 / order

(ii). Common DTCP2 Device Certificates

An Adopter in the category of DTCP2 Adopter-Large may order Common DTCP2 Device Keys and Common DTCP2 Device Certificates, in Unit Options or Blanket Options.

(a) Under the Unit Options, a particular Common DTCP2 Device Certificate may be used in no more than the number of units or copies, as specified below, of the same Licensed Product or Robust Licensed Component. Such "same" Licensed Product or Robust Licensed Component may include, for purposes of assessment of fees under this Fee Schedule, units or copies that are substantially identical but are marketed under different names or model designations, and units or copies that have different version numerical designations to the right of the decimal point. If within a given year Adopter wishes to use the same Common DTCP2 Device Certificate in a greater number of units or copies than would have been permitted under its original order, Adopter shall provide DTLA with an amended Order Form indicating the new desired maximum number of units or copies and, when invoiced by DTLA, shall pay the difference between the fees under the original and amended orders. However, Adopter may order no more than 4 sets of Common DTCP2 Device Keys and Common DTCP2 Device Certificates within a year under the option to obtain no more than 4 keys to be used in a maximum of 20,000 units or copies.

(b) Any Adopter that orders one or more Common DTCP2 Device Certificate(s) pursuant to a Unit Option shall maintain accurate records of the number of Devices into which each Common DTCP2 Device Certificate was implemented by or with the authorization of Adopter. Adopter agrees to permit DTLA to audit those records at Adopter's place of business during normal business hours within sixty (60) days of receipt of written notice from DTLA of DTLA's intent to conduct said audit, or at such other place and time as may be mutually agreed by DTLA and Adopter. Adopter shall not be required to undergo an audit under this section more than once during a single calendar year. Such audit may cover the three-year period preceding the audit. During said audit, Adopter shall provide the auditor with complete access to the aforementioned records and to records of shipments and sales of all products that incorporate DTCP2 for the period covered by the audit, and shall provide all reasonable assistance to the auditors. Such audits shall be conducted by an independent auditor hired by DTLA and shall be conducted pursuant to generally accepted auditing standards. The costs to DTLA of the audit shall be borne by DTLA, except that if any such audit should reveal that any Common DTCP2 Device Certificate was implemented in more than the number of products covered by the selected Unit Option (other than by a de minimis amount), Adopter shall pay DTLA's costs of such audit, as well as pay the discrepancy in fees. Adopter's failure to comply with any provisions of this paragraph shall constitute a material breach of the Agreement.

(c) Under the Blanket Option, Adopter can order up to 5 Common DTCP2 Device Certificates for a flat annual fee, with an option to purchase additional Common DTCP2 Device Certificates for $1,000 each. Each Common DTCP2 Device Certificate can be used in an unlimited number of units or copies.

Per Common DTCP2 Certificate Fee (DTCP2 Adopter - Large Only)
Unit Options Up to a maximum of 4 keys/total 20,000 units or copies -- $1,000 Up to 100,000 units or copies -- $2,000 Up to 200,000 units or copies -- $4,000 Up to 500,000 units or copies -- $6,000 Up to 1,000,000 units or copies -- $10,000 Up to 2,000,000 units or copies -- $12,000 Up to 5,000,000 units or copies -- $15,000 Up to10,000,000 units or copies -- $25,000 Up to 30,000,000 units or copies -- $50,000 Blanket Option Up to a maximum of 5 Common DTCP2 Device Keys and Common DTCP2 Device Certificates -- $100,000 Additional Common DTCP2 Device Keys and Common DTCP2 Device Certificates -- $1,000

Shipping and Handling - $200.00 / order

C. PGP key registration fee
The fee for replacing a PGP key is $3000.00.

D. Fee for additional Hard Copies of the DTCP2 Specification.
The fee for additional Hard Copies of the DTCP2 Specification which are Confidential Information or Highly Confidential Information is $500.00 per copy.

E. Implementation ID
The Adopter ID will be provided free of charge.

1. PROCEDURES FOR HANDLING DTCP2 DEVICE CERTIFICATES AND DTCP2 DEVICE KEYS

Private DTCP2 Device Keys and random seed values associated with the keying material are Highly Confidential Information and Adopters must protect them from exposure and loss using methods that equivalent to or exceed that which is used by DTLA to deliver them to the Adopter and at a minimum that they are kept in a secure controlled environment with controlled access.

2. PROCEDURE FOR ORDERING DTCP2 DEVICE CERTIFICATES AND DTCP2 DEVICE KEYS; REQUIREMENTS FOR USE OF COMMON DTCP2 DEVICE CERTIFICATES AND COMMON DTCP2 DEVICE KEYS

2.1 Adopter will be supplied with a form and associated tools for ordering DTCP2 Device Certificates and DTCP2 Device Keys. As set out in the DTCP2 Specification, such DTCP2 Device Certificates will reflect certain capabilities of the device into which they are intended to be installed. The number of DTCP2 Device Certificates and DTCP2 Device Keys which may be ordered will be constrained to the Adopter's reasonably anticipated production run rate.

2.2 Common DTCP2 Device Certificates and common DTCP2 Device Keys may be used only in Licensed Products or Robust Licensed Components

(i) where

(x) such common DTCP2 Device Keys and common DTCP2 Device Certificates are (a) implemented in software, firmware or a combination of software and firmware; and (b) are or will be capable of being replaced, via an Update, by valid DTCP2 Device Certificates and valid DTCP2 Device Keys, including if and when such original common DTCP2 Device Keys and common DTCP2 Device Certificates are Revoked; and

(y) the DTCP2 functions in each individual unit or copy of such Licensed Product or of a Licensed Product incorporating such Robust Licensed Component cease to function no later than one (1) year after the DTCP2 functions of such unit or copy first functioned, unless the common DTCP2 Device Key and corresponding common DTCP2 Device Certificate in such individual units or copies were sooner replaced via an Update, in which event the DTCP2 functions shall cease to function no later than one (1) year from the date of such replacement or any subsequent replacement via an Update. Without limiting the last sentence of Section 2.3 of the Agreement, in the event the DTCP2 functions of such individual units or copies so cease to function, Adopter may thereafter reactivate or cause the reactivation of such DTCP2 functions by an Update that replaces the Common DTCP2 Device Key and corresponding Common DTCP2 Device Certificate in such unit or copy with a new DTCP2 Device Key and corresponding DTCP2 Device Certificate, in which event the DTCP2 functions shall cease to function no later than one (1) year after such replacement or any subsequent replacement via an Update; and

(z) each such Common DTCP2 Device Certificate and Common DTCP2 Device Key is not used in connection with the activation of the DTCP2 functions of a Licensed Product more than one (1) year after the first activation of a Licensed Product using such Common DTCP2 Device Certificate and Common DTCP2 Device Key;

or

(ii) that are not capable of performing Sink Functions (and, in the case of Robust Licensed Components, not capable of becoming or being incorporated into Licensed Products that perform

Sink Functions), that have Source Functions that are part of remotely-managed devices (e.g., set-top boxes, smartcard-controlled devices or devices using renewable software), and that have Common DTCP2 Device Keys and Common DTCP2 Device Certificates that are capable of being replaced, via an Update, by valid DTCP2 Device Keys and valid DTCP2 Device Certificates if and when such original Common DTCP2 Device Keys and Common DTCP2 Device Certificates are revoked.

3. IMPLEMENTATION ID PROCEDURES AND REQUIREMENTS

3.1 As set forth in the DTCP2 Specification, the Implementation ID consists of an Adopter ID assigned by DTLA to Adopter, and an Implementation identification number uniquely assigned by Adopter to each Implementation in its Licensed Products.

3.2 Following Activation, DTLA shall assign Adopter a unique Adopter identification number to be used by Adopter in creation of Adopter's Implementation IDs in accordance with the DTCP2 Specification.

3.3 Where, pursuant to Section 5.1 of the Agreement, Adopter uses an Implementation ID, such Implementation ID shall uniquely identify the particular Implementation.

3.3.1 Adopter shall assign a unique Implementation identification number to each unique Implementation. Different Implementations shall not use the same Implementation ID.

3.3.2 The Implementation identification number created by Adopter shall not consist of all zeroes (0s) or ones (1s).

3.3.3 DTLA recommends that Adopter number its Implementation identification numbers beginning as [00...1].

Adopter acknowledges that it has read and understands the requirements for usage of the Implementation ID under the Agreement, including Sections 2.4, 4.2.2, and 5 of the Agreement and this Section 3 of the Procedural Appendix. Adopter further acknowledges its obligations, where an Implementation ID is used, to assign a different Implementation ID to each different Implementation and to use the correct Implementation ID for the Implementation used in each Licensed Product.

3.4 Adopter shall register with DTLA each Implementation ID, using the form provided by DTLA, within 30 business days of its first use in any commercially-distributed Licensed Products.

4. ROBUSTNESS VERIFICATION LIST FOR THIRD PARTY REVIEW AND RENEWABLE PRODUCTS.

***Reference Note**: The Robustness Verification Lists and additional requirements pertinent to the Robustness Verification List are set forth in Exhibit C Robustness Rules. "L1 protection" and "L2 protection" are defined in Exhibit B Audiovisual: Compliance Rules for DTCP2 – Introduction.*

If Adopter elects to submit an Implementation (or portion thereof) to Third Party Review pursuant to Section 4.3 of the Agreement, the terms of Section 4.1-4.3 below shall apply with respect to such Implementation. If Adopter elects to make a Renewable or Partially Renewable Implementation

pursuant to Section 4.2 of the Agreement, the terms of Section 4.4 below shall apply with respect to such Implementation.

4.1 **Approved Third Party Review Facilities.** DTLA shall make available to Adopter a list of third party facilities that have been approved by DTLA for Third Party Review (each, a "Third Party Robustness Authority") in accordance with Section 4.3 of the Agreement.

4.2 **Robustness Verification List**. The Robustness Verification List shall be completed by Adopter for each Implementation (or portion thereof) for which Adopter seeks Third Party Review. DTLA may amend the Robustness Verification List form from time to time in accordance with Section 3.3 of the Agreement.

4.3 **Submission of Robustness Verification List to Third Party Robustness Authority.**

4.3.1 If an Implementation (or portion thereof) is submitted to Third Party Review, Adopter shall comply with the terms below in this Section 4.3.1.

4.3.1.1 Adopter shall submit to a Third Party Robustness Authority a separate Robustness Verification List for each Implementation that it submits for Third Party Review. Adopter concurrently shall provide to the Third Party Robustness Authority additional documentation supporting Adopter's responses in the Robustness Verification List ("Supporting Documentation"), and upon request by the Third Party Robustness Authority, any additional Supporting Documentation that the Third Party Robustness Authority reasonably requires to allow the assessment of whether Adopter's responses set forth in the completed Robustness Verification List indicate the Implementation's compliance with the applicable DTCP2 Robustness Rules. If Adopter does not wish to request review of a Partially Renewable portion of an Implementation, it shall so inform the Third Party Robustness Authority and clearly identify such Partially Renewable portion.

4.3.1.2 Following successful completion of such review, Adopter shall obtain from the Third Party Robustness Authority a Certificate affirming that the Robustness Verification List accurately describes the compliance of the Implementation (or portion thereof). Adopter shall maintain a copy of such Certificate, all Supporting Documentation that Adopter submits to the Third Party Robustness Authority, and any Notices received from the Third Party Robustness Authority and any responses thereto by Adopter, until three (3) years following the earlier of the cessation of manufacture or distribution by or on behalf of Adopter of products using the Implementation addressed in such report, or of the termination of the Agreement.

4.4 **Submission of Robustness Verification List for Renewable Products to DTLA.** If an Implementation is Renewable or Partially Renewable and has not been submitted by Adopter for Third Party Review (pursuant to Section 4.3.1), Adopter shall complete and submit to DTLA, prior to the first distribution of the first product embodying such Implementation, a Robustness Verification List that accurately describes the compliance of all Renewable portions of the Implementation, signed and dated by an individual designated by Adopter who has managerial responsibility for the

manufacture of such product. Adopter shall maintain documentation used to support each response on the Robustness Verification List until three (3) years following the earlier of the cessation of manufacture or distribution by or on behalf of Adopter of products using the Implementation addressed in such Robustness Verification List, or of the termination of the Agreement.

5. REVOCATION PROCEDURES

The procedures set forth in this Section 5 shall apply to Revocation other than Revocation of Common DTCP2 Device Certificates as contemplated in the last sentence of Section 5.4 of the Agreement.

5.1 Notice of Revocation. In the event that Revocation is requested, DTLA shall provide any Fellow DTCP2 Adopter to whom DTLA or its designee had issued a DTCP2 Device Certificate for which Revocation has been requested with notice of such requested Revocation, provided, however, that DTLA may, in its sole discretion, reduce such notice period where it deems circumstances warrant. If Adopter notifies DTLA in writing that Adopter consents to such Revocation of any DTCP2 Device Certificate issued to it hereunder, or if DTLA is required to Revoke pursuant to Section 5.2.3 of the Agreement, DTLA may take steps to Revoke the applicable DTCP2 Device Certificate.

5.2 Assent to Revocation/Dispute Resolution.

5.2.1 No more than fifteen (15) calendar days after the date of notice from DTLA, Adopter shall notify DTLA whether Adopter desires to contest the grounds for such Revocation. If Adopter notifies DTLA that it does not wish to contest the requested Revocation, or if Adopter fails to respond timely to the notice from DTLA, the Revocation shall be deemed to be without objection (each a "Constructive Revocation Determination") and may proceed. If Adopter timely notifies DTLA of its intent to object to the requested Revocation, Adopter shall submit a written statement, under oath, which sets out any facts which disprove or contradict DTLA's stated grounds for Revocation ("Revocation Objection"). Within ten (10) business days after receipt of the Revocation Objection, DTLA shall provide notice of the Revocation Objection and the Revocation Objection itself to the entity that requested the Revocation. Within thirty (30) days after receipt from the DTLA of the notice of the Revocation Objection, the entity or entities that requested Revocation (the "Revocation Initiators") may initiate an arbitration in accordance with the provisions of Section 5.4 to determine whether the requested Revocation may proceed.

5.2.2 **Request for Revocation**. Adopter may seek Revocation by providing proof in a sworn affidavit (the "Adopter Affidavit") of any of the facts relating to any particular DTCP2 Device Certificate and/or associated DTCP2 Device Keys issued to Adopter hereunder that would warrant Revocation of such certificate and satisfy one or more of the DTCP2 Revocation Criteria. The Adopter Affidavit shall be sufficiently detailed that DTLA can determine solely on the basis of such affidavit whether the facts averred on their face would satisfy one or more of the DTCP2 Revocation Criteria.

5.3 Indemnification. If Adopter has sought Revocation, it shall indemnify and hold harmless and, at DTLA's option, defend DTLA, the Founders, Generator, any Content Participant that carries the Revocation Information applicable to such Revocation and each of their officers, directors, equivalent corporate officials, employees, representatives and agents ("Indemnified Parties") from and against any and all (i) claims, actions, suits, proceedings or litigation and any losses, deficiencies, damages, liabilities, costs and expenses associated therewith, including but not limited to reasonable attorneys' fees and expenses, arising out of the Revocation or rescission of Revocation of any DTCP2 Device Certificate for which Adopter had sought Revocation and (ii) other costs or expenses incurred by DTLA and/or such Content Participant in connection with such Revocation or rescission of Revocation, including but not limited to any costs and expenses associated with the generation and distribution of information necessary to effect such revocation or rescission and any amounts paid by DTLA to Adopters (or to Adopters' affected customers) or any other party on account of such Revocation. DTLA may require a bond or security reasonably anticipated for such costs.

5.4 Arbitration Procedures.

5.4.1 The parties to the arbitration shall be the Revocation Initiators, the affected Fellow DTCP2 Adopter(s), if any, that objected to the Revocation in accordance with their respective DTCP2 Adopter Agreement and/or any affected person or entity that such Fellow DTCP2 Adopter(s) may designate (such Fellow DTCP2 Adopters and designees, collectively, the "Affected DTCP2 Adopters") and/or at its election, DTLA (collectively, the "Arbitrating Parties"). The Revocation Initiators shall bear the burden of proof in demonstrating, by a preponderance of the evidence, that one or more of the DTCP2 Revocation Criteria have been satisfied.

5.4.2 There shall be a sole arbitrator, who shall be selected by the Arbitrating Parties from the National Panel of Commercial Arbitrators of the American Arbitration Association within fourteen (14) days of the initiation of arbitration; provided, however, that in the event the Arbitrating Parties cannot agree on a sole arbitrator within such fourteen (14)-day period, the Revocation Initiators, on the one hand, and the other Arbitrating Parties, on the other hand, shall each, promptly thereafter, select one arbitrator from the National Panel of Commercial Arbitrators of the American Arbitration Association and those two arbitrators shall jointly select a third arbitrator from the National Panel of Commercial Arbitrators of the American Arbitration Association, who shall serve as the presiding arbitrator and chairperson of such arbitration.

5.4.3 The arbitration shall be conducted in Los Angeles, California, in accordance with the International Arbitration Rules of the American Arbitration Association. The language of the arbitration shall be English.

5.4.4 The arbitrator(s) may conduct the arbitration in such manner as he, she or they shall deem appropriate, including the imposition of time limits that he, she or they consider(s) reasonable for each phase of the proceeding, but with due regard for the need to act, and make a final determination, in an expeditious manner. The arbitrator(s) shall set a schedule to endeavor to complete the arbitration within one (1) month.

5.4.5 The arbitrator(s) shall permit and facilitate such limited discovery as he, she or they shall determine is reasonably necessary, taking into account the needs of the Arbitrating Parties and the desirability of making discovery as expeditious and cost-effective as possible,

recognizing the need to discover relevant information and that only one party may have such information.

5.4.6 The Arbitrating Parties and the arbitrator(s) shall treat the arbitration proceedings, any related discovery, documents and other evidence submitted to, and the decision of, the arbitrator(s) as Confidential Information. In addition, and as necessary, the arbitrator(s) may issue orders to protect the confidentiality of proprietary information, trade secrets and other sensitive information disclosed in discovery or otherwise during the arbitration.

5.4.7 Any decision by the arbitrator(s) shall be final and binding on the Arbitrating Parties, except that whether the arbitrator(s) exceeded his, her or their authority, as specifically described in the Agreement, shall be fully reviewable by a court of competent jurisdiction. Judgment upon any award shall be entered in a court of competent jurisdiction.

5.4.8 The arbitrator(s) shall be compensated at his, her or their hourly rates, determined at the time of appointment, for all time spent in connection with the arbitration, and shall be reimbursed for reasonable travel and other expenses. The arbitrator(s) shall determine all costs of the arbitration, including the arbitrator(s)' fees and expenses, the costs of expert advice and other assistance engaged by the arbitrator(s), the cost of a transcript and the costs of meeting and hearing facilities.

5.4.9 The arbitrator(s) is (are) empowered solely to determine (a) whether one or more of the DTCP2 Revocation Criteria have been satisfied and (b) if so, only in the circumstance set forth in clause (x) of this Section 5.4.9, whether Revocation is warranted. Any such determination by the arbitrator(s) shall be final and binding on the parties to the arbitration and on DTLA if it is not a party to the arbitration, except that whether the arbitrator(s) exceeded his, her or their, authority as specifically described in this Section 5.4.9 shall be fully reviewable by a court of competent jurisdiction. In any such arbitration, the Affected DTCP2 Adopter(s), if any, may introduce evidence solely to support the position that one or more of the DTCP2 Revocation Criteria have not been satisfied. In the event that the Arbitrator(s) determine(s) that the DTCP2 Revocation Criteria set forth in Section 5.2.2 of the Agreement have been satisfied, (x) if DTLA is a party to the arbitration and objects to Revocation, it shall have the burden of demonstrating, by a preponderance of the evidence, that Revocation is not warranted, and if DTLA fails to meet such burden, Revocation shall be deemed warranted and (y) if DTLA is not a party to the arbitration, Revocation shall be deemed to be warranted. In the event that the arbitrator(s) determine(s) that the Revocation Criteria set forth in Section 5.2.1 of the Agreement have been satisfied, Revocation shall be deemed warranted.

5.4.10 All costs and fees shall be shared equally as between the Revocation Initiators, on the one hand, and the Affected DTCP2 Adopters, if any, that participate in the arbitration, on the other, provided, however, the arbitrator(s) may otherwise apportion such costs and fees among such Revocation Initiators and Affected DTCP2 Adopters, if any, as the arbitrator(s) may determine.

5.4.11 The prevailing party in such arbitration shall provide to DTLA a copy of the arbitrator(s) decision. If, pursuant to this Section 5.4, Revocation is warranted or if the arbitrator(s) determine the DTCP2 Revocation Criteria 5.2.4 or 5.2.5 have been satisfied, DTLA may, after it receives such decision, take steps to cause such Revocation, subject to the requirements of Section 5 of the Agreement.

6. PROCEDURES FOR THIRD PARTY BENEFICIARY CLAIMS

6.1 Prior to initiating or instituting any third-party-beneficiary claim by a Fellow DTCP2 Adopter ("DTCP2 Adopter Beneficiary Claim") or by a Content Participant ("Content Participant Beneficiary Claim") (each, a "Beneficiary Claim") against Adopter, any other Fellow DTCP2 Adopter or a Content Participant, as the case may be (each, a "Defendant"), a Content Participant Beneficiary (defined below) or DTCP2 Adopter Beneficiary (defined below) (each, a "Third-Party Beneficiary") shall provide DTLA notice and consultation reasonable under the circumstances regarding a proposed Beneficiary Claim; provided that such consultation with DTLA shall not affect such Third-Party Beneficiary's discretion in initiating such a Beneficiary Claim. Such Third-Party Beneficiary shall further provide DTLA with notice of actual filing of a Beneficiary Claim and, upon DTLA's request, any copies of material documents to be filed in such Third-Party Beneficiary's initiation or pursuit of such Beneficiary Claim. DTLA shall cooperate reasonably with such Third-Party Beneficiary in providing appropriate and necessary information in connection with the Beneficiary Claim to the extent that such cooperation is consistent with the preservation of the integrity and security of DTCP2 and to the extent such cooperation does not involve release of information provided to DTLA by a Content Participant or Fellow DTCP2 Adopter that such Content Participant or Fellow DTCP2 Adopter has designated to DTLA to be its confidential and proprietary information. Documents provided to DTLA under these third-party-beneficiary procedures shall not include any documents filed or to be filed under seal in connection with such Beneficiary Claim.

6.1.1 "DTCP2 Adopter Beneficiaries" means Adopter (for so long as Adopter is in compliance with all of the terms and conditions of the Agreement), together with any one (or more) other Fellow DTCP2 Adopters that is (or are) eligible to bring third-party-beneficiary claims in accordance with a Content Participant Agreement.

6.1.2 "Content Participant Beneficiaries" means any one (or more) Content Participant(s) that is (or are) eligible to bring third-party-beneficiary claims against Adopter in accordance with Section 11.6 of the Agreement or against other Fellow DTCP2 Adopters in accordance with comparable provisions of their respective DTCP2 Adopter Agreements.

6.2 DTLA shall provide all Fellow DTCP2 Adopters (in the case of a DTCP2 Adopter Beneficiary Claim) and all Content Participants (in the case of a Content Participant Beneficiary Claim) with prompt notice of DTLA's receipt of any notice of a Beneficiary Claim against a Defendant (a "Claim Notice"). Within thirty (30) days of the date of mailing of a Claim Notice, all DTCP2 Adopter Beneficiaries (in the case of an DTCP2 Adopter Beneficiary Claim), or all Content Participant Beneficiaries (in the case of a Content Participant Beneficiary Claim), shall elect whether to join such Beneficiary Claim, and the failure of any Fellow DTCP2 Adopter or Content Participant to provide written notice to DTLA of such election and to move to join such Beneficiary Claim within such thirty (30)-day period shall be deemed a waiver of such Fellow DTCP2 Adopter's or Content Participant's third-party-beneficiary right under its respective DTCP2 Adopter Agreement or Content Participant Agreement, as the case may be, with respect to all Beneficiary Claims against Defendant arising out of the alleged breach by Defendant raised in such Beneficiary Claim asserted by the Third-Party Beneficiary. The Third-Party Beneficiary instituting or initiating a Beneficiary Claim shall support, and Defendant shall not object to, any motion to so join by such Third-Party Beneficiaries electing to join such Beneficiary Claim within such thirty (30)-day period. Any judgment entered upon such Beneficiary Claim shall be binding on all Fellow DTCP2 Adopters and

Content Participants that failed to join such Beneficiary Claim as if they had joined such Beneficiary Claim. Neither any Fellow DTCP2 Adopter's or Content Participant's failure to notify or consult with or to provide copies to DTLA, nor DTLA's failure to give notice to any Fellow DTCP2 Adopter or Content Participant pursuant to these third-party-beneficiary procedures, shall be a defense against any Beneficiary Claim or grounds for a request to delay the granting of any preliminary relief requested.

6.3 Third-Party Beneficiaries shall have no right to, and Adopter agrees that it will not, enter into any settlement that: (i) amends any material term of any DTCP2 Adopter Agreement or Content Participant Agreement; (ii) has an adverse effect on the integrity, performance and/or security of DTCP2 or on the operation of DTCP2 with respect to protecting Commercial Audiovisual Content from any unauthorized output, transmission, interception or copying, or the rights of Content Participants with respect to DTCP2; or (iii) affects any of DTLA's or the Founders' rights in and to DTCP2 or any intellectual property right embodied therein, unless DTLA shall have provided prior written consent thereto.

6.4 Nothing contained in these third-party-beneficiary procedures is intended to limit remedies or relief available pursuant to statutory or other claims that a Third-Party Beneficiary may have under separate legal authority.

EXHIBIT "A"
CONFIDENTIALITY AGREEMENT

1. PERMITTED USE.

1.1 For avoidance of doubt, all references to "Proprietary Information" in this Agreement shall be deemed to include Confidential Information and Highly Confidential Information.

1.2 **Use Restrictions**.

1.2.1 Adopter shall use Proprietary Information (and tangible embodiments thereof) solely for purposes of its own implementation of DTCP2 in accordance with the terms of this Agreement, and shall not intentionally copy, and shall not intentionally memorize, Proprietary Information in order to copy the methods disclosed therein.

1.2.2 Adopter shall not use any mentally-retained recollections of Proprietary information to circumvent the methods disclosed in Proprietary Information or to circumvent any obligations under this Agreement.

1.3 The use restrictions contained in Section 1.2.1 of this Confidentiality Agreement shall not apply to Proprietary Information that Adopter can demonstrate is or becomes or has become generally known to the public through no breach of Adopter's obligations owed to DTLA hereunder or the Founders and which DTLA failed to remove from public availability or to enjoin such public disclosure within 120 days after the date such information is or becomes generally known as set forth above; provided, that nothing in this Section 1.3 shall be deemed to create a license (express, implied, or otherwise) under any intellectual property right of DTLA or the Founders with respect to the use of such Proprietary Information.

2. CONFIDENTIALITY.

2.1 **Highly Confidential Information.** Adopter shall maintain the confidentiality of Highly Confidential Information in the following manner:

2.1.1 Adopter shall employ procedures for safeguarding Highly Confidential Information at least as rigorous as Adopter would employ for its own most highly confidential information, such procedures to include, at a minimum: (1) maintaining on Adopter's premises a secure location in which any and all Highly Confidential Information shall be stored; (2) such secure location shall be accessible only by authorized employees; (3) employees shall sign in and out each time such employees visit such secure location; and (4) when Highly Confidential Information is not in use, such information shall be stored in a locked safe at such secure location.

2.1.2 Adopter may disseminate Highly Confidential Information only to (a) the strictest minimum possible number of regular employees and individuals retained as regular independent contractors subject to confidentiality obligations equivalent to those applicable to regular employees of Adopter: (1) who have an absolute need to know such Highly Confidential Information in order to enable Adopter to implement DTCP2 in compliance with the DTCP2 Specification; and, (2) who are bound in writing by obligations of

confidentiality sufficient to protect the Highly Confidential Information in accordance with the terms of this Agreement; provided that Adopter shall be liable to DTLA for any failure by any such employee or individual to maintain the confidentiality of Confidential Information in accordance with the terms of this Confidentiality Agreement; and, (b) a third party that is providing services to Adopter pursuant to the right under Section 6.2 of the Agreement to "have made" Licensed Products or Licensed Components, provided that such third party is either a Fellow DTCP2 Adopter or has executed a nondisclosure agreement with DTLA consistent with the provisions hereof that authorizes such third party to receive such Highly Confidential Information.

2.1.3 Adopter shall not make any copies of any Highly Confidential Information, except where (i) copying of Cryptographic Constants which are Highly Confidential Information is necessary for the production process of Licensed Component or Licensed Product, or (ii) Adopter has a secure document access control system which provides security level equivalent to what is required in this section 2.1, in which case Adopter may scan the DTLA Highly Confidential Information into their system. Adopters may also request additional copies of DTCP2 Specification documents which are Highly Confidential Information, and DTLA may in its sole discretion fulfill any such request.

2.2 **Confidential Information**. Adopter may disclose Confidential Information only to (i) regular employees and individuals retained as independent contractors subject to confidentiality obligations equivalent to those applicable to regular employees of Adopter who have a reasonable need-to-know and are bound in writing by obligations of confidentiality sufficient to protect the Confidential Information in accordance with the terms of this Agreement, (ii) Fellow DTCP2 Adopters, (iii) entities subject to a non-disclosure agreement with DTLA or Adopter that includes provisions substantially in the form of the provisions of this Confidentiality Agreement that relate to Confidential Information, provided that Adopter may disclose to such parties only information that such parties are entitled to receive under their DTCP2 Adopter Agreement or nondisclosure agreement and, in the event that any such entity is not a Fellow DTCP2 Adopter, Adopter shall be liable for any failure by such entity to maintain the confidentiality of Confidential Information in accordance with the terms of this Confidentiality Agreement; or (iv) Adopter's attorneys, auditors or other agents who owe Adopter a duty of confidentiality and are bound to maintain such information in confidence as a result of a fiduciary relationship. Adopter shall use the same degree of care, but no less than a reasonable degree of care, to avoid unauthorized disclosure or use of Confidential Information as such party employs with respect to its comparably important confidential information. Notwithstanding the foregoing, Adopter and DTLA may disclose Adopter's status (or lack of it) as a licensee of DTCP2, and such disclosure shall not constitute Confidential Information.

3. GENERAL.

3.1 Adopter shall make all reasonable efforts to assist DTLA in relation to any claim, action, suit, proceeding, or litigation with respect to any improper or unauthorized acts of any of its former employees or of such third parties identified in Section 2.1 and 2.2 of this Confidentiality Agreement.

3.2 Contact Person and Provision of DTCP2 Information. Adopter shall designate a single main employee contact and an alternate employee license contact who shall receive all Confidential Information and Highly Confidential Information (the "Adopter Contact(s)") disclosed by DTLA.

3.3 Notification of Unauthorized Use or Disclosure. Adopter shall notify DTLA in writing immediately upon discovery of any unauthorized use of Proprietary Information and any unauthorized disclosure of Confidential Information or Highly Confidential Information, and will cooperate with DTLA in every reasonable way to regain possession of Confidential Information and Highly Confidential Information and prevent its further unauthorized disclosure and to prevent further unauthorized use of Proprietary Information.

3.4 **Disclosure Required by Law.** If Adopter is required by law, regulation or order of a court or other authority of competent jurisdiction to disclose Confidential Information or Highly Confidential Information, Adopter shall notify DTLA as promptly as possible, and shall, upon such DTLA's request, reasonably cooperate in challenging or restricting the scope of such required disclosure.

3.5 **Confidentiality Exceptions**. The confidentiality restrictions contained in Section 2.1 and 2.2 of this Confidentiality Agreement shall not apply to information that Adopter can demonstrate: (i) is either Confidential or Highly Confidential Information which is or becomes or has become generally known to the public through no breach of Adopter's obligations owed to DTLA hereunder or the Founders and which DTLA failed to remove from public availability or to enjoin such public disclosure within 120 days after the date such information is or becomes generally known as set forth above; or (ii) is or has been developed by Adopter's employees (whether independently or jointly with others) without having reliance on or use of (whether directly or through any intermediaries) to any such Confidential Information or Highly Confidential Information (or any translation, derivation or abstractions of Confidential Information or Highly Confidential Information) and without any breach of Adopter's obligations to DTLA or the Founders, provided that the confidentiality restrictions shall continue to apply to DTCP2 Device Keys provided to Adopter; or (iii) is or has been disclosed to Adopter by a third party which had developed (whether independently or jointly with others) such information without reliance on or use of (whether directly or through any intermediaries) to any Confidential Information or Highly Confidential Information and without any breach of any such third party's obligations to DTLA or the Founders.

4. PERIOD.

The confidentiality obligations set forth herein shall continue until the later of (i) three (3) years after the last commercial use of DTCP2 by DTLA or any Fellow DTCP2 Adopter; or (ii) the expiration of the last copyright that protects any DTCP2-encrypted/scrambled content which then exists in any country adhering to the Agreement on Trade Related Aspects of Intellectual Property Rights of the World Trade Organization dated April 15, 1994.

5. OTHER TERMS.

Nothing herein shall be construed as an inducement or license for Adopter to reverse engineer any products of any Adopter or third party.

EXHIBIT "B": COMPLIANCE RULES FOR DTCP2

This Exhibit B is divided into two portions: "Exhibit B Audiovisual" and "Exhibit B Audio."

EXHIBIT B AUDIOVISUAL: COMPLIANCE RULES FOR DTCP2
INTRODUCTION

1. GENERALLY

1.1 This Exhibit B Audiovisual (the "Compliance Rules Audiovisual") is divided into separate Parts, which may be applicable, depending on the nature of the Licensed Product, and, in particular, on whether it has Sink Functions or Source Functions (Parts 1 and 2, respectively). The definitions in this Introduction to Exhibit B Audiovisual apply to each Part of this Exhibit B Audiovisual. Unless otherwise expressly provided, for purposes of this Exhibit B Audiovisual, all section references in any Part of this Exhibit B Audiovisual shall be deemed references to sections in such Part. For purposes of this Exhibit B Audiovisual, all references below to "Exhibit B" shall be deemed references to this Exhibit B Audiovisual.

1.2 **Implementation and Robustness.** Licensed Products shall comply with the requirements of the DTCP2 Specification, this Exhibit B and Exhibit C. Where these Compliance Rules require the application of L2 protection (defined below), Licensed Products shall comply with the requirements of the DTCP2 Specification, this Exhibit B and Exhibit C applicable to L2 protection. Where these Compliance Rules permit the application of L1 protection (defined below), Licensed Products shall comply with the requirements of the DTCP2 Specification, this Exhibit B and Exhibit C applicable to either L1 protection or L2 protection.

1.3 **Types of Functions**

1.3.1 "**Sink Function**" means the function of a Licensed Product to use DTCP2 to receive and decrypt Commercial Entertainment Content.

1.3.2 "**Source Function**" means the function of a Licensed Product to use DTCP2 to encrypt and transmit Commercial Entertainment Content.

1.3.3 A Licensed Product may have both Source Functions and Sink Functions. In such a case, the requirements applicable to Source Functions and Sink Functions shall apply to the respective portions of such Licensed Product.

2. DEFINITIONS

Harmonization. Where a capitalized term is used but not otherwise defined in this Exhibit B, the meaning ascribed thereto elsewhere in the Agreement shall apply.

2.1 "Analog Sunset Content" shall mean Decrypted AACS Content.

2.2 "Analog Sunset Token" shall mean the Analog Sunset Token defined in the DTCP2 Specification, used to trigger certain restrictions on the analog output of Analog Sunset Content in Licensed Products having Sink Functions.

2.3 "Analog Sunset Token Content" shall mean Decrypted DT Data for which the Analog Sunset Token has been asserted.

2.4 "Audio Enhancement Token" shall mean the Audio Enhancement Token defined in the DTCP2 Specification, that is used to indicate permission to transmit in a digital form the audio portion of Decrypted DT Data sampled at greater than 48 kHz and more than 16 bits but no greater than 192 kHz and no more than 24 bits.

2.5 "BF Eligible Broadcast Television" shall mean the transmission of any service, Program or schedule of Programs, via an unencrypted digital terrestrial broadcast television transmission originating in any Broadcast Flag Jurisdiction and any substantially simultaneous re-transmission thereof made by an entity located within the country or territory in which the broadcast originated, regardless of whether such entity subjects such further transmission to an access control method.

2.6 "Bound CC Recording" shall have the meaning given in Section 2.8.2 of Part 1 of this Exhibit B.

2.7 "Broadcast Flag" shall mean, (i) for unencrypted digital terrestrial broadcast television transmissions originating in the United States, its territories and possessions, and associated commonwealths under the jurisdiction of the Federal Communications Commission, the Redistribution Control descriptor (rc_descriptor()) described in ATSC Standard A/65B: "Program and System Information Protocol for Terrestrial Broadcast and Cable" and (ii) for unencrypted digital terrestrial broadcast television transmissions originating in any other jurisdiction in which a similar law or regulation requires consumer electronics products and information technology products to respond to a flag or trigger associated with such transmissions so as to restrict unauthorized redistribution of such transmissions (such jurisdictions referenced in clauses (i) and (ii), collectively, "Broadcast Flag Jurisdictions"), such flag or trigger so identified in such law or regulation.

2.8 "Broadcast Flag Jurisdiction" shall have the meaning set forth in the definition of "Broadcast Flag."

2.9 "CC Content" shall mean an instance of Digital Entertainment Content that is associated with information indicating the Number of Permitted CC Copies for such instance of content. For the avoidance of doubt, CC Content includes content that, when Transferred from a Source Device to a Sink Device, is associated with a valid CC Field.

2.10 "CC Field" shall mean the field set out in the DTCP2 Specification for the Copy Count function indicating, with respect to CC Content when Transferred from a Source Device to a Sink Device, the Number of Permitted CC Copies for such content. For purposes of these Compliance Rules, a setting of the CC Field to "invalid" (0000) indicates the Number of Permitted CC Copies is not being sent to the Sink Function, and a "valid" setting of the CC Field means a setting greater than or equal to 1.

2.11 "Commercial Advertising Messages" shall mean, with respect to any service, Program, or schedule or group of Programs, commercial advertising messages other than advertising relating to such service itself or the programming contained therein, or the programming of Content Participant, or any of its Affiliates, or any advertising which is displayed concurrently with the display of any part of such Program(s), including but not limited to "bugs," "frames" and "banners."

2.12 "Commercial Audiovisual Content" shall mean Commercial Entertainment Content in the form of audiovisual works, as defined in 17 U.S.C. § 101.

2.13 "Commercial Entertainment Content" shall mean works, including audio, video, text and/or graphics, that are (a) not created by the user of the Licensed Product; (b) offered for transmission, delivery or distribution, either generally or on demand, to subscribers or purchasers or the public at large, or otherwise for commercial purposes, not uniquely to an individual or a small, private group; and (c) received (i) by a Commercially-Adopted Access Control Method or (ii) as BF Eligible Broadcast Television marked with the applicable Broadcast Flag for the Broadcast Flag Jurisdiction in which such broadcast originated, or (iii) over a Protected Free-to-Air System.

2.14 "Commercially-Adopted Access Control Method" shall mean any commercially-adopted access control method, such as CSS, Digicypher, Harmony, DBS and other commercially-adopted access control technology, including digitally-controlled analog scrambling systems, whether now or hereafter in commercial use.

2.15 "Computer Product" shall mean a device which is designed for or permits the end user to install a wide variety of commercially available software applications thereon including, but not limited to, personal computers, handheld "Personal Digital Assistants," and the like and further includes a subsystem of such a device, such as a graphics card.

2.16 "Conditional Access Delivery" shall mean any delivery of a service, Program, or schedule or group of Programs via a Commercially-Adopted Access Control Method. Without limitation, "Conditional Access Delivery" includes Prerecorded Media; a Pay Television Transmission; Pay-Per-View; Video-on-Demand; Subscription-on-Demand; Non-Premium Subscription Television and Free Conditional Access Delivery. Notwithstanding the foregoing, "Conditional Access Delivery" does not include any service, Program, or schedule or group of Programs, that is a further transmission of a broadcast transmission (i.e., an over-the-air transmission for reception by the general public using radio frequencies allocated for that purpose) that, substantially simultaneously, is made by a terrestrial television broadcast station located within the country or territory in which the entity further transmitting such broadcast transmission also is located, where such broadcast transmission is not subject to a Commercially-Adopted Access Control Method (e.g., is broadcast in the clear and supported by advertising revenues or government mandated fees, without any other charge to members of the public receiving such broadcasts), regardless of whether such entity subjects such further transmission to an access control method. Notwithstanding the foregoing, Conditional Access Delivery shall include any service, Program, or schedule or group of Programs, that both (a) was primarily authored in a format with a resolution equal to or greater than 1000i or 700p ("High Definition") and (b) is transmitted via a Commercially-Adopted Access Control Method in High Definition, provided that such service, Program, or schedule or group of Programs, is not, substantially simultaneously, transmitted in High Definition by a terrestrial broadcast station located within the same country or territory, where such broadcast transmission is not subject to a Commercially-Adopted Access Control Method.

2.17 "Consensus Watermark" shall mean the watermark technology designated as the "Consensus Watermark" by DTLA.

2.18 "Constrained Image" shall mean an image having the visual equivalent of no more than 520,000 pixels per frame (e.g., an image with resolution of 960 pixels by 540 pixels for a 16:9 aspect ratio). A Constrained Image may be attained by reducing resolution, for example, by discarding, dithering, or averaging pixels to obtain the specified value. A Constrained Image can be displayed using video processing techniques such as line doubling or sharpening to improve the perceived quality of the image. By way of example, a Constrained Image may be stretched or doubled, and displayed full-screen, on a 1000-line monitor.

2.19 "Copy Freely" refers to Commercial Entertainment Content which, as set out in the DTCP2 Specification, has been encoded so that copy control using DTCP1 or DTCP2 is not asserted, but which remains subject to the rights of the copyright owner.

2.20 "Copy Never" refers to Commercial Entertainment Content which, as set out in the DTCP2 Specification, has been encoded as "Copy Never" indicating that it is not to be reproduced.

2.21 "Copy One Generation" refers to Commercial Entertainment Content which, as set out in the DTCP2 Specification, has been encoded as "Copy One Generation" indicating that only one generation of copies is to be made of it.

2.22 "Decrypted AACS Content" shall mean audiovisual content that was protected by AACS and is received by a Licensed Product's Source function directly from the AACS decryption function or from a bound copy of such content made in accordance with the "Compliance Rules" of the AACS Adopter Agreement. [NOTE: May need parallel definition after AACS2 approval]

2.23 "Decrypted DT Data" shall mean, with respect to any Licensed Product, DT Data that has been received by such Licensed Product's Sink Function and decrypted by such Licensed Product according to DTCP2 but has not been (a) protected by a one-generation copy protection technology identified or approved by DTLA pursuant to Sections 2.2.1.1 or 2.2.1.3 of Part 1-A or Part 1-B of this Exhibit B; (b) protected by a technology approved by DTLA pursuant to Section 4.4.4 of Part 1-A or Part 1-B of this Exhibit B or (c) passed to an output permitted by Part 1-A or Part 1-B of this Exhibit B.

2.24 "Digital Only Token" or "DOT" shall mean the Digital Only Token field as described in the DTCP2 Specification, used to trigger the limitation of output or recording of Decrypted DT Data.

2.25 "Digital Only Token Content" shall mean Decrypted DT Data for which the DOT field is asserted.

2.26 "DT Data" shall mean Commercial Entertainment Content that has been encrypted and transmitted using DTCP2. For avoidance of doubt, DT Data includes Decrypted DT Data.

2.27 "Enhanced Image" shall mean an audiovisual work with one or more image quality features that measurably surpass the quality of HD Audiovisual Works by using one or more image quality improvement techniques that have not been applied for HD Audiovisual Works, provided that "Enhanced Image" shall not include an image received by a Licensed Product as an HD Audiovisual

Work, or transmitted by a Source as an HD Audiovisual Work, regardless of whether video processing techniques have been or will be used to alter the perceived quality of the image.

2.28 "EI Token" shall mean the EI Token defined in the DTCP2 Specification, that is used to indicate whether an audiovisual work is an Enhanced Image.

2.29 "EPN Field" shall mean the field or bits, described in the DTCP2 Specification, used to indicate that Commercial Audiovisual Content is to be protected using DTCP1 or DTCP2 but that copy control restrictions are not being asserted over such content.

2.30 "FCC Waiver Order" shall mean the Memorandum Opinion and Order of the Media Bureau of the Federal Communications Commission in In the Matter of Motion Picture Association of America, Petition for Expedited Special Relief; Petition for Waiver of the Commission's Prohibition on the Use of Selectable Output Control (47 C.F.R. § 76.1903), CSR-7947-Z, MB Docket No. 08-82 (May 7, 2010).

2.31 "Free Conditional Access Delivery" shall mean a Conditional Access Delivery, as to which viewers are not charged any fee (other than government-mandated fees) for the reception or viewing of the programming contained therein.

2.32 "HD Audiovisual Works" shall mean an audiovisual work with image quality features commonly associated with HD quality at the commencement of the initial licensing of DTCP2. Such qualities include, by way of example, quantity of pixels (i.e. <= 1920x1080 pixels), standard bit depth for HD quality (i.e. 8 bits), frame rate (i.e. <= 60 fps), standard color space for HD quality (i.e. BT.709), and standard peak luminance for HD quality (i.e. 100 cd/m^2). For purposes of clarity, HD Audiovisual Works may include content that has been downconverted from an Enhanced Image to the resolutions specified above for HD Audiovisual Works.

2.33 "HDR Token" shall mean the HDR Token defined in the DTCP2 Specification, that is used to indicate whether certain content with High Dynamic Range may be downconverted to standard dynamic range.

2.34 "High Definition Analog Form" shall mean a format that is an analog video signal which has a resolution greater than a Constrained Image.

2.35 "High Definition Analog Output" shall mean an output capable of transmitting Commercial Audiovisual Content in High Definition Analog Form.

2.36 "Image Constraint Token" shall mean the field or bits, as described in the DTCP2 Specification, used to trigger the output of a "Constrained Image" in Licensed Products having Sink Functions.

2.37 "L1 protection" means (a) in Sink Functions, protection compliant with the requirements of Exhibit B Part 1-A: DTCP2 Compliance Rules for Sink Functions – L1 Protection and Exhibit C Part 1: Robustness Rules for L1 Protection in Licensed Products and (b) in Source Functions, protection

compliant with the requirements of Exhibit B Part 2: DTCP2 Compliance Rules for Source Functions and Exhibit C Part 1: Robustness Rules for L1 Protection in Licensed Products.

2.38 "L2 Only Token" shall mean the L2 Only Token defined in the DTCP2 Specification, that is used to indicate whether audiovisual content shall be protected using L2 protection.

2.39 "L2 protection" means (a) in Sink Functions, protection compliant with the requirements of Exhibit B Part 1-B: DTCP2 Compliance Rules for Sink Functions – L2 Protection and Exhibit C Part 2: Robustness Rules for L2 Protection in Licensed Products and (b) in Source Functions, protection compliant with the requirements of Exhibit B Part 2: DTCP2 Compliance Rules for Source Functions and Exhibit C Part2: Robustness Rules for L2 Protection in Licensed Products.

2.40 "Move" shall mean the transmission of Decrypted DT Data from a Licensed Product that has a Source Function to a Licensed Product that has a Sink Function pursuant to and in accordance with Section 3 of Part 1A, Section 3 of Part 1B and Section 3 of Part 2 of this Exhibit B.

2.41 "No More Copies" refers to Commercial Entertainment Content which, as set out in the DTCP2 Specification, has been encoded as "No More Copies," indicating that it may have originated as Copy One Generation, but that the version being transmitted is from that first generation copy and that therefore no more copies are permitted.

2.42 "Non-Enhanced Image" shall mean an audiovisual work with image quality at or below the image quality of HD Audiovisual Works. For the avoidance of doubt, Non-Enhanced Image includes an audiovisual work that has been downconverted to the image quality of a Non-Enhanced Image from an Enhanced Image as permitted under these Compliance Rules.

2.43 "Non-Premium Subscription Television" shall mean a Conditional Access Delivery of a service, or schedule or group of Programs (which may be offered for sale together with other services, or schedule or group of Programs), for which subscribers are charged a subscription fee for the reception or viewing of the programming contained therein, other than Pay Television Transmission and Subscription-on-Demand. By way of example, "basic cable service" and "extended basic cable service" in the United States (other than such programming contained therein that does not fall within the definition of Conditional Access Delivery) are "Non-Premium Subscription Television.

2.44 "Number of Permitted CC Copies" shall mean, with respect to a particular instance of content, the total number of copies that are associated with and permitted to be made of that instance of content, which number, when associated with a Bound CC Recording or other static copy of such content, shall include such Bound CC Recording or copy. By way of example, when a Sink Device receives CC Content with an associated valid CC Field indicating a Number of Permitted CC Copies of 4 and makes a Bound CC Recording thereof pursuant to Section 2.8 of Part 1 of this Exhibit B, the Number of Permitted CC Copies for such Bound CC Recording shall be 4, indicating that 3 additional copies are permitted.

2.45 "Other EPN Eligible Broadcast Television" shall mean the delivery or transmission of any service, Program, or schedule or group of Programs, that (a) is delivered or transmitted via a

Commercially-Adopted Access Control Method and (b) does not fall within the definition of "Conditional Access Delivery" or "BF Eligible Broadcast Television."

2.46 "Pay-Per-View" shall mean a delivery of a single Program or a specified group of Programs, as to which each such single Program is generally uninterrupted by Commercial Advertising Messages and for which recipients are charged a separate fee for each Program or specified group of Programs. The term "Pay-Per-View" shall also include delivery of a single Program as described above for which multiple start times are made available at time intervals which are less than the running time of such Program as a whole. If a given delivery qualifies both as Pay-Per-View and a Pay Television Transmission, then, for purposes of this Agreement, such delivery shall be deemed Pay-Per-View rather than a Pay Television Transmission.

2.47 "Pay Television Transmission" shall mean a transmission of a service or schedule of Programs, as to which each individual Program is generally uninterrupted by Commercial Advertising Messages and for which service or schedule of Programs subscribing viewers are charged a periodic subscription fee, such as on a monthly basis, for the reception of such programming delivered by such service whether separately or together with other services or programming, during the specified viewing period covered by such fee. If a given delivery qualifies both as a Pay Television Transmission and Pay-Per-View, Video-on-Demand, or Subscription-on-Demand then, for purposes of this Agreement, such delivery shall be deemed Pay-Per-View, Video-on-Demand or Subscription-on-Demand rather than a Pay Television Transmission

2.48 "Prerecorded Media" shall mean the delivery of one or more Programs, in prerecorded and encrypted or scrambled form, on packaged media, such as DVD discs.

2.49 "Program" shall mean any work of Commercial Audiovisual Content.

2.50 "Protected Free-to-Air System" shall mean the United Kingdom High Definition Digital Terrestrial Transmission service and the Freeview New Zealand service. Licensee is advised that DTLA may from time to time amend the Encoding Rules and these Compliance Rules to add additional services to this definition.

2.51 "Remote Access" shall mean the Remote Access function as set out in the DTCP2 Specification that permits the use of DTCP2 to protect transmissions of DT Data to a DTCP Sink Function located outside the physical home network.

2.52 "Retention State Field" shall mean the field or bits, as described in the DTCP2 Specification, used to specify the retention period that is associated with a Program received by a Sink Function.

2.53 "SD Interlace Modes" shall mean composite video, s-video, 480i component video and 576i video.

2.54 "SDO Token" shall mean the SDO (Standard Digital Output) Token, defined in the DTCP2 Specification, that can be used to indicate permission to output Decrypted DT Data, including an Enhanced Image, using permitted outputs in accordance with Section 4.4 to 4.6 of Exhibit B Part 1-

A: DTCP2 Compliance Rules for Sink Functions and Section 4.2 to 4.4 of Exhibit B Part 1-B: DTCP2 Compliance Rules for Sink Functions..

2.55 "Subscription-on-Demand" shall mean the delivery of a single Program or a specified group of Programs for which (i) a subscriber is able, at his or her discretion, to select the time for commencement of exhibition thereof; (ii) where each such single Program is generally uninterrupted by Commercial Advertising Messages; and (iii) for which Program or specified group of Programs subscribing viewers are charged a periodic subscription fee for the reception of programming delivered by such service during the specified viewing period covered by the fee. In the event a given delivery of a Program qualifies both as a Pay Television Transmission and Subscription-on-Demand, then for purposes of this Agreement, such delivery shall be deemed Subscription-on-Demand rather than a Pay Television Transmission.

2.56 "Transfer" shall mean (a) where used as a noun, the transmission of CC Content from a Source Device to one or more Sink Devices that make or enable the making of a persistent copy thereof pursuant to and in accordance with Section 2.8 of Part 1A, Section 2.8 of Part 1B, and Section 4.1 and 4.2 of Part 2 of this Exhibit B, and (b) where used as a verb, the act of making a transmission as described in clause (a).

2.57 "Transitory Image" shall mean data which has been stored temporarily for the sole purpose of enabling the immediate display, processing, or transmission, of content but which (a) does not persist materially after such display, processing, or transmission, and (b) is not stored in a way which permits copying or storing of such data for other purposes.

2.58 "Video-on-Demand" shall mean a delivery of a single Program or a specified group of Programs for which (i) each such individual Program is generally uninterrupted by Commercial Advertising Messages; (ii) recipients are charged a separate fee for each such single Program or specified group of Programs; and (iii) a recipient is able, at his or her discretion, to select the time for commencement of exhibition of such individual Program or specified group of Programs. In the event a delivery qualifies as both Video-on-Demand and a Pay Television Transmission, then for purposes of this Agreement, such delivery shall be deemed Video-on-Demand.

EXHIBIT B AUDIOVISUAL, PART 1: DTCP2 COMPLIANCE RULES FOR SINK FUNCTIONS--GENERAL

1. INTRODUCTION

1.1 **Applicability.** This Part 1 of this Exhibit B is applicable to Licensed Products that have a Sink Function. This Part 1 is divided into three sub-Parts: Part 1—General; Part 1-A—L1 Protection; and, Part 1-B—L2 Protection. A Licensed Product may have both Sink Function with L1 protection and Sink Function with L2 protection. In such a case, the requirements applicable to Sink Functions with L1 protection and Sink Functions with L2 protection shall apply to the respective portions of such Licensed Product.

1.2 **Guide and Rules for Application of L1 Protection and L2 Protection.** The Compliance Rules define the interaction of four (4) new tokens – the EI Token, HDR Token, L-2 Only Token, and SDO Token. The rules set forth below prescribe when L1 protection is permitted to be applied, and when L2 protection is required (L2 protection always is permitted).

1.2.1 L1 Protection. **Part 1-A** of this Exhibit B applies to Licensed Products that have a Sink Function that applies L1 protection. L1 protection is permitted to be applied to Decrypted DT Data only where L2-Only Token is set to 0 (not asserted) and EI Token is set to 0 (not asserted)

1.2.2 L2 Protection. **Part 1-B** of this Exhibit B applies to Licensed Products that have a Sink Function that applies L2 protection, in the following cases:

1.2.2.1 L2 protection is permitted to be applied to all Decrypted DT Data.

1.2.2.2 L2 protection is required to be applied to Decrypted DT Data (and L1 protection is not permitted) where—

(A) L2-Only Token is set to 1 (asserted); or,

(B) L2-Only Token is set to 0 (not asserted) and EI Token is set to 1 (asserted).

For the convenience of Adopter, Table 1 below describes when L1 protection is permitted and L2 protection is required and the Compliance Rules results for the token combinations for L1 protection and L2 protection.

Table 1: L1 protection and L2 protection applicability for Compliance Rules

Input status to Sink Function			**L1/L2 protection for Sink**
L2-Only Token	**HDR Token**	**EI Token**	
1 (Asserted)	1 (Asserted)	*Don't care*	• L2 required • *L1 not permitted*
1 (Asserted)	0 (Not Asserted)	*Don't care*	• L2 required • *L1 not permitted*
0 (Not Asserted)	*Don't care*	1 (Asserted)	• L2 required for Enhanced Image • Both L1 and L2 permitted for Non-Enhanced Image after down conversion
0 (Not Asserted)	*Don't care*	0 (Not Asserted)	• Both L1 and L2 permitted

EXHIBIT B AUDIOVISUAL, PART 1-A: DTCP2 COMPLIANCE RULES FOR SINK FUNCTIONS—L1 PROTECTION

1. INTRODUCTION TO PART 1-A

1.1 **Applicability.** This Part 1-A of this Exhibit B is applicable to Licensed Products that have a Sink Function and are capable of protecting Decrypted DT Data using L1 protection, as permitted in accordance with Section 1.2.1 of Part 1 General.

For the convenience of Adopter, Table 1 in Exhibit B, Part 1-General summarizes the combination of settings in cases to which the Compliance Rules for L1 protection in this Exhibit B Part 1-A apply.

NOTE: For clarification, for all cases in which L1 protection is permitted, L2 protection also is permitted.

2. SINK FUNCTION OBLIGATIONS REGARDING PERSISTENT STORAGE OF CONTENT

2.1 **Copy Never.** Licensed Products shall be constructed such that Copy Never DT Data received via their Sink Functions may not, once decrypted, be stored except as a Transitory Image or as otherwise permitted in Section 2.1.1:

2.1.1 Copy Never DT Data may be retained (i.e., stored) for such period as is specified by the Retention State Field, solely for purposes of enabling the delayed display of such DT Data. Such retained DT Data shall be stored using a method set forth in Section 2.2, and shall be obliterated or otherwise rendered unusable upon expiration of such period.

2.2 **Permitted Copy One Generation Copies.** Subject to the requirements of Sections 2.5-2.7, a Licensed Product may not make, or cause to be made, a copy of Copy One Generation Decrypted DT Data unless each copy (a) is made as a Transitory Image or (b) is made using a method set out in Section 2.2.1. A Licensed Product may, alternatively, treat such Decrypted DT Data as Copy Never, provided that no retention under Section 2.1.1 of this Part 1 is permitted.

2.2.1 Subject to the requirements of Sections 2.5-2.7, and except as set forth in Sections 2.2.2 and 2.2.3, a Licensed Product may make, or cause to be made, no more than two (2) first-generation copies of Decrypted DT Data, in different formats of storage device or media, by using only the methods described in Section 2.2.1.1 and Section 2.2.1.2:

2.2.1.1 The copy is made using a copy protection technology (such as scrambling or encryption) that is approved by DTLA now or in the future, as specified on the DTLA website or in a notice to Adopter;

2.2.1.2 The copy is stored using an encryption protocol that uniquely associates such copy with a single Licensed Product so that it cannot be played on another device or that no further usable copies may be made thereof (other than copies made from an output permitted by this Agreement or as otherwise permitted under Section 2.3 of this Part 1 or Section 3 or 4 of Part 2); or

2.2.1.3 Copy One Generation Decrypted DT Data that is copied in a personal video recorder or other bound recording medium pursuant to Section 2.2.1.2 may continue to be treated as Copy One Generation for a period of up to ninety (90) minutes from initial reception of each unit of such data (e.g., frame-by-frame, minute-by-minute, megabyte-by-megabyte, etc.), but in no event shall such unit of data exceed one minute of a Program.

2.2.2 In the event that a Licensed Product supports one (1) or more format(s) of storage devices or media in addition to those in which a copy or copies of Decrypted DT Data are made pursuant to Section 2.2.1, a Licensed Product may make, or cause to be made, one (1) additional first-generation copy of Decrypted DT Data, using any of the methods described in Sections 2.2.1.1 and 2.2.1.2, provided that (a) such DT Data is received by one separate Sink Function having a separate Device Certificate for such additional format of storage device or media and (b) such single copy is made in a format of storage device or media other than a format in which a copy has been made by a recording device supported by another Sink Function in such Licensed Product.

By way of example and not limitation, for purposes of this Section 2.2, the following constitute different formats of storage devices or media: BD-R; MPEG4 HDD recorder; MPEG2 HDD recorder; DVHS; all DVD-recordable having less than 20GB capacity (for example, DVD-RAM, DVD-RW, DVD+RW or DVD-R); SD Card; Memory Stick; Compact Flash; non-removable RAM; and non-removable flash memory.

2.2.3 Each copy made pursuant to Sections 2.2.1, 2.2.2 or 2.4 may be stored on one or more physical storage devices or media, and may include a back-up copy, so long as all such devices, media and back-up copy constitute only a single usable copy (*e.g.*, a back-up copy may be made on HDD or other media and the copy may be stored on RAID-type devices).

2.3 **No More Copies**. A Licensed Product may not make, or cause to be made, an analog copy of Decrypted DT Data that is encoded as No More Copies. A Licensed Product may not make, or cause to be made, a digital copy of any copy of Decrypted DT Data that is encoded as No More Copies except (a) as a Transitory Image, or (b) if the Licensed Product deletes or otherwise renders unusable the original copy such that, at any point in time, only a single useable copy persists as between such original and copy thereof, or (c) in the event that a Licensed Product that has a Sink Function receives DT Data via its Sink Function that was transmitted by a Licensed Product that has a Source Function pursuant to Section 3.1 (b) or 4.2.2 (b) of Part 2 of this Exhibit B.

2.4 **EPN Encoded Content**. Subject to the requirements of Sections 2.5-2.7, a Licensed Product may not make, or cause to be made, a digital copy of Decrypted DT Data for which the associated EPN Field is asserted except (a) as a Transitory Image or (b) if such copy is made using one or more of the methods set out in Section 2.2.1.1 and Section 2.2.1.2. Consistent with the assertion of EPN and with the preceding sentence, a Licensed Product may, subject to the requirements of Sections 2.5-2.6, make, or cause to be made, additional digital copies of Decrypted DT Data for which the associated EPN field has been asserted, provided that each such copy (a) is a Transitory Image or (b) is made using one or more of the methods set out in Section 2.2.1.1 and Section 2.2.1.2. For

clarification, Section 2.2.1.2 shall not be read to limit the number of copies that may be made of EPN encoded content, so long as each copy is made using a method set out in Section 2.2.1.1 and Section 2.2.1.2.

2.5 **Analog Sunset Token Content.** Notwithstanding the terms of Section 2.2-2.4, with respect to Analog Sunset Token Content, the copy protection technologies referenced in Section 2.2.1.1 shall be deemed further restricted to only those copy protection technologies, if any, approved by DTLA for Analog Sunset Token Content, now or in the future, as specified on the DTLA website or in a notice to Adopter.

2.6 **Digital Only Token Content.** Notwithstanding the terms of Section 2.2-2.4, with respect to Digital Only Token Content, the copy protection technologies referenced in Section 2.2.1.1 shall be deemed further restricted to only those copy protection technologies, if any, approved by DTLA for Digital Only Token Content, now or in the future, as specified on the DTLA website or in a notice to Adopter.

2.7 **Remote Access Content.** Notwithstanding the terms of Sections 2.2-2.4, a Licensed Product may not make, or cause to be made, a digital copy of Decrypted DT Data received via Remote Access except (i) as a Transitory Image, or (ii) where a Sink Function receives DT Data that was transmitted by a Licensed Product that has a Source Function pursuant to Section 3.1(b) or 4.2.2(b) of Part 2 of this Exhibit B.

2.8 **Copy Count Content.** Notwithstanding the terms of Sections 2.2-2.4, and except as provided in Section 2.1, a Licensed Product may not make, or cause to be made, a copy of CC Content except in compliance with Section 2.9 using one of the methods set forth in Sections 2.8.1-2.8.3:

2.8.1 via a recording technology approved by DTLA for CC Content, now or in the future, as specified on the DTLA website or in a notice to Adopter, and the Sink Device passes to such technology the Number of Permitted CC Copies to be associated with such content passed to such technology;

2.8.2 if the copy is stored pursuant to Section 2.2.1.2, provided that the Sink Device associates such stored copy with a persistent indicator of the Number of Permitted CC Copies (such copy, a "Bound CC Recording"); or

2.8.3 if the copy is made using a copy protection technology pursuant to 2.2.1.1, provided that (a) the Number of Permitted CC Copies is not passed to the downstream technology and (b) the Number of Permitted CC Copies made by such copy protection technology shall be deemed one.

2.9 **Additional Obligations Regarding Recording and Output of Copy Count Content.** For each CC Content received by the Sink Function, the Sink Function shall keep track of the Number of Permitted CC Copies for all recordings made pursuant to Sections 2.8.1-2.8.3 (collectively, the "Downstream Recording CC Copies") as well as the Number of Permitted CC Copies for all Downstream Output CC Copies (as defined in Section 4.9.1), provided that the total Number of Permitted CC Copies for all such Downstream Recording CC Copies and for all Downstream Output CC Copies shall be no greater than the Number of Permitted CC Copies associated with such CC

Content received by the Sink Device having such Sink Function or, where the cop(y)(ies)/output(s) is/are being made from a Bound CC Recording, no greater than the Number of Permitted CC Copies associated with such Bound CC Recording immediately prior to Transfer. Further, if any such output or copy is made from a Bound CC Recording on the Sink Device, the Sink Device shall decrement the Number of Permitted CC Copies associated with such Bound CC Recording by the number of all Downstream Recording CC Copies and all Downstream Output CC Copies, provided that if the decremented count would be zero, such Bound CC Recording shall be deleted or rendered unusable on the Sink Device.

3. SINK FUNCTION OBLIGATIONS REGARDING MOVE

3.1 **Move.** In the event that a Licensed Product that has a Sink Function receives DT Data via its Sink Function that was transmitted by a Licensed Product that has a Source Function pursuant to Section 3 or 4.2 of Part 2 of this Exhibit B, such Sink Function shall ensure that such DT Data is encoded as No More Copies and, for avoidance of doubt, in the event that DT Data was transmitted pursuant to section 3.1 (a) of Part 2 of this Exhibit B, such DT Data received by such Sink Function may not be treated as Copy One Generation pursuant to Section 2.2.1.3. Any Sink Function that receives DT Data pursuant to this Section 3 shall make or enable the making of only a single copy of such DT Data.

4. SINK FUNCTION PERMITTED OUTPUTS.

4.1 **Generally.** As set forth in more detail below, a Licensed Product shall not pass Decrypted DT Data, whether in digital or analog form, to an output except as permitted below.

4.1.1 **Outputs, Video.** A Licensed Product shall not pass any representation or conversion of the video portion of Decrypted DT Data to any output except:

4.1.1.1 Where Decrypted DT Data is output via an approved standard definition analog output in a manner pursuant to Section 4.2 of this Part of this Exhibit B;

4.1.1.2 Where Decrypted DT Data is output in a High Definition Analog Form in a manner pursuant to Section 4.3 of this Part of this Exhibit B;

4.1.1.3 Where Decrypted DT Data is output via a digital output in a manner pursuant to Section 4.4 of this Part of this Exhibit B; or

4.1.1.4 Where the Decrypted DT Data is encoded Copy Freely with the EPN Field not asserted, in which case there are no restrictions on output.

4.2 **Standard Definition Analog Output.** Subject to the requirements of Section 4.7, a Licensed Product shall not pass Decrypted DT Data to an NTSC, YUV, SECAM, PAL, or consumer RGB format analog output (including an S-video output for the listed formats) unless (a) the Decrypted DT Data is other than No More Copies, Copy Never, or Copy One Generation or (b) the Licensed Product is incorporated into a Computer Product and the output is either a VGA output or a similar output that was widely implemented as of May 1, 2001 that carries uncompressed video signals with a resolution less than or equal to a Constrained Image to a computer monitor or (c) the Licensed Product generates copy control signals according to the information provided in either such Decrypted DT Data or PCP-UR and E-EMI in accordance with the DTCP2 Specification. A

Licensed Product may, as follows, pass Decrypted DT Data to an output pursuant to clause (c) if it uses the following technologies:

4.2.1 For NTSC analog outputs, however transmitted, the specifications for the Automatic Gain Control and Colorstripe copy control systems (contained in the document entitled "Specification of the Macrovision Copy Protection Process for DVD Products, Revision 7.1.D1, September 30, 1999") and the CGMS-A specifications contained in IEC 61880 (for inclusion on Line 20) or in EIA-608-B (for inclusion on Line 21), provided that, except as otherwise expressly provided in Section 4.2.5, all of such technologies must be utilized in order to meet this requirement.

4.2.2 For PAL, SECAM or YUV outputs, the appropriate specifications (i) for the Automatic Gain Control copy control system (contained in the document entitled "Specification of the Macrovision Copy Protection Process for DVD Products, Revision 7.1.D1, September 30, 1999") and (ii) for the CGMS-A copy control system (contained in IEC 61880 (for inclusion on Line 20) or in EIA-608-B (for inclusion on Line 21) or in EIA-805 (for inclusion on Line 41) for YUV (525/60 systems) outputs or in ETS 300294 for PAL, SECAM, and YUV (625/50 systems) outputs), provided that, except as otherwise expressly provided in Section 4.2.5, both of these technologies must be utilized in order to meet this requirement. (Note; "YUV as used herein means a component video output comprised of a luminance signal (Y) and two color difference signal (U and V) and specifically includes the following component video signals (Y,Pb,Pr), (Y,Cb,Cr), (Y, Db, Dr), and (Y, B-Y, R-Y).)

4.2.3 For 480p progressive scan outputs, the appropriate specification for (i) the Automatic Gain Control copy control system (contained in the document entitled "Specification of the Macrovision AGC Copy Protection Waveforms for DVD Applications with 525p (480p) Progressive Scan Outputs, Revision 1.03 (December 22, 1999)") and (ii) CGMS-A copy control system (contained in, or adapted without material change from, EIAJCPR1204-1 (defining the signal waveform carrying the CGMS-A) and IEC61880 (defining the bit assignment for CGMS-A)).

4.2.4 For SCART connectors, the Automatic Gain Control specifications for the PAL and SECAM signal carried by that connector, provided that the connector must be configured so that the component signal carried by the connector must always be accompanied by a composite signal and such composite signal must provide the only synchronization reference for the component signal.

4.2.5 A Licensed Product shall not apply Analog Protection System (APS) to Copy One Generation Decrypted DT Data, but it shall pass through, without alteration, the value of any APS trigger bits (as described in the DTCP2 Specification) in accordance with the specifications relating to APS contained in (a) IEC 61880 (for inclusion of such value on Line 20) or EIA-608-B (for inclusion of such value on Line 21) for NTSC outputs or (b) IEC 61880 (for inclusion of such value on Line 20) or EIA-608-B (for inclusion of such value on Line 21) for YUV (525/60 systems) outputs. Notwithstanding the foregoing, the requirements to comply with the CGMS-A specification and to pass any values of APS trigger bits set forth in this Section 4.2 shall not apply to a Licensed Product incorporated into a Computer Product.

4.2.6 DTLA may amend certain obligations set out in this Section 4.2, or specify alternative means to comply, if DTLA finds that the required technologies are not available on fair, reasonable and nondiscriminatory terms.

4.3 **High Definition Analog Output.** Subject to the requirements of Section 4.7, Licensed Products shall not pass Decrypted DT Data to a High Definition Analog Output, except as set forth in this Section 4.3:

4.3.1 Licensed Products may pass Decrypted DT Data to a High Definition Analog Output as a Constrained Image.

4.3.2 Licensed Products that recognize and respond to the Image Constraint Token in accordance with the DTCP2 Specification may pass Decrypted DT Data to an output in High Definition Analog Form when authorized by the setting of the Image Constraint Token.

4.3.3 Licensed Products incorporated into Computer Products may pass Copy One Generation or No More Copies Decrypted DT Data without image constraint to SVGA (1024x768 and greater), XGA (1024x768), SXGA and UXGA or similar computer video outputs that were widely implemented as of May 1, 2001 (but not to such typical consumer electronics outputs as NTSC, PAL, SECAM, SCART, YUV, S-Video and consumer RGB, whether or not such outputs are found on any Computer Product) in High Definition Analog Form for devices manufactured prior to December 31, 2010, unless otherwise notified by DTLA.

4.3.4 Licensed Products may pass Decrypted DT Data in High Definition Analog Form to a High Definition Analog Output where such Decrypted DT Data is encoded Copy Freely.

4.4 **Digital Outputs.** Subject to the requirements of Section 4.8-4.9 of this Part 1-A, Licensed Products may only pass Decrypted DT Data to a digital output as follows:

4.4.1 To DTCP1 protected outputs that use DTCP1 Specification Revision 1.7 or higher;

4.4.2 To DTCP2 protected outputs, preserving the settings of the L2-Only Token, HDR Token, EI Token, and SDO Token, provided that the SDO Token may be set to 1 (asserted);

4.4.3 To any digital output where the Decrypted DT Data is encoded Copy Freely with the EPN Field not asserted; or

4.4.4 Via other methods that may be approved by DTLA in the future.

4.5 **Audio, Analog.** There are no prohibitions relating to analog audio outputs.

4.6 **Audio, Digital.** Except as otherwise provided in Section 4.4, Licensed Products shall not output the audio portions of Decrypted DT Data in digital form except in compressed audio format (such as AC3) or in Linear PCM format in which (a) the transmitted information is sampled at no more than 48 kHz and no more than 16 bits, or (b) where the Audio Enhancement Token is set to 1 (asserted), the transmitted information is sampled at no more than 192 kHz and no more than 24 bits. Adopter is cautioned and notified that the requirements relating to audio may be revised.

4.7 **Analog Sunsets.** Notwithstanding the provisions of Sections 4.2 and 4.3, no Licensed Product may pass Decrypted DT Data marked with the Analog Sunset Token to any analog video output.

4.8 **Digital Only Token Content.** Notwithstanding the terms of Sections 4.1-4.4 and 4.7, and except as provided in Sections 4.5 and 4.6, a Licensed Product shall not pass Digital Only Token Content to any output except:

4.8.1 To DTCP1 protected outputs according to DTCP1 Specification Revision 1.7 or higher, setting DOT field to DOT-asserted;

4.8.2 To DTCP2-protected outputs, setting DOT field to DOT-asserted;

or

4.8.3 Via other methods approved by DTLA for Digital Only Token Content, now or in the future, as specified on the DTLA website or in a notice to Adopter.

4.9 **Copy Count Content.** Notwithstanding the terms of Sections 4.1-4.4 and 4.7-4.8, and except as provided in Sections 4.5 and 4.6, a Licensed Product shall not pass CC Content to any output except as provided in Sections 4.9.1 or 4.9.2:

4.9.1 A Licensed Product may pass CC Content using a method described in Section 4.9.1.1 or 4.9.1.2:

4.9.1.1 To DTCP1 protected outputs according to DTCP1 Specification Volume 1 Revision 1.7 or higher that implement the requirements pertaining to CC Content in Part 2 of this Exhibit;

4.9.1.2 To DTCP2 protected outputs; or

4.9.1.3 Via other methods approved by DTLA for CC Content, now or in the future, as specified on the DTLA website or in a notice to Adopter.

When passing CC Content pursuant to Section 4.9.1.1 or 4.9.1.2, a Sink Function also shall pass the Number of Permitted CC Copies for each output (collectively, the "Downstream Output CC Copies"), and shall comply with the requirements of Section 2.9.

4.9.2 In addition to outputs permitted under Section 4.9.1, in the case that the CC Content being output is made from a Bound CC Recording, a Licensed Product may pass such CC Content to any output permitted under Sections 4.1-4.4 if no copies can be made from such output; the content is treated as No More Copies content; and no Number of Permitted CC Copies is passed to such output.

5. INTERNET RETRANSMISSION.

5.1 **Generally.** The parties acknowledge that Licensed Products shall not permit retransmission of Decrypted DT Data to the Internet except as permitted in Section 4.4.3.

6. CONSENSUS WATERMARK NON-INTERFERENCE.

6.1 **Phase-in Period.** During the period commencing on the Effective Date and ending (i) with respect to the Consensus Watermark, eighteen (18) months after the date DTLA declares the Consensus Watermark, and (ii) with respect to all other Presently Known Watermark Technologies, on the date DTLA declares the Consensus Watermark, Adopter shall not knowingly design or knowingly develop a Licensed Product or a component thereof for the primary purpose of stripping, interfering with or obscuring such Consensus Watermark or other Presently Known Watermark Technologies in DT Data received by such Licensed Product's Sink Function or knowingly promote or knowingly advertise or knowingly cooperate in the promotion or advertising of Licensed Products or components thereof for the purpose of stripping, interfering or obscuring such watermarks in such DT Data. For purposes of this Section 6.1, a "Presently Known Watermark Technology" shall mean each of the technologies submitted by the Galaxy group of companies and by the Millennium Group to the DVD Copy Control Association, Inc. in August 1999, and the technology defined as "ARIS/SOLANA-4C," as required by the SDMI Portable Device Specification, Part 1, Version 1.0 (July 8, 1999).

6.2 **Protection of the Watermark**. Without limiting the terms of Section 6.1,

6.2.1 Commencing on the date that DTLA declares the Consensus Watermark, Adopter:

6.2.1.1 Shall, when selecting among technological implementations for product features of Licensed Products designed after such date, take commercially reasonable care (taking into consideration the reasonableness of the costs of implementation, as well as the comparability of their technical characteristics, of applicable commercial terms and conditions, and of their impact on Decrypted DT Data and on the effectiveness and visibility of the Consensus Watermark) that Licensed Products and components thereof do not strip, interfere with or obscure the Consensus Watermark in DT Data received by their Sink Functions;

6.2.1.2 Shall not design new Licensed Products or components thereof for which the primary purpose is to strip, interfere with or obscure the Consensus Watermark in DT Data received by their Sink Functions; and

6.2.1.3 Shall not knowingly promote or knowingly advertise or knowingly cooperate in the promotion or advertising of Licensed Products or components thereof for the purpose of stripping, interfering with or obscuring the Consensus Watermark in DT Data received by their Sink Functions.

6.2.2 Commencing eighteen (18) months after DTLA declares the Consensus Watermark, Adopter:

6.2.2.1 Shall not produce Licensed Products or components thereof for which the primary purpose is to strip, interfere with or obscure the Consensus Watermark in DT Data received by their Sink Functions; and

6.2.2.2 Shall not knowingly distribute or knowingly cooperate in distribution of Licensed Products or components thereof for the purpose of stripping, interfering with or obscuring the Consensus Watermark in DT Data received by their Sink Functions.

6.3 **Product Features.** This Section 6 shall not prohibit a Licensed Product or Licensed Component from incorporating legitimate features (i.e., zooming, scaling, cropping, picture-in-picture, compression, recompression, image overlays, overlap of windows in a graphical user interface, audio mixing and equalization, video mixing and keying, downsampling, upsampling, and line doubling, or conversion between widely-used formats for the transport, processing and display of audiovisual signals or data, such as between analog and digital formats and between PAL and NTSC or RGB and YUV formats, as well as other features as may be added to the foregoing list from time to time by DTLA by amendment to these Compliance Rules Audiovisual) that are not prohibited by law, and such features shall not be deemed to strip, interfere with or obscure the Consensus Watermark in DT Data, provided that (a) Adopter shall, at all times after DTLA declares the Consensus Watermark, take commercially reasonable care, in accordance with Section 6.2.1, that such features in a Licensed Product do not strip, obscure, or interfere with the Consensus Watermark in DT Data received by such Licensed Product's Sink Function, and (b) Adopter shall not knowingly market or knowingly distribute, or knowingly cooperate in marketing or distributing, such Licensed Products or Licensed Components for the purpose of stripping, obscuring or interfering with the Consensus Watermark in DT Data.

6.4 Adopter is alerted that the requirements of this Section 6, and the declaration of the Consensus Watermark, may be rescinded by DTLA if, during the two (2)-year period immediately preceding the fourth anniversary of such declaration, the Consensus Watermark has not been implemented by major Content Participants in more than thirty-three percent (33%) of DVD discs of new theatrical motion pictures produced for DVD release by such Content Participants in the United States of America and Canada during such period.

7. REQUIREMENTS WITH CERTAIN OPERATING SYSTEMS.

7.1 **TTL Exception**. The requirement in Section 4.6.2 of DTCP2 Specification that "receiving devices shall discard such received IP datagrams which have a TTL value greater than 3" shall not apply where it is not technically feasible and commercially reasonable for a Licensed Product to determine from its operating system the TTL value of a received IP datagram.

7.2 **Wireless LAN Security Exception**. Section 4.6.3 of the DTCP2 Specification shall not apply where it is not technically feasible and commercially reasonable for a Licensed Product to determine from its operating system whether Wireless LAN security is engaged.

7.3 Eighteen (18) months after it becomes technically feasible and commercially reasonable for a Licensed Product to conform to Sections 4.6.2 and/or 4.6.3 of the DTCP2 Specification, the exceptions 7.1 and/or 7.2 respectively will cease to apply to such device.

EXHIBIT B AUDIOVISUAL, PART 1-B: DTCP2 COMPLIANCE RULES FOR SINK FUNCTIONS—L2 PROTECTION

1. INTRODUCTION TO PART 1-B

1.1 **Applicability.** This Part 1-B of this Exhibit B is applicable to Licensed Products that have a Sink Function and are capable of protecting Decrypted DT Data using L2 protection in accordance with Section 1.2.2 of Part 1 General..

1.2 **Sink Function obligation regarding down conversion of Enhanced Image.**

1.2.1 If L2-Only Token is set to 1 (asserted) and HDR Token is set to 1 (asserted), Licensed Products shall not downconvert Decrypted DT Data to standard dynamic range.

1.2.2 If L2-Only Token is set to 0 (not asserted)and EI Token is set to 1 (asserted), Decrypted DT Data may be down converted to Non-Enhanced Image in which case EI Token shall be changed to 0 (not asserted) and L1 protection (Part 1-A of this Exhibit A) may be applied.

1.3 For the convenience of Adopter, Table 1 in Exhibit B Part 1-General summarizes the combination of settings in cases to which the Compliance Rules for L2 protection in this Exhibit B Part 1-B apply.

2. SINK FUNCTION OBLIGATIONS REGARDING PERSISTENT STORAGE OF CONTENT

2.1 **Copy Never.** Licensed Products shall be constructed such that Copy Never DT Data received via their Sink Functions may not, once decrypted, be stored except as a Transitory Image or as otherwise permitted in Section 2.1.1:

2.1.1 Copy Never DT Data may be retained (i.e., stored) for such period as is specified by the Retention State Field, solely for purposes of enabling the delayed display of such DT Data. Such retained DT Data shall be stored using a method set forth in Section 2.2. and shall be obliterated or otherwise rendered unusable upon expiration of such period.

2.2 **Permitted Copy One Generation Copies.** Subject to the requirements of Sections 2.5-2.7, a Licensed Product may not make, or cause to be made, a copy of Copy One Generation Decrypted DT Data unless each copy (a) is made as a Transitory Image or (b) is made using a method set out in Section 2.2.1. A Licensed Product may, alternatively, treat such Decrypted DT Data as Copy Never, provided that no retention under Section 2.1.1 of this Part 1 is permitted.

2.2.1 Subject to the requirements of Sections 2.5-2.7, and except as set forth in Sections 2.2.2 and 2.2.3, a Licensed Product may make, or cause to be made, no more than two (2) first-generation copies of Decrypted DT Data, in different formats of storage device or media, by using only the methods described in Section 2.2.1.1 and Section 2.2.1.2:

2.2.1.1 The copy is made using a copy protection technology (such as scrambling or encryption) that is approved by DTLA now or in the future for the copying of Decrypted DT Data using L2 protection, as specified on the DTLA website or in a notice to Adopter;

2.2.1.2 The copy is stored using an encryption protocol that uniquely associates such copy with a single Licensed Product so that it cannot be played on another device or that no further usable copies may be made thereof (other than copies made from an output permitted by this Agreement or as otherwise permitted under Section 2.3 of this Part 1-B or Section 3 or 4 of Part 2), provided that, where the L2-Only Token is set to 1 (asserted) and HDR Token is set to 1 (asserted) a copy may not be stored in a form that has been downconverted to standard dynamic range; or

2.2.1.3 Copy One Generation Decrypted DT Data that is copied in a personal video recorder or other bound recording medium pursuant to Section 2.2.1.2 may continue to be treated as Copy One Generation for a period of up to ninety (90) minutes from initial reception of each unit of such data (e.g., frame-by-frame, minute-by-minute, megabyte-by-megabyte, etc.), but in no event shall such unit of data exceed one minute of a Program.

2.2.2 In the event that a Licensed Product supports one (1) or more format(s) of storage devices or media in addition to those in which a copy or copies of Decrypted DT Data are made pursuant to Section 2.2.1, a Licensed Product may make, or cause to be made, one (1) additional first-generation copy of Decrypted DT Data, using any of the methods described in Sections 2.2.1.1 and 2.2.1.2, provided that (a) such DT Data is received by one separate Sink Function having a separate Device Certificate for such additional format of storage device or media and (b) such single copy is made in a format of storage device or media other than a format in which a copy has been made by a recording device supported by another Sink Function in such Licensed Product.

By way of example and not limitation, for purposes of this Section 2.2, the following constitute different formats of storage devices or media: BD-R; MPEG4 HDD recorder; MPEG2 HDD recorder; DVHS; all DVD-recordable having less than 20GB capacity (for example, DVD-RAM, DVD-RW, DVD+RW or DVD-R); SD Card; Memory Stick; Compact Flash; non-removable RAM; and non-removable flash memory.

2.2.3 Each copy made pursuant to Sections 2.2.1, 2.2.2 or 2.4 may be stored on one or more physical storage devices or media, and may include a back-up copy, so long as all such devices, media and back-up copy constitute only a single usable copy (e.g., a back-up copy may be made on HDD or other media and the copy may be stored on RAID-type devices).

2.3 **No More Copies**. A Licensed Product may not make, or cause to be made, an analog copy of Decrypted DT Data that is encoded as No More Copies. A Licensed Product may not make, or cause to be made, a digital copy of any copy of Decrypted DT Data that is encoded as No More Copies except (a) as a Transitory Image, or (b) if the Licensed Product deletes or otherwise renders unusable the original copy such that, at any point in time, only a single useable copy persists as between such

original and copy thereof, or (c) in the event that a Licensed Product that has a Sink Function receives DT Data via its Sink Function that was transmitted by a Licensed Product that has a Source Function pursuant to Section 3.1 (b) or 4.2.2 (b) of Part 2 of this Exhibit B.

2.4 **EPN Encoded Content**. Subject to the requirements of Sections 2.5-2.7, a Licensed Product may not make, or cause to be made, a digital copy of Decrypted DT Data for which the associated EPN Field is asserted except (a) as a Transitory Image or (b) if such copy is made using one or more of the methods set out in Section 2.2.1.1 and Section 2.2.1.2. Consistent with the assertion of EPN and with the preceding sentence, a Licensed Product may, subject to the requirements of Sections 2.5-2.6, make, or cause to be made, additional digital copies of Decrypted DT Data for which the associated EPN field has been asserted, provided that each such copy (a) is a Transitory Image or (b) is made using one or more of the methods set out in Section 2.2.1.1 and Section 2.2.1.2. For clarification, Section 2.2.1.2 shall not be read to limit the number of copies that may be made of EPN encoded content, so long as each copy is made using a method set out in Section 2.2.1.1 and Section 2.2.1.2.

2.5 **Analog Sunset Token Content.** Notwithstanding the terms of Section 2.2-2.4, with respect to Analog Sunset Token Content, the copy protection technologies referenced in Section 2.2.1.1 shall be deemed further restricted to only those copy protection technologies, if any, approved by DTLA for Analog Sunset Token Content, now or in the future, as specified on the DTLA website or in a notice to Adopter.

2.6 **Digital Only Token Content.** Notwithstanding the terms of Section 2.2-2.4, with respect to Digital Only Token Content, the copy protection technologies referenced in Section 2.2.1.1 shall be deemed further restricted to only those copy protection technologies, if any, approved by DTLA for Digital Only Token Content, now or in the future, as specified on the DTLA website or in a notice to Adopter.

2.7 **Remote Access Content.** Notwithstanding the terms of Sections 2.2-2.4, a Licensed Product may not make, or cause to be made, a digital copy of Decrypted DT Data received via Remote Access except (i) as a Transitory Image, or (ii) where a Sink Function receives DT Data that was transmitted by a Licensed Product that has a Source Function pursuant to Section 3.1(b) or 4.2.2(b) of Part 2 of this Exhibit B.

2.8 **Copy Count Content.** Notwithstanding the terms of Sections 2.2-2.4, and except as provided in Section 2.1, a Licensed Product may not make, or cause to be made, a copy of CC Content except in compliance with Section 2.9 using one of the methods set forth in Sections 2.8.1-2.8.3:

2.8.1 via a recording technology approved by DTLA for CC Content, now or in the future, as specified on the DTLA website or in a notice to Adopter, and the Sink Device passes to such technology the Number of Permitted CC Copies to be associated with such content passed to such technology;

2.8.2 if the copy is stored pursuant to Section 2.2.1.2, provided that the Sink Device associates such stored copy with a persistent indicator of the Number of Permitted CC Copies (such copy, a “Bound CC Recording”); or

2.8.3 if the copy is made using a copy protection technology pursuant to 2.2.1.1, provided that (a) the Number of Permitted CC Copies is not passed to the downstream technology and (b) the Number of Permitted CC Copies made by such copy protection technology shall be deemed one.

2.9 **Additional Obligations Regarding Recording and Output of Copy Count Content.** For each CC Content received by the Sink Function, the Sink Function shall keep track of the Number of Permitted CC Copies for all recordings made pursuant to Sections 2.8.1-2.8.3 (collectively, the "Downstream Recording CC Copies") as well as the Number of Permitted CC Copies for all Downstream Output CC Copies (as defined in Section 4.9.1), provided that the total Number of Permitted CC Copies for all such Downstream Recording CC Copies and for all Downstream Output CC Copies shall be no greater than the Number of Permitted CC Copies associated with such CC Content received by the Sink Device having such Sink Function or, where the cop(y)(ies)/output(s) is/are being made from a Bound CC Recording, no greater than the Number of Permitted CC Copies associated with such Bound CC Recording immediately prior to Transfer. Further, if any such output or copy is made from a Bound CC Recording on the Sink Device, the Sink Device shall decrement the Number of Permitted CC Copies associated with such Bound CC Recording by the number of all Downstream Recording CC Copies and all Downstream Output CC Copies, provided that if the decremented count would be zero, such Bound CC Recording shall be deleted or rendered unusable on the Sink Device.

3. SINK FUNCTION OBLIGATIONS REGARDING MOVE

3.1 **Move.** In the event that a Licensed Product that has a Sink Function receives DT Data via its Sink Function that was transmitted by a Licensed Product that has a Source Function pursuant to Section 3 or 4.2 of Part 2 of this Exhibit B, such Sink Function shall ensure that such DT Data is encoded as No More Copies and, for avoidance of doubt, in the event that DT Data was transmitted pursuant to section 3.1 (a) of Part 2 of this Exhibit B, such DT Data received by such Sink Function may not be treated as Copy One Generation pursuant to Section 2.2.1.3. Any Sink Function that receives DT Data pursuant to this Section 3 shall make or enable the making of only a single copy of such DT Data.

4. SINK FUNCTION PERMITTED OUTPUTS.

4.1 **Generally.** As set forth in more detail below, a Licensed Product shall not pass Decrypted DT Data, whether in digital or analog form, to an output except as permitted below.

4.1.1 **Outputs, Video.** A Licensed Product shall not pass any representation or conversion of the video portion of Decrypted DT Data to any output except:

4.1.1.1 Where Decrypted DT Data is output via a digital output in a manner pursuant to Section 2 of this Part of this Exhibit B; or

4.1.1.2 Where the Decrypted DT Data is encoded Copy Freely with the EPN Field not asserted, in which case there are no restrictions on output.

4.2 **Digital Outputs.** Subject to the requirements of Section 4.5-4.6, Licensed Products may only pass Decrypted DT Data to a digital output as follows:

4.2.1 Where the L2 Only Token is set to 1 (asserted), to DTCP2 protected outputs as follows:

4.2.1.1 Where the HDR Token is set to 1 (asserted), Decrypted DT Data shall be passed with no downconversion to standard dynamic range;

4.2.1.2 Where the HDR Token is set to 0 (not asserted), Decrypted DT Data may be passed as an Enhanced Image or with downconversion as a Non-Enhanced Image.

4.2.2 Where the L2 Only Token is set to 0 (not asserted), to DTCP2 protected outputs as follows:

4.2.2.1 Where the EI Token is set to 1 (asserted)—

(a) as an Enhanced Image, and,

(b) as a Non-Enhanced Image, the EI Token shall be set to 0 (not asserted) and the SDO Token may be set to 1 (asserted);

4.2.2.2 Where the EI Token is set to 0 (not asserted), the SDO Token may be set to 1 (asserted);

4.2.3 Where the SDO Token is set to 1 (asserted), to outputs permitted in Sections 4.4 to 4.6 of Part 1-A of Exhibit B and in Sections 4.2 to 4.4 of Part 1-B of Exhibit B;

4.2.4 To any digital output where the Decrypted DT Data is encoded Copy Freely with the EPN Field not asserted; or

4.2.5 Via other methods that may be approved by DTLA in the future.

4.3 **Audio, Analog.** There are no prohibitions relating to analog audio outputs.

4.4 **Audio, Digital.** Except as otherwise provided in Section 4.2, Licensed Products shall not output the audio portions of Decrypted DT Data in digital form except in compressed audio format (such as AC3) or in Linear PCM format in which (a) the transmitted information is sampled at no more than 48 kHz and no more than 16 bits; or, (b) where the Audio Enhancement Token is set to 1 (asserted), the transmitted information is sampled at no more than 192 kHz and no more than 24 bits.

Adopter is cautioned and notified that the requirements relating to audio may be revised.

4.5 **Digital Only Token Content.** Notwithstanding the terms of Sections 4.1-4.2, and except as provided in Sections 4.3 and 4.4, a Licensed Product shall not pass Digital Only Token Content to any output except:

4.5.1 To DTCP2 -protected outputs in accordance with Section 4.2.1 of this Part 1-B of Exhibit B, setting DOT field to DOT-asserted; or

4.5.2 Via other methods approved by DTLA for Digital Only Token Content, now or in the future, as specified on the DTLA website or in a notice to Adopter.

4.6 **Copy Count Content.** Notwithstanding the terms of Sections 4.1-4.2 and 4.5, and except as provided in Sections 4.3 and 4.4, a Licensed Product shall not pass CC Content to any output except as provided in Sections 4.6.1 or 4.6.2:

4.6.1 A Licensed Product may pass CC Content using a method described in Section 4.6.1.1 or 4.6.1.2:

4.6.1.1 To DTCP2-protected outputs in accordance with Section 4.2.1 of this Part 1-B of Exhibit B; or,

4.6.1.2 Via other methods approved by DTLA for CC Content, now or in the future, as specified on the DTLA website or in a notice to Adopter.

When passing CC Content pursuant to Section 4.6.1.1 or 4.6.1.2, a Sink Function also shall pass the Number of Permitted CC Copies for each output (collectively, the "Downstream Output CC Copies"), and shall comply with the requirements of Section 2.9.

4.7.2 In addition to outputs permitted under Section 4.6.1, in the case that the CC Content being output is made from a Bound CC Recording, a Licensed Product may pass such CC Content to any output permitted under Sections 4.1-4.2 if no copies can be made from such output; the content is treated as No More Copies content; and no Number of Permitted CC Copies is passed to such output.

5. INTERNET RETRANSMISSION.

5.1 **Generally.** The parties acknowledge that Licensed Products shall not permit retransmission of Decrypted DT Data to the Internet except as permitted in Section 4.2.4

6. CONSENSUS WATERMARK NON-INTERFERENCE.

6.1 **Phase-in Period.** During the period commencing on the Effective Date and ending (i) with respect to the Consensus Watermark, eighteen (18) months after the date DTLA declares the Consensus Watermark, and (ii) with respect to all other Presently Known Watermark Technologies, on the date DTLA declares the Consensus Watermark, Adopter shall not knowingly design or knowingly develop a Licensed Product or a component thereof for the primary purpose of stripping, interfering with or obscuring such Consensus Watermark or other Presently Known Watermark Technologies in DT Data received by such Licensed Product's Sink Function or knowingly promote or knowingly advertise or knowingly cooperate in the promotion or advertising of Licensed Products or components thereof for the purpose of stripping, interfering or obscuring such watermarks in such DT Data. For purposes of this Section 6.1, a "Presently Known Watermark Technology" shall mean each of the technologies submitted by the Galaxy group of companies and by the Millennium Group to the DVD Copy Control Association, Inc. in August 1999, and the technology defined as "ARIS/SOLANA-4C," as required by the SDMI Portable Device Specification, Part 1, Version 1.0 (July 8, 1999).

6.2 **Protection of the Watermark**. Without limiting the terms of Section 6.1,

6.2.1 Commencing on the date that DTLA declares the Consensus Watermark, Adopter:

6.2.1.1 Shall, when selecting among technological implementations for product features of Licensed Products designed after such date, take commercially reasonable care (taking into consideration the reasonableness of the costs of implementation, as well as the comparability of their technical characteristics, of applicable commercial terms and conditions, and of their impact on Decrypted DT Data and on the effectiveness and visibility of the Consensus Watermark) that Licensed Products and components thereof do not strip, interfere with or obscure the Consensus Watermark in DT Data received by their Sink Functions;

6.2.1.2 Shall not design new Licensed Products or components thereof for which the primary purpose is to strip, interfere with or obscure the Consensus Watermark in DT Data received by their Sink Functions; and

6.2.1.3 Shall not knowingly promote or knowingly advertise or knowingly cooperate in the promotion or advertising of Licensed Products or components thereof for the purpose of stripping, interfering with or obscuring the Consensus Watermark in DT Data received by their Sink Functions.

6.2.2 Commencing eighteen (18) months after DTLA declares the Consensus Watermark, Adopter:

6.2.2.1 Shall not produce Licensed Products or components thereof for which the primary purpose is to strip, interfere with or obscure the Consensus Watermark in DT Data received by their Sink Functions; and

6.2.2.2 Shall not knowingly distribute or knowingly cooperate in distribution of Licensed Products or components thereof for the purpose of stripping, interfering with or obscuring the Consensus Watermark in DT Data received by their Sink Functions.

6.3 **Product Features.** This Section 6 shall not prohibit a Licensed Product or Licensed Component from incorporating legitimate features (i.e., zooming, scaling, cropping, picture-in-picture, compression, recompression, image overlays, overlap of windows in a graphical user interface, audio mixing and equalization, video mixing and keying, downsampling, upsampling, and line doubling, or conversion between widely-used formats for the transport, processing and display of audiovisual signals or data, such as between analog and digital formats and between PAL and NTSC or RGB and YUV formats, as well as other features as may be added to the foregoing list from time to time by DTLA by amendment to these Compliance Rules Audiovisual) that are not prohibited by law, and such features shall not be deemed to strip, interfere with or obscure the Consensus Watermark in DT Data, provided that (a) Adopter shall, at all times after DTLA declares the Consensus Watermark, take commercially reasonable care, in accordance with Section 6.2.1, that such features in a Licensed Product do not strip, obscure, or interfere with the Consensus Watermark in DT Data received by such Licensed Product's Sink Function, and (b) Adopter shall not knowingly market or knowingly distribute, or knowingly cooperate in marketing or distributing, such Licensed Products or Licensed Components for the purpose of stripping, obscuring or interfering with the Consensus Watermark in DT Data.

6.4 Adopter is alerted that the requirements of this Section 6, and the declaration of the Consensus Watermark, may be rescinded by DTLA if, during the two (2)-year period immediately preceding the fourth anniversary of such declaration, the Consensus Watermark has not been

implemented by major Content Participants in more than thirty-three percent (33%) of DVD discs of new theatrical motion pictures produced for DVD release by such Content Participants in the United States of America and Canada during such period.

7. REQUIREMENTS WITH CERTAIN OPERATING SYSTEMS.

7.1 **TTL Exception**. The requirement in Section 4.6.2 of the DTCP2 Specification that "receiving devices shall discard such received IP datagrams which have a TTL value greater than 3" shall not apply where it is not technically feasible and commercially reasonable for a Licensed Product to determine from its operating system the TTL value of a received IP datagram.

7.2 **Wireless LAN Security Exception**. Section 4.6.3 of the DTCP2 Specification shall not apply where it is not technically feasible and commercially reasonable for a Licensed Product to determine from its operating system whether Wireless LAN security is engaged.

7.3 Eighteen (18) months after it becomes technically feasible and commercially reasonable for a Licensed Product to conform to Sections 4.6.2 and/or 4.6.3 of the DTCP2 Specification, the exceptions 7.1 and/or 7.2 respectively will cease to apply to such device.

EXHIBIT B AUDIOVISUAL, PART 2: DTCP2 COMPLIANCE RULES FOR SOURCE FUNCTIONS

1. SOURCE FUNCTION OBLIGATIONS

1.1 **Applicability.** This Part 2 of this Exhibit B is applicable to Licensed Products that have a Source Function with L1 protection or L2 protection. A Source Function shall not have both L1 protection and L2 protection.

For the convenience of Adopter, Table 1 in Exhibit B, Part 1-General summarizes the combination of settings in cases to which L1 protection or L2 protection is permitted.

2. VIDEO CONTENT

2.1 **Encoding Rules.** Adopter acknowledges that Content Participants may only encode Commercial Audiovisual Content using DTCP2 to prevent or limit copying as set out Sections 2.1.1 and 2.1.2.

2.1.1 **Copy Never.** Commercial Audiovisual Content delivered as follows may be encoded and transmitted as Copy Never Content:

2.1.1.1 Prerecorded Media,

2.1.1.2 Pay-Per-View,

2.1.1.3 Subscription-On-Demand,

2.1.1.4 Video-on-Demand,

2.1.1.5 New business models that are comparable to 2.1.1.1 - 2.1.1.4.

For the avoidance of doubt, content delivered over a Protected Free-to-Air System may not be encoded and transmitted as Copy Never.

2.1.2 **Copy One Generation.**

2.1.2.1 Commercial Audiovisual Content delivered as follows may be encoded and transmitted on such system as Copy One Generation Content:

2.1.2.1.1 Prerecorded Media,

2.1.2.1.2 Pay-Per-View,

2.1.2.1.3 Subscription-On-Demand,

2.1.2.1.4 Video-on-Demand,

2.1.2.1.5 Pay Television Transmission,

2.1.2.1.6 Non-Premium Subscription Television,

2.1.2.1.7 Free Conditional Access Delivery,

2.1.2.1.8 New business models that are comparable to 2.1.2.1.1 – 2.1.2.1.7.

2.1.2.2 Content delivered over a Protected Free-to-Air System may be encoded and transmitted as Copy One Generation Content as follows:

a. content that previously has been available only in theatrical release and/or on Prerecorded Media in any country of the world, and has not previously been licensed for television broadcast in any country of the world; or,

b. content that --

i. was transmitted in North America, Japan, any Western European country, Australia, or in any country constituting a major market for such audiovisual programming (each a "Major Market"), by or under license from a person or entity authorized to license such transmission, and each such transmission has been made over Video on Demand, Pay-Per-View, Subscription-on-Demand, or Undefined Business Models that are comparable to the foregoing, or Pay Television Transmissions, and

ii. either—

A. has not been lawfully transmitted in any Major Market in greater than Standard Definition format without using one or more digital copy protection methods (*i.e.*, methods that impose numerical copy restrictions), including by way of example DTCP encoding and display-only methods, or,

B. is a version created specifically for the market covered by a Protected Free-to-Air System, other than by minor editing processes typically performed for English-speaking foreign-produced programs re-broadcast in such market, of a program that was broadcast or is scheduled to be broadcast in another country; or,

c. content that is co-produced by Content Participant and one or more other entities and is scheduled to be transmitted in a Major Market by or under license from one or more of the other co-production partners using a method of delivery set out in b(i) above and satisfies the condition set out in b(ii)(A), or,

d. content that was permitted to be transmitted, and was transmitted, using DTCP Copy One Generation encoding in accordance with this Section 2.1.2.2.

2.1.3 **No More Copies.** Licensed Products shall only encode as "No More Copies" content received as Copy One Generation and stored via a method set out in, or approved pursuant to, Exhibit B, Part 1, Section 2.2.

2.1.4 **Encryption Plus Non-assertion Encoding.** Content that is broadcast over the Protected Free-to-Air System may be encoded and transmitted as EPN, except that EPN encoding may not be applied to content that is broadcast (a) over another service, in the same market as the Protected Free-to-Air System, in High Definition, (b) at or about the same date as

the broadcast over the Protected Free-to-Air System, (c) without using one or more digital protection methods (*i.e.*, methods that impose numerical copy restrictions, restrictions upon retransmission, or both), including by way of example DTCP1 or DTCP2 EPN encoding. Adopter acknowledges that EPN Encoding may not be asserted by Content Participants with respect to Other EPN Eligible Broadcast Television, except by such eligible Content Participants that are identified by DTLA. "EPN Encoding" means such encoding used by or at the direction of a Content Participant so as to cause a service or Program to be encrypted with DTCP1 or DTCP2 but not to be subject to copy control restrictions.

2.1.5 **DOT and AST.** Adopter acknowledges that Content Participant may not encode, or direct to be encoded, using the Digital Only Token or the Analog Sunset Token, Commercial Audiovisual Content except--

(a) in the case of Video-on-Demand in a particular country, any Program until the earlier of (x) 120 days from the first application of DOT by any Video-on-Demand service for such Program or (y) the retail release in such country of such Program in any pre-recorded format except if such pre-recorded format both (i) is designed to prevent all products from outputting such Program in analog format (whether output from a product then- manufactured or distributed or from any legacy product) and (ii) includes an indicator requiring the Source Device to set the DOT to asserted for such Program, if such Program can be output via DTCP1,

(b) to the same extent in any country of the world as is allowed in the United States by the FCC Waiver Order, or,

(c) any Program on Prerecorded Media, or delivered via an Undefined Business Model that is Comparable to Prerecorded Media unless such model is also a Defined Business Model other than Prerecorded Media or an Undefined Business Model that is Comparable thereto.

2.2 **Image Constraint and Downconversion.**

2.2.1 Adopter acknowledges that Content Participants are not permitted to encode, or direct to be encoded, Commercial Audiovisual Content so as to require Decrypted DT Data to be output as a Constrained Image except with respect to Prerecorded Media, Pay Television Transmission, Video-on-Demand, Subscription-on-Demand, Pay-Per-View, a new business model comparable to any of the foregoing or any other Conditional Access Delivery of a Program that (i) had a theatrical release or was released direct-to-video and (ii) is transmitted or delivered uninterrupted by Commercial Advertising Messages. Licensed Products that have a Source Function (a "Source Device") shall set, in accordance with the DTCP2 Specification, the Image Constraint Token associated with a Program so as to permit any Licensed Product with a Sink Function to output such Program in High Definition Analog Form if such Source Device outputs such Program in unprotected High Definition Analog Form other than as permitted in Section 4.3.3 of Part 1 of Exhibit B. In addition, a Source Device shall set, in accordance with the DTCP2 Specification, the Image Constraint Token associated with a Program so as to permit any Licensed Product with a Sink Function to output such Program in High Definition Analog

Form if such Program was not specifically encoded to output such Program as a Constrained Image when received by the Source Device.

2.2.2 If L2-Only Token and HDR Token both are set to 1 (asserted), downconversion to standard dynamic range is not permitted. For clarification, only Source Functions with L2 protection are permitted to handle this type of content. (If Source Functions with L1 protection receive this type of content, such content shall not be transmitted to any Sink Functions.)

2.2.3 If L2-Only Token is set to 0 (not asserted) and EI Token is set to 1 (asserted), downconversion to Non-Enhanced Image is permitted, in which case Source Device shall set EI Token to 0 (not asserted) and may set SDO Token to 1 (asserted). For clarification, Source Functions with L1 protection shall downconvert this type of content before transmission to any Sink Function.

2.3 **Retention of Copy Never Content**. Except for Prerecorded Media, a Source Device shall set, in accordance with the DTCP2 Specification, the Retention State Field associated with any Commercial Audiovisual Content that is encoded as Copy Never for a period equal to the greatest of (a) ninety (90) minutes from initial receipt of each unit of such data (e.g., frame-by-frame, minute-by-minute, megabyte-by-megabyte, etc.); (b) such other period of time specified in the DTCP2 Specification as a content owner may affirmatively permit; or (c) if the amount of time that such content may be retained in such Source Device is determined pursuant to rules, standards or obligations that were developed under an open-standards process, such period of time specified in the DTCP2 Specification that is closest to, but not exceeding, the period of time that such Source Device is permitted to retain such content. In the case of Prerecorded Media, or if the Commercial Audiovisual Content has previously been retained, the Source Device shall encode the Commercial Audiovisual Content such that no further retention shall be permitted.

2.4. **Analog Sunset.** A Source Device shall set, in accordance with the DTCP2 Specification, the Analog Sunset Token on Analog Sunset Content. A Source Device may not set the Analog Sunset Token on any content other than Analog Sunset Content.

2.5. **Setting of Tokens Based on Upstream Encoding.** A Source Function shall not set the following tokens to asserted except where the encoding upstream from the Source Function directs the Source Function to assert such tokens in the Source Function:

2.5.1 Audio Enhancement Token
2.5.2 Digital Only Token
2.5.3 EI Token
2.5.4 HDR Token
2.5.5 L2-Only Token
2.5.6 SDO Token.

For the avoidance of doubt, the Source Device need not set such token to asserted where such DT Data has not been encoded in accordance with the requirements of the Encoding Rules. Notwithstanding Section 2.5.6, the SDO Token may be set by a Source Device in accordance with the provisions of Section 2.2.3 of this Exhibit B Part 2 or when L2-Only Token and EI Token are both set to 0 (not asserted). Source Device may treat the SDO Token as set to 1 (asserted) where usage rules associated with the content as received by the Source Function permit the content to be passed, without downconversion, to an output technology whose robustness requirements are no more stringent than for L1 protection. Source Device may treat the L2-Only Token as set to 0 (not asserted) where usage rules associated with an Enhanced Image as received by the Source Function permit the content to be passed, after downconversion to Non-Enhanced Image, to an output or recording protection technology whose robustness requirements are no more stringent than for L1 protection. Source Device may treat the HDR Token as set to 0 (not asserted) if it ascertains that no SDR version of the same content is concurrently available.

2.6 **Remote Access.** A Licensed Product having a Source Function shall not permit the transmission of DT Data to another Licensed Product using Remote Access except as follows:

2.6.1 A Source Function may concurrently transmit DT Data via Remote Access to no more than one (1) Sink Function. Notwithstanding the foregoing, if the Source Function is provided with an affirmative indication (e.g. such as in a flag or descriptor associated with such DT Data) that Remote Access is permitted to more multiple Sink Functions, it shall be allowed according to such indication.

2.6.2 A Source Function may not permit the transmission via Remote Access of DT Data simultaneous with its reception from a Sink Function.

2.6.3 A Source Function may permit via Remote Access the transmission of stored content to a Sink Function where such content has been encoded as EPN or No More Copies; provided that the recording of such stored content shall have been completed prior to such transmission, except for any Source Devices made pursuant to government or quasi-government regulation in effect on April 1, 2011 where such regulation does not permit Remote Access for DTCP; or,

2.6.4 A Source Function otherwise may permit via Remote Access the transmission of content it has not stored (except as a Transitory Image) to a Sink Function only where such Source Function is provided with an affirmative indication (e.g., such as in a flag or descriptor associated with such DT Data) that Remote Access transmission is permitted, and in such case the Source Function shall transmit such content encoded as No More Copies.

2.7. **Requirements with Certain Operating Systems.**

2.7.1 **TTL Exception**. The requirement in Section 4.6.2 of the DTCP2 Specification that "receiving devices shall discard such received IP datagrams which have a TTL value greater than 3" shall not apply where it is not technically feasible and commercially reasonable for a Licensed Product to determine from its operating system the TTL value of a received IP datagram.

2.7.2 **Wireless LAN Security Exception**. Section 4.6.3 of the DTCP2 Specification shall not apply where it is not technically feasible and commercially reasonable for a Licensed Product to determine from its operating system whether Wireless LAN security is engaged.

2.7.3 Eighteen (18) months after it becomes technically feasible and commercially reasonable for a Licensed Product to conform to Sections 4.6.2 and/or 4.6.3 of the DTCP2 Specification, the exceptions 2.7.1 and/or 2.7.2 respectively will cease to apply to such device.

3. SOURCE FUNCTION OBLIGATIONS REGARDING MOVE.

3.1 If Copy One Generation content recorded on a personal video recorder or other bound recording medium ("PVR") has been encoded as No More Copies, such content may remain encoded as No More Copies; and transmitted to a single Sink Function in a single Licensed Product (regardless of whether such Licensed Product has multiple Sink Functions), provided that such content on the originating PVR is deleted or otherwise rendered unusable.

3.2 Multiple sequential Moves from a Licensed Product having a Source Function to a Licensed Product having a Sink Function, consistent with the requirements set forth in this Section 3 and Section 3 of Part 1A or Section 3 of Part 1B, are permitted.

3.3 A Source Function may permit a Move via Remote Access in accordance with the requirements set forth in Section 3 of Part 1A or Section 3 of Part 1B of Exhibit B and this Section 3 of Part 2 of Exhibit B.

3.4 When the Source Function receives Digital Only Token Content and Moves it in accordance with Section 3.1 above, it shall set the Digital Only Token to DOT asserted.

3.5 When the Source Function receives Analog Sunset Token Content and Moves it in accordance with Section 3.1 above, it shall set the Analog Sunset Token to AST asserted.

4. SOURCE FUNCTION OBLIGATIONS REGARDING COPY COUNT. When a Source Function receives CC Content, it may not transmit or Transfer such CC Content except by using one or more of the methods set forth in this Section 4:

4.1 **Transfer with a valid CC Field**. A Source Function may Transfer CC Content with a valid CC Field to a Sink Function as follows:

4.1.1 The Transfer may occur only over a unique connection between that Source Function and a specific Sink Function established using a method set forth in the DTCP2 Specification, provided that:

4.1.1.1 The Source Function may establish a series of such unique connections with multiple individual specific Sink Functions in order to Transfer copies of such CC Content to each such Sink Function.

4.1.1.2 In any Transfer of CC Content (x) where the Transfer is to a single Sink Function, the Source Function shall set the CC Field to a number that is no greater than the Number of Permitted CC Copies associated with the CC Content as received by the Source Function, or (y) where a series of unique connections are established to multiple Sink Functions for Transfer of such CC Content to each such Sink Function, the Source Function shall set the CC Fields for such Transfers so that the sum of all of the CC Fields is a number no greater than the Number of Permitted CC Copies associated with the CC Content as received by the Source Function.

4.1.1.3 If the Transfer is being made from a Bound CC Recording, when the Source Function confirms that the transmission is complete, the Source Function shall ensure that the Licensed Product decrements the Number of Permitted CC Copies associated with the Bound CC Recording by the number of CC Copies that have been Transferred and shall otherwise comply with the requirements of Section 2.9 of Part 1 of this Exhibit B.

4.2 **Transfer without valid CC Field (i.e. CC Field is 0000, or CC Field is not present).** A Source Function may Transfer a single copy of CC Content to a single Sink Function (regardless of whether such Licensed Product has multiple Sink Functions), either without a CC Field or with a CC Field set to invalid as follows:

4.2.1 where the copy is made from a Bound CC Recording, by following the requirements of Section 3.1 (Move), except that the requirement in Section 3.1 to delete or render unusable the bound recording shall not apply and instead (a) the terms of Section 2.9 of Part 1 of this Exhibit B shall apply and (b) for purposes of such Section 2.9, the Number of Permitted CC Copies for CC Content Transferred pursuant to this Section 4.2 shall be deemed one;

4.2.2 where the copy is not made from a Bound CC Recording, by transmitting the content using the Move protocols in the DTCP2 Specification.

4.3 **Transmit without CC Field.** Notwithstanding Sections 4.1-4.2, above, a Source Function may transmit CC Content other than by Move or Transfer, to one or more Sink Functions, provided that if the transmission is of Bound CC Recording content, it shall be treated by the Source Function as No More Copies.

4.4 **Proper Encoding**. Where CC Content is encoded, or should be encoded pursuant to the Encoding Rules, as EPN, the Source Function may transmit such content via DTCP2 without regard to the associated Number of Permitted CC Copies (i.e., it may treat such content as if it were not CC Content). Where the Source Function transmits such content using a DTCP2 output that includes a CC Field, the CC Field shall be set as invalid (i.e., setting the CC Field bits to 0000).

5. AUDIO, SUBSCRIPTION AND ON-DEMAND SERVICES.

5.1 A Licensed Product may send Commercial Entertainment Content comprising "on-demand" or "pay-per-listen" or subscription audio content that is not part of an audio-visual work to a DTCP2 input using Full Authentication with Copy Never encoding or with Restricted Authentication. Adopter is advised to consult with the providers of such audio services to determine their requirements for such activities.

EXHIBIT "C"
ROBUSTNESS RULES – GENERAL

1. INTRODUCTION

1.1. Applicability. This Exhibit C "Robustness Rules" is divided into separate Parts, which may be applicable, depending on the nature of the Licensed Product (Parts 1 and 2, respectively). A Licensed Product may have both L1 protection and L2 protection. In such a case, the requirements applicable to L1 protection and L2 protection shall apply to the respective portions of such Licensed Product.

1.2. Secrecy and Integrity. Licensed Products as shipped shall meet the applicable Compliance Rules set forth in Exhibit B, and shall be manufactured in a manner clearly designed to effectively frustrate attempts to (a) modify such Licensed Products to defeat the content protection requirements of DTCP2 set forth in the DTCP2 Specification and Compliance Rules, (b) discover or reveal values identified on Table 1 below as "Secrecy Required," and (c) cause such products to use values identified on Table 1 below as "Integrity Required" after unauthorized modification of such values occurs.

Table 1: DTCP2 Secrecy and Integrity Required Values

Abbreviation	Description	Protection
X^{-1}	Device Private Key	Secrecy Required
u	random value for each signature computation	Secrecy Required
X_K	random value for each EC-DH computation	Secrecy Required
K_{AUTH}	Key derived from EC-DH used as transport key	Secrecy Required
K_M	Multicast Exchange Key	Secrecy Required
K_{XM}	Move Exchange Key	Secrecy Required
K_S	Session Exchange Key	Secrecy Required
K_R	Remote Exchange Key	Secrecy Required
K_C	Content Key	Secrecy Required
RNG seed	Seed for Pseudo Random Number Generation	Secrecy Required
C^1	DTLA Root CA Public Key	Integrity Required
L^1	DTCP2 Device CA Public Key	Integrity Required
X^1	Device Public Key	Integrity Required
X_{SRMV}	Version Number of SRM	Integrity Required
X_{SRMC}	Number of Stored SRM parts	Integrity Required
ID_U	Unique ID of Common Key Device	Integrity Required
IID	Implementation ID	Integrity Required
N_C	Nonce for Content Channel in a Source Function	Integrity Required
ID_{SM}	Context data for Multicast Content Channel in a Source Function	Integrity Required
ID_{SU}	Context data for Unicast Content Channel in a Sink Function	Integrity Required
CMI	Content Management Information	Integrity Required
SRM	System Renewability Message	Integrity Required

Values listed as "Secrecy Required" on Table 1 are Highly Confidential Information.

In addition to those "Secrecy Required" Values, intermediate data items that are derived from such Secrecy Required Values shall also be treated as Secrecy Required. Examples include but are not limited to K_i and V_i of the pseudo random number generator defined in the DTCP2 Specification.

1.3. Rules for Application of L1 Protection and L2 Protection. DTCP2 Compliance Rules Exhibit B Audiovisual define the interaction of three (3) new tokens – the EI Token, HDR Token, and L2-Only Token – that prescribe the scope of permitted use of L1 protection or L2 protection.

1.3.1. Part 1 of this Exhibit C is applicable to Licensed Products for audiovisual works for which L1 protection is permitted.
1.3.2. Part 2 of this Exhibit C is applicable to Licensed Products for audiovisual works for which L2 protection is required or permitted.

For the convenience of Adopter, Table 2 below shows when Robustness Rules must be applied, based on the combination of settings for these tokens, for L1 protection and L2 protection.

Table 2: Robustness Rules for L1 and L2 protection

Applicable Robustness Rules			
L2-Only Token	**HDR Token**	**EI Token**	
1 (Asserted)	1 (Asserted)	*Don't care*	• L2 protection required • *L1 protection not permitted*
1 (Asserted)	0 (Not Asserted)	*Don't care*	• L2 protection required • *L1 protection not permitted*
0 (Not Asserted)	*Don't care*	1 (Asserted)	• L2 protection required for Enhanced Image • Both L1 protection and L2 protection permitted for Non-Enhanced Image after downconversion
0 (Not Asserted)	*Don't care*	0 (Not Asserted)	• Both L1 protection and L2 protection permitted

1.4 <u>Robustness Verification List</u>. Before distributing any Licensed Product, Adopter must perform tests and analyses (as prescribed herein) to assure compliance with these Robustness Rules. A Robustness Verification List for Implementations is attached as Exhibit C-1 for Implementations of

L1 protection, and as Exhibit C-2 for Implementations of L2 protection. The purpose of the Robustness Verification List is to enumerate tests that must be performed by Adopter, covering the important aspects of these Robustness Rules, thereby to assist Adopter in ensuring that its products achieve the prescribed levels of robustness and effectively frustrate known and anticipated attacks. Adopter shall reflect the results of the tests and analyses referenced above in a completed Robustness Verification List for each of its Implementations. Inasmuch as the Robustness Verification Lists may not address all elements required for the manufacture of a Compliant product, Adopter is strongly advised to review carefully the DTCP2 Specification and Compliance Rules (including, for avoidance of doubt, these Robustness Rules) so as to evaluate thoroughly both its testing procedures and the compliance of its Implementations in Licensed Products. Adopter further is referred to the additional obligations relating to the Robustness Verification List required under Section 4 of the Procedural Appendix.

2. DEFINITIONS.

Harmonization. Where a capitalized term is used but not otherwise defined in this Exhibit C, the meaning ascribed thereto elsewhere in the Agreement, including but not limited to Exhibit B, shall apply.

2.1 "**Circumvention Device**" shall mean a device or technology, whether hardware or software, that is designed and made available for the specific purpose of bypassing or circumventing the protection technologies required by DTLA in connection with the implementation of DTCP2, provided that (i) no Licensed Product is excused from full compliance with any Robustness Rule and/or Compliance Rule due to the existence of one or more relevant Circumvention Devices, and (ii) the broad distribution and widespread use by consumers of a particular Circumvention Device should be examined by Adopter and will be examined by DTLA to determine whether the particular situation related to a particular Circumvention Device constitutes a "New Circumstance" as that term is defined and used in Section 3.7 "Advance of Technology" of Part 1 and Part 2 of the Robustness Rules.

2.2 "**Decrypted DT Data**" shall have the meaning set forth in Exhibit B Audiovisual: Compliance Rules for DTCP2 Introduction, but for the purpose of this Exhibit C, shall also include audiovisual content being processed (e.g., down converted) before applying DTCP2 encryption in a Source Function of a Licensed Product.

EXHIBIT "C" PART 1
ROBUSTNESS RULES FOR L1 PROTECTION

The Robustness Rules set forth in this Exhibit C Part 1 apply to Licensed Products manufactured in compliance with the DTCP2 Specification when receiving or transmitting Commercial Entertainment Content using L1 protection.

For the convenience of Adopter, Table 2 in Exhibit C-General summarizes the combination of settings in cases in which the Robustness Rules for L1 protection in this Exhibit C Part 1 may be applied.

NOTE: For clarification, for all cases in which L1 protection is permitted, the Robustness Rules for L2 protection in Part 2 also may be applied.

1. CONSTRUCTION

1.1. **Secrecy and Integrity.** Licensed Products using L1 protection shall protect Secrecy Required Values and Integrity Required Values in accordance with the requirements of Exhibit C – General Section 1.2.

1.2. **Defeating Functions.** Licensed Products shall not include:

(a) switches, buttons, jumpers or software equivalents thereof**,**
(b) specific traces that can be cut, or
(c) functions (including service menus and remote-control functions),

in each case by which the mandatory provisions of the DTCP2 Specification or the Compliance Rules, including the content protection technologies, analog protection systems, output protections, output restrictions, recording protections or recording limitations can be defeated, or by which compressed Decrypted DT Data in such Licensed Products can be exposed to output, interception, retransmission or copying, in each case other than as permitted under this Agreement.

2. DATA PATHS

Decrypted DT Data shall not be available on outputs other than those specified in the Compliance Rules. Within a Licensed Product that includes Sink Functions, Decrypted Type 2 Audio DT Data, Decrypted Type 3 Audio DT Data, and the video portion of Decrypted DT Data, shall not be present on any user-accessible buses in analog or unencrypted, compressed form.

2.1 A "User Accessible Bus" means (a) an internal analog connector that: (i) is designed and incorporated for the purpose of permitting end user upgrades or access or (ii) otherwise readily facilitates end user access or (b) a data bus that is designed for end user upgrades or access, such as an implementation of a smartcard, PCMCIA, Cardbus, or PCI that has standard sockets or otherwise

readily facilitates end user access. A "User Accessible Bus" does not include memory buses, CPU buses, or similar portions of a device's internal architecture that do not permit access to content in a form useable by end users.

Clause 2.1(a) should be interpreted and applied so as to allow Adopter to design and manufacture its products to incorporate means, such as test points, used by Adopter or professionals to analyze or repair products; but not to provide a pretext for inducing consumers to obtain ready and unobstructed access to internal analog connectors. Without limiting the foregoing, with respect to clause 2.1(a), an internal analog connector shall be presumed to not "readily facilitate end user access" if (i) such connector and the video signal formats or levels of signals provided to such connector, are of a type not generally compatible with the accessible connections on consumer products, (ii) such access would create a risk of product damage, or (iii) such access would result in physical evidence that such access had occurred and would void any product warranty.

2.2 Licensed Products shall be clearly designed such that when the video portion of uncompressed, Decrypted DT Data with a resolution greater than a Constrained Image is transmitted over a User Accessible Bus, such Decrypted DT Data are reasonably secure from unauthorized interception by using either Widely Available Tools or Specialized Tools, except with difficulty, other than Circumvention Devices. The level of difficulty applicable to Widely Available Tools is such that a typical consumer should not be able to use Widely Available Tools, with or without instructions, to intercept such Decrypted DT Data without risk of serious damage to the product or personal injury. Without limiting the foregoing, if Adopter at any time (the "Applicable Date") distributes a Licensed Product that uses a Common Device Key and that is capable of protecting uncompressed Decrypted DT Data over a User Accessible Bus as set forth in this Section 2.2, Adopter shall at such time and thereafter cause, to the extent technically feasible and commercially reasonable, all first activations of the DTCP2 functions of units or copies of all versions of such Licensed Product to protect uncompressed Decrypted DT Data over a User Accessible Bus as set forth in this Section 2.2. In the event that Adopter reasonably concludes that a software application contains or consists of a copy of such Licensed Product whose DTCP2 functions were activated prior to the Applicable Date on a particular device and subsequently re-installed on the same device, the activation or re-activation of the DTCP2 functions of such re-installed copy shall not be deemed to be a "first activation" for purposes of this Section 2.2 If a software application containing or consisting of a copy of such Licensed Product whose DTCP2 functions were first activated on a particular device is installed and activated via an Update on a different device, such activation of the DTCP2 functions of such copy installed on the different device shall be deemed to be a "first activation" for purposes of this Section 2.2, subject to the reasonableness standard of the preceding sentence.

3. METHODS OF MAKING FUNCTIONS ROBUST

Licensed Products shall be manufactured using at least the following techniques in a manner that is clearly designed to effectively frustrate attempts to defeat the content protection requirements set forth below.

3.1 **Distributed Functions.** In a Licensed Product having Sink Functions**,** where DT Data is delivered from one part of the Licensed Product to another, whether among integrated circuits, software modules, or otherwise or a combination thereof, the portions of the Licensed Product that perform authentication and decryption and the MPEG (or similar) decoder shall be designed and manufactured in a manner associated and otherwise integrated with each other such that Decrypted DT Data in any usable form flowing between these portions of the Licensed Product shall be reasonably secure from being intercepted or copied except as authorized by the Compliance Rules.

3.2 **Software.** Any portion of the Licensed Product that implements any of the content protection requirements of the DTCP2 Specification or Section 2.2.1.2 of Part 1-A of Exhibit B in Software shall include all of the characteristics set forth in Sections 1 and 2 of this Exhibit C Part 1. For the purposes of these Robustness Rules, "Software" shall mean the implementation of the content protection requirements as to which this Agreement requires a Licensed Product to be compliant through any computer program code consisting of instructions or data, other than such instructions or data that are included in Hardware. Such implementations also shall:

3.2.1 Protect the Secrecy Required Values in compliance with Section 1.1 of this Exhibit C Part 1 by a reasonable method including but not limited to: encryption, execution of a portion of the implementation in ring zero or supervisor mode, and/or embodiment in a secure physical implementation; and, in addition, in every case of implementation in Software, using techniques of obfuscation clearly designed to effectively disguise and hamper attempts to discover the approaches used.

3.2.2 Be designed so as to perform self-checking of the integrity of its component parts such that unauthorized modifications will be expected to result in a failure of the implementation to provide the authorized authentication and/or decryption function. For the purpose of this provision, a “modification” includes any change in, or disturbance or invasion of, features or characteristics, or interruption of processing, relevant to Sections 1 and 2 of this Exhibit C Part 1. This provision requires at a minimum the use of “signed code” or more robust means of “tagging” operating throughout the code.

3.3 **Hardware.**

Any portion of the Licensed Product that implements Primary L1 Core Functions (defined in Section 3.5 below), which shall be implemented in Hardware, and any of the content protection requirements of the DTCP2 Specification or Section 2.2.1.2 of Exhibit B Part 1-A in Hardware shall include all of the characteristics set forth in Sections 1 and 2 of this Exhibit C Part 1. For the purposes of these Robustness Rules, “Hardware” shall mean a physical device, including a component, that implements any of the content protection requirements as to which this Agreement requires that a Licensed Product be compliant and that (i) does not include instructions or data other than such instructions or

data that are permanently embedded in such device or component; or (ii) includes instructions or data that are not permanently embedded in such device or component where such instructions or data have been customized for such Licensed Product or Licensed Component and such instructions or data are not accessible to the end user through the Licensed Product or Licensed Component (i.e., a hardened execution environment). Such implementations also shall:

3.3.1 Protect the Secrecy Required Values in compliance with Section 1.1 of this Exhibit C Part 1 by any reasonable method including but not limited to embedding DTCP2 Device Keys and Highly Confidential cryptographic algorithms in silicon circuitry or firmware that cannot reasonably be read, or employing the techniques described above for Software (in each case, with a hardware root of trust).

3.3.2 Be designed such that attempts to remove, replace, or reprogram Hardware elements in a way that would compromise the content protection requirements of DTCP2 (including compliance with the Compliance Rules and DTCP2 Specification) in Licensed Products would pose a serious risk of rendering the Licensed Product unable to receive, decrypt, or decode DT Data. By way of example, a component that is soldered rather than socketed, or a hardware root of trust, may be appropriate for this means.

3.4 **Hybrid.** The interfaces between Hardware and Software portions of a Licensed Product shall be designed so that the Hardware portions comply with the level of protection that would be provided by a pure Hardware implementation, and the Software portions comply with the level of protection which would be provided by a pure Software implementation.

3.5 **Level of Protection.** "L1 Core Functions" of DTCP2 consist of "Primary L1 Core Functions" and "Other L1 Core Functions."

3.5.1 The Primary L1 Core Functions shall be implemented in Hardware, and include the following:

(a) handling in plaintext form of the DTCP2 Device Private Key, Exchange Keys (K_M, K_S, K_R and K_{XM} in Table 1 in Exhibit C-General), and parameters applicable to DTCP2 disclosed by DTLA as Highly Confidential Information (collectively, the "DTCP2 L1 Core Keys"), such as calculations of device signature and Content Key;
(b) maintaining the confidentiality and integrity of (i) DTCP2 L1 Core Keys, (ii) algorithms classified by DTLA as Highly Confidential Information, and (iii) other information or materials, including but not limited to cryptographic keys used to encrypt or decrypt the DTCP2 L1 Core Keys, from which any of the DTCP2 L1 Core Keys could reasonably be derived including the values of u, X_K and K_{AUTH} in Table 1 in Exhibit C-General;
(c) verifying the signature signed by DTLA or another device during the DTCP2 authentication protocol; and,
(d) maintaining the integrity of the usage rules defined in the DTCP2 Specification.
(e) maintaining the integrity of the values of C^1, L^1, X^1, X_{SRMV}, X_{SRMC}, ID_U, IID, N_C, ID_{SM}, ID_{SU}, CMI and SRM in Table 1 in Exhibit C-General.

3.5.2 The "Other L1 Core Functions" of DTCP2 include encryption, decryption, authentication, the functions described in Sections 2 (excluding Sections 2.2.1.1 and 2.2.1.3), 3, 4.4.1 and 4.4.2 of Part 1-A of this Exhibit B and Sections 2.3 and 3 of Exhibit B Part 2 and preventing exposure of compressed, Decrypted DT Data, which are not Primary L1 Core Functions.

3.5.3 The L1 Core Functions of DTCP2 shall be implemented in a reasonable method so that they:

3.5.3.1 Cannot be defeated or circumvented merely by using general-purpose tools or equipment that are widely available at a reasonable price, such as screwdrivers, jumpers, clips, file editors, and soldering irons ("Widely Available Tools"), or using specialized electronic tools or specialized software tools that are widely available at a reasonable price, such as EEPROM readers and writers, debuggers or decompilers, integrated development environments and similar software development products ("Specialized Tools"), or software tools such as disassemblers, loaders, patchers, or any other software tools, techniques or methods not described in Widely Available Tools and Specialized Tools (e.g., the software equivalent of in-circuit emulators, software tools used for reverse engineering and penetration testing), as would be used primarily by persons of professional skill and training ("Professional Software Tools"), other than Circumvention Devices); and

3.5.3.2 Can only with difficulty be defeated or circumvented using professional tools or equipment, such as logic analyzers, PCB rework stations, oscilloscopes, electromagnetic probes, chip disassembly systems, or in-circuit emulators or any other tools, equipment, methods, or techniques not described in Section 3.5.3.1 ("Professional Hardware Tools") such as would be used primarily by persons of professional skill and training, but not including professional tools or equipment that are made available only on the basis of a non-disclosure agreement or Circumvention Devices.

3.6 The following shall be implemented in a reasonable method that is intended to make such functions difficult to defeat or circumvent by the use of Widely Available Tools, not including Circumvention Devices or Specialized Tools as defined in Section 3.5.1:

(i) delivery of Decrypted DT Data to the functions described in Part 1-A of Exhibit B, Sections 4.2, 4.3, and 4.6; and

(ii) the method by which the DTCP2 functions in individual units or copies of certain Licensed Products or Licensed Products incorporating Robust Licensed Components are designed to cease to function as required by Section 2.2(i)(y) of the Procedural Appendix.

3.7 **Advance of Technology.** Although an implementation of a Licensed Product when designed and first shipped may meet the above standards, subsequent circumstances may arise which, had they existed at the time of design of a particular Licensed Product, would have caused such products to fail to comply with these Robustness Rules ("New Circumstances"). If an Adopter has (a) actual notice of New Circumstances, or (b) actual knowledge of New Circumstances (the occurrence of (a) or (b) hereinafter referred to as "Notice"), then within eighteen (18) months after Notice such

Adopter shall cease distribution of such Licensed Product and shall only distribute Licensed Products that are compliant with the Robustness Rules in view of the then-current circumstances.

4. EXAMINATION

4.1 **Generally.** A group of Content Participants is being or has been formed ("CPUG"). If CPUG so requests via DTLA, Adopter shall provide, once per model or version of product, any publicly available technical design documentation and, under a reasonable, mutually-acceptable non-disclosure agreement, the service manual for such product, in order to assist in the evaluation of the compliance of such product with these Robustness Rules.

4.2 **Inspection and Report.** Upon a reasonable and good faith belief that a particular hardware model or software version of a Licensed Product designed or manufactured by Adopter does not comply with the Robustness Rules then in effect for such Licensed Product, and upon reasonable notice to Adopter via DTLA, CPUG may request Adopter to submit promptly to an independent expert (acceptable to Adopter, which acceptance shall not be unreasonably withheld) for inspection such detailed information as Adopter deems necessary to understand such product's implementation of the DTCP2 Specification and Compliance Rules, such as would be sufficient to determine whether such product complies with these Robustness Rules. Adopter's participation in this inspection procedure is voluntary; no adverse inference may be drawn from Adopter's refusal of the CPUG request or refusal to participate, in whole or in part, in such inspection. The conduct of such inspection and the contents of any report made by the independent expert shall be subject to the provisions of a nondisclosure agreement, mutually-agreeable to CPUG, Adopter, and such expert, such agreement not to be unreasonably withheld, that also provide protections for Confidential Information and Highly Confidential Information relating to DTCP2 that are no less stringent than those provided for in this Agreement. Such examination and report shall be conducted at the sole expense of CPUG. Nothing in this paragraph shall limit the role or testimony of such expert, if any, in a judicial proceeding under such protective orders as a court may impose. Adopter shall not be precluded or estopped from challenging the opinion of such expert in any forum; nor shall any party be entitled to argue that any greater weight or evidentiary presumption should be accorded to the expert report than to any other relevant evidence. This provision may not be invoked more than once per hardware model or software version, provided that such right of inspection shall include the right to re-inspect the implementation of such model or version if it has been revised in an effort to cure any alleged failure of compliance.

EXHIBIT "C" PART 2:
ROBUSTNESS RULES FOR L2 PROTECTION

The following Robustness Rules apply to Licensed Products and Licensed Components manufactured in compliance with the DTCP2 Specification when receiving or transmitting Commercial Entertainment Content using L2 protection.

For the convenience of Adopter, Table 2 in Exhibit C-General summarizes the combination of settings in cases in which the Robustness Rules for L2 Protection in this Exhibit C Part 2 may be applied.

NOTE: For clarification, the Robustness Rules for L2 protection in Part 2 always may be applied to Enhanced Image and Non-Enhanced Image.

1. CONSTRUCTION

1.1 **Secrecy and Integrity.** Licensed Products using L2 protection shall protect Secrecy Required Values and Integrity Required Values in accordance with the requirements of Exhibit C – General Section 1.2.

1.2 **Defeating Functions.** Licensed Products shall not include:

(a) switches, buttons, jumpers or software equivalents thereof**,**
(b) specific traces (electrical connections) that can be cut, or
(c) special functions or modes of operation (including service menus and remote-control functions), or
(d) active JTAG ports, active emulator interfaces or active test points, to probe security functions,

in each case by which the mandatory provisions of the DTCP2 Specification or the Compliance Rules, including the content protection technologies, analog protection systems, output protections, output restrictions, recording protections or recording limitations can be defeated, or by which Decrypted DT Data in such Licensed Products can be exposed to output, interception, retransmission or copying, in each case other than as permitted under this Agreement.

2. DATA PATHS

Decrypted DT Data shall not be available on outputs other than those specified in the Compliance Rules. Within a Licensed Product that includes Sink Functions, Decrypted Type 2 Audio DT Data, Decrypted Type 3 Audio DT Data, and the video portion of Decrypted DT Data, shall not be present on any user-accessible buses in analog or unencrypted form.

2.1 A "User Accessible Bus" means, for Decrypted DT Data where L2 protection is applied, a data bus that is designed and incorporated for the purpose of permitting end user upgrades or access

such as an implementation of a smartcard, PCMCIA, Cardbus, or PCI that has standard sockets or otherwise readily facilitates end user access. A "User Accessible Bus" does not include memory buses, CPU buses, or similar portions of a device's internal architecture that do not permit access to content in a form useable by end users.

3. METHODS OF MAKING FUNCTIONS ROBUST

Licensed Products shall be manufactured using at least the following techniques in a manner that is clearly designed to effectively frustrate attempts to defeat the content protection requirements of the DTCP2 Specification and the Compliance Rules.

3.1 **Distributed Functions.** Where Decrypted DT Data is delivered from one portion of a Licensed Product to another, whether among integrated circuits, software modules, or a combination thereof, such portion shall be designed and manufactured in a manner and associated and otherwise integrated with each other such that Decrypted DT Data, in a usable form flowing between them, shall be reasonably secure from being intercepted or copied except as authorized by Compliance Rules. At least such portions shall be secure against access from non-trusted code.

3.2 **Software.** Any portion of the Licensed Product that implements any of the content protection requirements of the DTCP2 Specification in Software shall include all of the characteristics set forth in Sections 1 and 2 of this Exhibit C Part 2. For the purposes of these Robustness Rules, "Software" shall mean the implementation of the content protection requirements as to which this Agreement requires a Licensed Product to be compliant through any computer program code consisting of instructions or data, other than such instructions or data that are included in Hardware. Such implementations also shall:

3.2.1 Protect the Secrecy Required Values in compliance with Section 1.1 of this Exhibit C Part 2 by a reasonable method including but not limited to: encryption, execution of a portion of the implementation in ring zero or supervisor mode, and/or embodiment in a secure physical implementation; and, in addition, in every case of implementation in Software, using techniques of obfuscation clearly designed to effectively disguise and hamper attempts to discover the approaches used.

3.2.2 Be designed so as to perform self-checking of the integrity of its component parts such that unauthorized modifications will be expected to result in a failure of the implementation to provide the authorized authentication and/or decryption function. For the purpose of this provision, a "modification" includes any change in, or disturbance or invasion of, features or characteristics, or interruption of processing, relevant to Sections 1 and 2 of this Exhibit C Part 2. This provision requires at a minimum the use of "signed code" or more robust means of "tagging" operating throughout the code.

3.3 **Hardware.** Any portion of the Licensed Product that implements any of the content protection requirements of the DTCP2 Specification or the DTCP2 Primary Core Functions (defined in Section 3.5 of this Exhibit C Part 2) in Hardware shall include all of the characteristics set forth in Sections 1 and 2 of this Exhibit C Part 2. For the purposes of these Robustness Rules, "Hardware"

shall mean a physical device, including a component, that implements any of the content protection requirements as to which this Agreement requires that a Licensed Product be compliant and that (i) does not include instructions or data other than such instructions or data that are permanently embedded in such device or component; or (ii) includes instructions or data that are not permanently embedded in such device or component where such instructions or data have been customized for such Licensed Product or Licensed Component and such instructions or data are not accessible to the end user through the Licensed Product or Licensed Component (i.e., a hardened execution environment). Such implementations shall:

3.3.1 Protect the Secrecy Required Values in compliance with Section 1.1 of this Exhibit C – Part 2 by any reasonable method including but not limited to embedding DTCP2 Device Keys and Highly Confidential cryptographic algorithms in silicon circuitry or firmware that cannot reasonably be read, or employing the techniques described above for Software (in each case, with a hardware root of trust).

3.3.2 Be designed such that attempts to remove, replace, or reprogram Hardware elements in a way that would compromise the content protection requirements of DTCP2 (including compliance with the Compliance Rules and DTCP2 Specification) in Licensed Products would pose a serious risk of rendering the Licensed Product unable to receive, decrypt, or decode DT Data. By way of example, a component that is soldered rather than socketed, or a hardware root of trust, may be appropriate for this means.

3.4 **Hybrid.** The interfaces between Hardware and Software portions of a Licensed Product shall be designed so that the Hardware portions comply with the level of protection that would be provided by a pure Hardware implementation, and the Software portions comply with the level of protection which would be provided by a pure Software implementation.

3.5 **L2 Level of Protection for DTCP2 Core Functions. "**DTCP2 Core Functions**"** consist of the "DTCP2 Primary Core Functions" and the "Other DTCP2 Core Functions," as defined in this Section 3.5.

The following "DTCP2 Primary Core Functions" for L2 protection shall be implemented in Hardware:

(a) encryption of video portions of Commercial Audiovisual Content to which L2 protection is applied;
(b) decryption of video portions of DT Data that is Commercial Audiovisual Content to which L2 protection is applied;
(c) protecting the video portions of Decrypted DT Data to which L2 protection is applied against unauthorized exposure;
(d) handling in plaintext form of the DTCP2 Device Private Key, Exchange Keys (K_M, K_S, K_R and K_{XM} in Table 1 in Exhibit C-General), Content Key for L2 protection, and parameters applicable to DTCP2 disclosed by DTLA as Highly Confidential Information (collectively, the "DTCP2 Core Keys"), such as calculations of device signature and Content Key;
(e) maintaining the confidentiality and integrity of (i) DTCP2 Core Keys, (ii) algorithms

classified by DTLA as Highly Confidential Information, and (iii) other information or materials, including but not limited to cryptographic keys used to encrypt or decrypt the DTCP2 Core Keys, from which any of the DTCP2 Core Keys could reasonably be derived including the values of u, X_K and K_{AUTH} in Table 1 in Exhibit C-General;
(f) verifying the signature signed by DTLA or another device during the DTCP2 authentication protocol; and,
(g) maintaining the integrity of the usage rules defined in the DTCP2 Specification.
(h) maintaining the integrity of the values of C^1, L^1, X^1, X_{SRMV}, X_{SRMC}, ID_U, IID, N_C, ID_{SM}, ID_{SU},, CMI and SRM in Table 1 in Exhibit C-General.

"Other DTCP2 Core Functions" include encryption, decryption, authentication, the functions described in Sections 2 (excluding Sections 2.2.1.1 and 2.2.1.3), 3, 4.2.1, 4.2.2 of Part 1-B of Exhibit B, Section 4.4.1 of Part 1-A of Exhibit B and Section 2.3 and 3 of Part 2 of Exhibit B, which are not DTCP2 Primary Core Functions.

All DTCP2 Core Functions shall be implemented in a reasonable method so that they:

3.5.1 Cannot be defeated or circumvented merely by using general-purpose tools or equipment that are widely available at a reasonable price, such as screwdrivers, jumpers, clips, file editors, and soldering irons ("Widely Available Tools"), or using specialized electronic tools or specialized software tools that are widely available at a reasonable price, such as EEPROM readers and writers, debuggers, or decompilers, integrated development environments and similar software development products ("Specialized Tools"), or software tools such as disassemblers, loaders, patchers, or any other software tools, techniques or methods not described in Widely Available Tools and Specialized Tools (e.g., the software equivalent of in-circuit emulators, software tools used for reverse engineering and penetration testing), as would be used primarily by persons of professional skill and training ("Professional Software Tools"), other than Circumvention Devices, and

3.5.2 Can only with difficulty be defeated or circumvented using professional tools or equipment, such as logic analyzers, PCB rework stations, oscilloscopes, electromagnetic probes, chip disassembly systems, or in-circuit emulators or any other tools, equipment, methods, or techniques not described in Section 3.5.1 ("Professional Hardware Tools") such as would be used primarily by persons of professional skill and training, but not including professional tools or equipment that are made available only on the basis of a non-disclosure agreement or Circumvention Devices.

3.6 The following shall be implemented in a reasonable method that is intended to make such functions difficult to defeat or circumvent by the use of Widely Available Tools, not including Circumvention Devices or Specialized Tools as defined in Section 3.5.1:

(i) delivery of Decrypted DT Data to the functions described in Part 1-B of Exhibit B, Sections 4.4; and

(ii) the method by which the DTCP2 functions in individual units or copies of certain

Licensed Products or Licensed Products incorporating Robust Licensed Components are designed to cease to function as required by Section 2.2(i)(y) of the Procedural Appendix.

3.7 **Advance of Technology.** Although an implementation of a Licensed Product when designed and first shipped may meet the above standards, subsequent circumstances may arise which, had they existed at the time of design of a particular Licensed Product, would have caused such products to fail to comply with these Robustness Rules ("New Circumstances"). If an Adopter has (a) actual notice of New Circumstances, or (b) actual knowledge of New Circumstances (the occurrence of (a) or (b) hereinafter referred to as "Notice"), then within eighteen (18) months after Notice such Adopter shall cease distribution of such Licensed Product and shall only distribute Licensed Products that are compliant with the Robustness Rules in view of the then-current circumstances.

4. EXAMINATION

4.1 **Generally.** A group of Content Participants is being or has been formed ("CPUG"). If CPUG so requests via DTLA, Adopter shall provide, once per model or version of product, any publicly available technical design documentation and, under a reasonable, mutually-acceptable non-disclosure agreement, the service manual for such product, in order to assist in the evaluation of the compliance of such product with these Robustness Rules.

4.2 **Inspection and Report.** Upon a reasonable and good faith belief that a particular hardware model or software version of a Licensed Product designed or manufactured by Adopter does not comply with the Robustness Rules then in effect for such Licensed Product, and upon reasonable notice to Adopter via DTLA, CPUG may request Adopter to submit promptly to an independent expert (acceptable to Adopter, which acceptance shall not be unreasonably withheld) for inspection such detailed information as Adopter deems necessary to understand such product's implementation of the DTCP2 Specification and Compliance Rules, such as would be sufficient to determine whether such product complies with these Robustness Rules. Adopter's participation in this inspection procedure is voluntary; no adverse inference may be drawn from Adopter's refusal of the CPUG request or refusal to participate, in whole or in part, in such inspection. The conduct of such inspection and the contents of any report made by the independent expert shall be subject to the provisions of a nondisclosure agreement, mutually-agreeable to CPUG, Adopter, and such expert, such agreement not to be unreasonably withheld, that also provide protections for Confidential Information and Highly Confidential Information relating to DTCP2 that are no less stringent than those provided for in this Agreement. Such examination and report shall be conducted at the sole expense of CPUG. Nothing in this paragraph shall limit the role or testimony of such expert, if any, in a judicial proceeding under such protective orders as a court may impose. Adopter shall not be precluded or estopped from challenging the opinion of such expert in any forum; nor shall any party be entitled to argue that any greater weight or evidentiary presumption should be accorded to the expert report than to any other relevant evidence. This provision may not be invoked more than once per hardware model or software version, provided that such right of inspection shall include the right to re-inspect the implementation of such model or version if it has been revised in an effort to cure any alleged failure of compliance.

Exhibit C-1

DTCP2 Robustness Verification List

1. INTRODUCTION

1.1 Purpose

This list is to help to ensure construction of compliant DTCP2 Licensed Products. DTCP2 Robustness Rules describe two levels of robustness protection.

- Licensed Products built to Level 1 Robustness (L1 protection) can only be used for certain types of content as described by the Compliance Rules.
- Licensed Products built to Level 2 Robustness (L2 protection) can process all types of content.

This Exhibit C-1 does not address all aspects of the DTCP2 Specification and Compliance Rules necessary to create a product that is fully compliant. Failure to perform necessary tests and analysis could result in a failure to comply fully with the DTCP2 Specification, Compliance Rules, or Robustness Rules in breach of the DTCP2 Adopter Agreement and, as a consequence, appropriate legal action of DTLA and Eligible Content Participants.

Additional requirements pertaining to the completion and use of this DTCP2 Robustness Verification List, including related to submission to, and use by, a Third Party Robustness Authority, are set forth in Sections 3.2 and 4.3 of the DTCP2 Adopter Agreement, Section 1.4 of Exhibit C Robustness Rules – General, and in Section 4 of the Procedural Appendix.

1.2 Overview

This list is based on the DTCP2 Robustness Rules and does not prescribe specific methods for making Licensed Products Robust. To comply with the Robustness Rules, Adopters are encouraged to employ typical secure deployment lifecycle practices from design through product release, for example:

- Use of security trained designers and implementers
- Identification of applicable requirements in DTCP2
- Identification of threats and associated threat countermeasures
- Robustness Rules define the level of protection required.
- Design and Implementation
    - Includes security review of the design and peer code review of security elements of the implementation

- Verification and testing
    - Includes attempts or simulations to break or hack the Implementation to ensure that it meets each of the applicable Robustness Rules.
- Product release

The Adopter must make those design decisions, whether by contracting with third parties experienced in secure product development, or using such competency within their own company.

In general, the Robustness Verification List provides a tool for the Adopter to ensure compliance with the Robustness Rules applicable to all elements of a Licensed Product, including not limited to Hardware, firmware, and software elements, through which an unauthorized user could attempt to (a) modify such product to defeat the content protection requirements of DTCP2 set forth in the DTCP2 Specification and Compliance Rules, (b) discover or reveal values identified on Table 1 of Exhibit C - General as "Secrecy Required," and (c) cause such product to use values identified on Table 1 of Exhibit C - General as "Integrity Required" after unauthorized modification of such values occurs.

1.3 Organization

Since there are 2 levels of Robustness, Adopters need to pay close attention to the differences in:

- Data Path requirements
    - L1 protection requirements are similar to DTCP1 requirements
    - L2 protection has increased robustness requirements
- Core functions
    - L1 protection requirements are similar to DTCP1 requirements where not all core functions are in Hardware
    - L2 protection has increased robustness requirements so that all core functions are in Hardware.

The DTCP2 Robustness Rules are organized into four key areas as follows:

- **Construction** - General questions about the "construction," or design, of the Licensed Product. This includes resisting modifications that defeat the Content Protection Requirements, not including means by which those requirements can be defeated, and maintaining secrecy and integrity of keys and other items.
- **Data paths** - Questions about where Decrypted DTCP2 Data may be found and how it is protected between decryption and output.
- **Protection methods** - Questions about the methods used to meet data path and construction requirements in hardware and software.
- **Levels of Protection** - Questions about how resistant protection methods are to attack, as expressed in terms of tools and level of effort used in the attack.

1.4 Instructions for Completion and Submission

Adopter must comply with all requirements pertinent to the Robustness Verification List set forth in Section 1.4 of Exhibit C Robustness Rules – General and Section 4 of the Procedural Appendix of the DTCP2 Adopter Agreement.

In accordance with Section 1.4 of Exhibit C Robustness Rules – General, a separate Robustness Verification List must be completed by Adopter for each Implementation of DTCP2 in its Licensed Products.

- "Implementation" is defined in Section 1.26 of the DTCP2 Adopter Agreement.

In addition:

- Adopter shall complete Section 3 for an Implementation that is capable of Level 1 Robustness (L1 protection).
- Adopter shall complete Section 4 for an Implementation that is capable of Level 2 Robustness (L2 protection).
- For an Implementation that has both Level 1 and Level 2 Robustness (L1 and L2 protection), Adopter shall complete both Sections 3 and 4.

Adopter shall be able to document in detail its responses to the questions in Sections 2, 3, and 4 applicable to the Implementation. For the specific sections of this Robustness Verification List that state "Documentation is Required":

- For an Implementation that has both Level 1 and Level 2 Robustness (L1 and L2 protection), Adopter shall complete both Sections 3 and 4.
- For an Implementation that is Renewable that the Adopter does not submit for Third Party Robustness review, Adopter shall retain all such documentation for the period provided below.
- For an Implementation that is submitted for Third Party Robustness review, Adopter shall submit such documentation as Supporting Documentation (defined in Section 4.3.1.1 of the Procedural Appendix of this Agreement) to the Third Party Robustness Authority performing such review.
- For an Implementation that has a Partially Renewable portion, Adopter shall (i) retain all such documentation for such Partially Renewable portion, (ii) submit to the Third Party Robustness Authority (x) the Supporting Documentation for such portion that is not Renewable and (y) any additional documentation reasonably required by the Third Party Robustness Authority for Renewable portions as necessary to enable a full review of compliance of the non-Renewable portions as described in the Robustness Verification List.

Adopter shall maintain all such documentation (including but not limited to Supporting Documentation) used to support each response on the Robustness Verification List until three (3) years following the earlier of the cessation of manufacture or distribution by or on behalf of Adopter of products using the Implementation addressed in such Robustness Verification List, or of the termination of this Adopter's DTCP2 Adopter Agreement.

If the Implementation is not Renewable in accordance with Section 4.2 of the DTCP2 Adopter Agreement, Third Party Robustness review is mandatory. Also, if the Implementation is Partially Renewable in accordance with Section 4.2 of the DTCP2 Adopter Agreement, then Third Party Robustness review is mandatory for Implementation other than the portion which is Partially Renewable.

The Robustness Verification List shall be completed, dated, and signed in accordance with Section 4 of the Procedural Appendix. A signature page is provided at the end of the document. If additional space is needed for signatures, please provide such signatures on a separate duplicate signature page.

1.5 Definitions

1.5.1 **Harmonization**. Any term not specifically defined herein shall have the meaning ascribed thereto in the DTCP2 Adopter Agreement, the Procedural Appendix, Exhibit B-Compliance Rules, and Exhibit C-Robustness Rules.

1.6 Implementation Identifier

Adopter must give each Implementation an Identifier (e.g., a name or alphanumeric designation) and shall enter below the Identifier for the Implementation that is covered by the completed Robustness Verification List being submitted by Adopter. When making future submissions for or relating to this Implementation, Adopter shall refer to this Identifier in any such future submission.

This Robustness Verification List is being submitted by Adopter _____ for an Implementation of DTCP2 that Adopter has given the following Identifier:

_____

1.7 Applicable Robustness Rules

Check the applicable boxes below to indicate which Robustness Rules apply to this Implementation (*i.e.*, whether the Implementation is applicable to L1 protection, L2 protection, or both):

- □ Exhibit C Part 1 Robustness Rules for L1 protection
- □ Exhibit C Part 2 Robustness Rules for L2 protection

2. General

2.1 Secrecy and Integrity Values

Section 1.2 of Exhibit C Robustness Rules – General		
#		Y/N
2.2.0	Check the boxes below to indicate which Compliance Rules are applicable to the Implementation: ☐Exhibit B Part 1A (Sink Function with L1 protection) ☐Exhibit B Part 1B (Sink Function with L2 protection) ☐Exhibit B Part 2 (Source Function)	
2.2.1	Does product meet all applicable Compliance Rules set forth in Exhibit B?	
Is your product clearly designed to effectively frustrate attempts to:		
2.2.2	Modify such Licensed Products to defeat the content protection requirements of DTCP2 set forth in the DTCP2 Specification? *[Documentation is required.]*	
2.2.3	Modify such Licensed Products to defeat the content protection requirements of DTCP2 set forth in the DTCP2 Compliance Rules? *[Documentation is required.]*	
2.2.4	Discover or reveal values identified on Table 1: DTCP2 Secrecy and Integrity Required Values of Exhibit C - General as "Secrecy Required," including intermediate data items that are derived from such Secrecy Required items? *[Documentation is required.]*	
2.2.5	Cause such products to use values identified on Table 1: DTCP2 Secrecy and Integrity Required Values of Exhibit C – General as "Integrity Required" after unauthorized modification of such values occurs? *[Documentation is required.]*	

3. Exhibit "C" Part 1 RR For L1 Protection

The answer to the questions is in general either YES or NO. NA for Not Applicable may be used when the associated function is not implemented.

3.1 Construction – Defeating Functions

Construction – Defeating Functions - Section 1.2 of Exhibit C-Part 1		
Has your product been designed without the following "defeating functions" – i.e., functions that can defeat the mandatory provisions of the DTCP2 Specification or the Compliance Rules, including the content protection technologies, analog protection systems, output protections, output restrictions, recording protections, recording limitations, or that can expose compressed Decrypted DT Data to unauthorized output, interception, retransmission or copying?		
#		Y/N
3.1.1	switches, buttons, jumpers or software equivalents thereof	
3.1.2	specific traces that can be cut	
3.1.3	functions (including service menus and remote-control functions).	
3.1.4	Have you specified a process and requirement whereby all debug functions and software traces that constitute Defeating Functions in the production version will comply with these Robustness Rules requirements including, by way of example, by (a) removing such debug functions or software traces, or (b) rendering inactive such debug functions or software traces where such method of making inactive meets the Level of Protection requirement in Section 3.5 of Exhibit C-Part1? Note: Adopter shall pay special attention to serial, USB, or other interfaces to the hardware that provide external access to the kernel to execute debug functions, or other commands, relating to DTCP2. *[Documentation is required.]*	

3.2 Data Paths

Data Paths -- Section 2 of Exhibit C Part 1		
#		Y/N
3.2.0	Which of the following functions does your Implementation have in L1 protection? ☐Source Function ☐Sink Function Note: Questions 3.2.1 and 3.2.2 are applicable only to an Implementation that has Sink Functions with L1 protection.	
3.2.1	Have you identified and documented all outputs of product? *[Documentation is required.]*	
3.2.2	Have you performed and documented tests that ensure that Decrypted DT Data does not appear on outputs that are not specified in the Compliance Rules? *[Documentation is required.]* Note: Permitted outputs are identified in Section 4 of Exhibit B Part 1A.	
3.2.3	Have you identified and documented all User Accessible Buses in product? *[Documentation is required.]* Note: "User Accessible Bus" is defined in Section 2.1 of Exhibit C Part 1.	
3.2.4	Have you performed and documented tests that ensure Decrypted Type 2 Audio DT Data, Decrypted Type 3 Audio DT Data, and the video portion of Decrypted DT Data are not present on any user-accessible buses in analog or unencrypted, compressed form? *[Documentation is required.]* Note: "Decrypted DT Data: is defined in Section 2.2 in Exhibit C - General.	
3.2.5	Have you identified threats from use of "Widely Available Tools" in the context of Section 3.5.3.1 of Exhibit C - Part 1? Note: "Widely Available Tools" is defined in Section 3.5.3.1 in Exhibit C Part 1.	
3.2.6	Have you identified threats from use of "Specialized Tools" in the context of Section 3.5.3.1 of Exhibit C - Part 1? Note: "Specialized Tools" is defined in section 3.5.3.1 of Exhibit C Part 1.	
3.2.7	If the video portion of uncompressed, Decrypted DT Data with a resolution greater than a Constrained Image is transmitted over a User Accessible Bus, is such Decrypted DT Data reasonably secure from unauthorized interception by using "Widely Available Tools" and "Specialized Tools" except with difficulty? *[Documentation that assesses the level of difficulty is required.]*	

3.3 Methods of Making Function Robust

Distributed Functions -- Section 3.1 of Exhibit C - Part 1		
#		Y/N
3.3.1	Have you identified and documented all distributed functions in the product? *[Documentation is required.]* Note: Distributed Functions obligations are defined in Section 3.1 of Exhibit C Part 1.	
3.3.2	Do the distributed functions meet the requirements in Section 3.1 of Exhibit C – Part 1 about protection of Decrypted DT Data in any usable form flowing between portions that perform authentication and decryption and the MPEG (or similar) decoder? *[Documentation is required.]*	

3.4 Software

Section 3.2.1 of Exhibit C - Part 1		
#		Y/N
3.4.0	For Section 3.2 of Exhibit C Part 1: Have you identified the portions that will be implemented in Software and how they will meet requirements set forth in Sections 1 and 2 of Exhibit C Part 1? *[Documentation is required.]*	
3.4.1	Have you identified portion(s) that implements content protection requirements of DTCP2 Specification and Section 2.2.1.2 of Exhibit B Part 1-A in Software? *[Documentation is required.]*	
3.4.2	Have you identified and documented method(s) used to comply with Section 3.2.1 of Exhibit C Part 1 concerning protection of Secrecy Required Values? *[Documentation is required.]*	
3.4.3	Have you determined the methods used to protect instructions and data of Software from unauthorized access and modification (such as by isolating or protecting execution environment used to execute software)? By way of example, a secure allocation and/or encryption of memory space, clearing of memory space as a final operation, whenever possible, if clearing of the memory space is not achievable the memory space contents are unusable, and authentication of Software that can and cannot execute herein. It will provide secure interfaces to these functions, while creating a secure boundary. *[Documentation is required.]*	
Section 3.2.2 of Exhibit C - Part 1		
#		Y/N
3.4.4	Have you identified and documented method(s) used to perform self-checking of the integrity of component parts of the implementation as prescribed? *[Documentation is required.]*	
3.4.5	Does the implementation fail to provide authorized authentication and/or decryption when an unauthorized modification is attempted? Note: Modification is defined in Section 3.2.2 of Exhibit C Part 1.	
3.4.6	Does the provision use, at a minimum, "signed code" or more robust means of "tagging" operating throughout the code? *[Documentation is required.]*	

3.5 Hardware

Section 3.3 of Exhibit C - Part 1		
#		Y/N
3.5.1	Have you identified Primary L1 Core Functions? *[Documentation is required.]* Note: Primary L1 Core Functions are defined in Section 3.5.1 of Exhibit C Part 1.	
3.5.2	Have you identified portion(s) that implements content protection requirements of DTCP2 Specification or Section 2.2.1.2 of Part 1A of Exhibit B in Hardware? *[Documentation is required.]*	
3.5.3	Do portions above include all of the characteristics required in Sections 1 (Construction) and 2 (Data Paths) of Exhibit C Part 1? *[Documentation is required.]*	

Section 3.3.1 of Exhibit C - Part 1		
#		Y/N
3.5.4	For portion(s) that implement(s) content protection requirements of DTCP2 Specification implemented in Hardware and Primary L1 Core Function, have you identified and documented method(s) used to comply with Section 3.3.1 of Exhibit C Part 1 concerning protection of Secrecy Required Values? *[Documentation is required.]* Note: Examples of such methods are provided in Section 3.3.2 of Exhibit C Part 1.	
3.5.5	Which is used for implementation in Hardware? (Check all that apply): ☐silicon circuitry ☐firmware that cannot be reasonably read, with hardware root of trust ☐firmware employing the techniques described for Software with hardware root of trust ☐other method providing equivalent level of protection *[Documentation is required.]*	

3.5.6	Have you determined the methods used to enforce a secure hardware boundary for DTCP2 functions? By way of example, a secure allocation and/or encryption of memory space, clearing of memory space as a final operation, whenever possible, if clearing of the memory space is not achievable the memory space contents are unusable, and authentication of software and/or firmware that can and cannot execute herein. It will provide secure interfaces to these functions, while creating a secure boundary. *[Documentation is required.]*	
3.5.7	If hardened execution environment is used for your Implementation, have you documented how such hardened execution environment is established, such as with descriptions of the hardware root of trust and secure software loading mechanism? *[Documentation is required.]*	

Section 3.3.2 of Exhibit C - Part 1

#		Y/N
3.5.8	Would attempts to remove, replace, or reprogram Hardware elements that would compromise the content protection requirements of DTCP2 (including compliance with the Compliance Rules and DTCP2 Specification) in your Implementation pose a serious risk of rendering the final product unable to receive, decrypt, or decode DT Data? *[Documentation is required.]* Note: Examples of such methods are provided in Section 3.3.2 of Exhibit C Part 1.	

3.6 Level of Protection (L1 Level)

Primary L1 Core Functions, Section 3.5.1 of Exhibit C - Part 1		
#		Y/N
3.6.1	Are all of the Primary L1 Core functions in your Implementation implemented in Hardware as required in section 3.5.1 of Exhibit C Part 1? *[Documentation is required.]* Notes: Primary L1 Core Functions are defined in Section 3.5.1 of Exhibit C Part 1. Hardware is defined in Section 3.3 of Exhibit C Part 1.	
Other L1 Core Functions, Section 3.5.2 of Exhibit C - Part 1		
#		Y/N
3.6.2	Have you identified the Other L1 Core Functions? *[Documentation is required.]* Note: Other L1 Core Functions are defined in Section 3.5.2 of Exhibit C Part 1.	
L1 Core Functions of DTCP2 (Primary L1 Core Functions and Other L1 Core Functions) -- Section 3.5.3.1 of Exhibit C - Part 1		
#		Y/N
3.6.3	Have you identified threats from the use of "Widely Available Tools" in the context of Section 3.5.3.1 of Exhibit C - Part 1? *[Documentation is required.]* Note: Widely Available Tools are defined in Section 3.5.3.1 in Exhibit C Part 1.	
3.6.4	Have you identified threats from the use of "Specialized Tools" in the context of Section 3.5.3.1 of Exhibit C - Part 1? *[Documentation is required.]* Note: Specialized Tools are defined in Section 3.5.3.1 in Exhibit C Part 1.	
3.6.5	Have you identified threats from the use of "Professional Software Tools" in the context of Section 3.5.3.1 of Exhibit C - Part 1? *[Documentation is required.]* Note: Professional Software Tools are defined in Section 3.5.3.1 of Exhibit C Part 1.	
3.6.6	Does implementation of L1 Core Functions meet the requirements of Section 3.5.3.1 about attack using Widely Available Tools, Specialized Tools and Professional Software Tools? *[Documentation is required.]* Note: "L1 Core Function" means Primary L1 Core Functions and Other L1 Core Functions.	

L1 Core Functions of DTCP2 -- Section 3.5.3.2 of Exhibit C - Part 1		
#		Y/N
3.6.7	Have you identified threats from the use of "Professional Hardware Tools" in the context of Section 3.5.3.2 of Exhibit C - Part 1? *[Documentation is required.]* Note: Professional Hardware Tools are defined in Section 3.5.3.2 of Exhibit C Part 1.	
3.6.8	Does implementation of L1 Core Functions meet the requirements of Section 3.5.3.2 of Exhibit C Part 1 concerning attacks using Professional Hardware Tools? Note: "L1 Core Function" means Primary L1 Core Functions and Other L1 Core Functions.	
Section 3.6 of Exhibit C - Part 1		
#		Y/N
3.6.9	Have you identified threats from the use of "Widely Available Tools" in the context of Section 3.6 of Exhibit C - Part 1 and added to your threat list? *[Documentation is required.]* Note: Widely Available Tools are defined in Section 3.5.3.1 in Exhibit C Part 1.	
3.6.10	Does your implementation meet the requirements of Section 3.6(i) of Exhibit C - Part 1 concerning protection of delivery of Decrypted DT Data to outputs specified in such section?	
3.6.11	If a Common Device Key and corresponding Common Device Certificate is used, does your Implementation meet the requirements of Section 3.6(ii) of Exhibit C - Part 1 about protection of the method by which the DTCP2 functions are designed to cease to function in case of an attempt to defeat such functions?	

4. Exhibit C Part 2 RR For L2 Protection

The answer to the questions is in general either YES or NO however; NA for Not Applicable may be used when the associated function is not implemented.

4.1 Construction – Defeating Functions

Construction – Defeating Functions - Section 1.2 of Exhibit C - Part 2		
Has your product been designed without the following "defeating functions" – i.e., functions that can defeat the mandatory provisions of the DTCP2 Specification or the Compliance Rules, including the content protection technologies, analog protection systems, output protections, output restrictions, recording protections, recording limitations, or can expose Decrypted DT Data to unauthorized output, interception, retransmission, or copying?		
#		Y/N
4.1.1	switches, buttons, jumpers or software equivalents thereof	
4.1.2	specific traces (electrical connections) that can be cut	
4.1.3	special functions or modes of operation (including service menus and remote-control functions)	
4.1.4	active JTAG ports, active emulator interfaces or active test points, to probe security functions *[Documentation is required showing how such ports, interfaces, and test points are rendered inactive.]*	
4.1.5	Have you specified a process and requirement whereby all debug functions and software traces that constitute Defeating Functions in the production version will comply with these Robustness Rules requirements including, by way of example, by (a) removing such debug functions or software traces, or (b) rendering inactive such debug functions or software traces where such method of making inactive meets the Level of Protection requirement in Section 3.5 of Exhibit C-Part2? Note: Adopter shall pay special attention to serial, USB, or other interfaces to the hardware that provide external access to the kernel to execute debug functions, or other commands, relating to DTCP2. *[Documentation is required.]*	

4.2 Data Paths

Data Paths - Section 2 of Exhibit C - Part 2		
#		Y/N
4.2.0	Which of the following functions does your Implementation have in L2 protection? ☐Source Function ☐Sink Function Note: Questions 4.2.1 to 4.2.2 are applicable only to an Implementation that has Sink Function with L2 protection.	
4.2.1	Have you identified and documented all outputs of product? *[Documentation is required.]*	
4.2.2	Have you performed and documented tests that ensure Decrypted DT Data does not appear on outputs that are not specified in the Compliance Rules? *[Documentation is required.]* Note: Permitted outputs are specified in Section 4 of Exhibit B Part 1B.	
4.2.3	Have you identified and documented all user accessible buses in product? *[Documentation is required.]* Note: User Accessible Bus is defined in Section 2.1 of Exhibit C Part 2.	
4.2.4	Have you performed and documented tests that ensure Decrypted Type 2 Audio DT Data, Decrypted Type 3 Audio DT Data, and the video portion of Decrypted DT Data are not present on any user-accessible buses in analog or unencrypted form? *[Documentation is required.]* Note: Decrypted DT Data is defined in Section 2.2 of Exhibit C General.	

4.3 Methods of Making Functions Robust

Distributed Functions - Section 3.1 of Exhibit C - Part 2		
#		Y/N
4.3.1	Have you identified all distributed functions in product? *[Documentation is required.]* Note: Distributed Functions are described in Section 3.1 of Exhibit C Part 2.	
4.3.2	Do the distributed functions meet the requirement in Section 3.1 of Exhibit C, Part 2 concerning protection of Decrypted DT Data in any usable form flowing between portions in your product? *[Documentation is required.]*	

4.4 Software

Section 3.2.1 of Exhibit C - Part 2		
#		Y/N
4.4.0	For Section 3.2 of Exhibit C Part 2: Have you identified the portions that will be implemented in Software and how they will meet requirements set forth in Sections 1 and 2 of Exhibit C Part 2? *[Documentation is required.]*	
4.4.1	Have you identified portion(s) that implement content protection requirements of the DTCP2 Specification in Software? *[Documentation is required.]* Note: Software is defined in Section 3.2 of Exhibit C Part 2.	
4.4.2	Have you identified and documented method(s) used to comply with Section 3.2.1 of Exhibit C Part 2 concerning protection of Secrecy Required Values? *[Documentation is required.]*	
4.4.3	Have you identified the technique(s) of obfuscation (product or process name) used for Software to comply with the requirements of Section 3.2.1 of Exhibit C Part 2? *[Documentation is required.]*	
4.4.4	Have you determined the methods used to protect instructions and data of Software from unauthorized access and modification (such as by isolating or protecting execution environment used to execute software)? By way of example, a secure allocation and/or encryption of memory space, clearing of memory space as a final operation, whenever possible, if clearing of the memory space is not achievable the memory space contents are unusable, and authentication of Software that can and cannot execute herein. It will provide secure interfaces to these functions, while creating a secure boundary. *[Documentation is required.]*	
Section 3.2.2 of Exhibit C - Part 2		
#		Y/N
4.4.4	Have you identified and documented method(s) used to perform self-checking of the integrity of component parts of the implementation as prescribed? *[Documentation is required.]*	
4.4.5	Does the implementation fail to provide authorized authentication and/or decryption with its code having unauthorized modification? Note: Modification is defined in Section 3.2.2 of Exhibit C Part 2.	

4.4.6	Does the provision use “signed code” or more robust means of “tagging” operation throughout the code? *[Documentation is required.]*	

4.5 Hardware

Section 3.3 of Exhibit C - Part 2		
#		Y/N
4.5.1	Have you identified and documented portion(s) that implement content protection requirements of the DTCP2 Specification in Hardware? *[Documentation is required.]* Note: Hardware is defined in Section 3.3 of Exhibit C Part 2.	
4.5.2	Have you identified and documented DTCP2 Primary Core Functions? *[Documentation is required.]* Note: DTCP2 Primary Core Functions are defined in Section 3.5 of Exhibit C Part 2.	
4.5.3	Do portions above include all of the characteristics required in Sections 1 (Construction) and 2 (Data Paths) of Exhibit C Part 2?	

Section 3.3.1 of Exhibit C - Part 2		
#		Y/N
4.5.4	For portion(s) that implement content protection requirements of DTCP2 Specification in Hardware and DTCP2 Primary Core Function, have you identified and documented method(s) used to comply with Section 3.3.1 of Exhibit C - Part 2 concerning protection of Secrecy Required Values? *[Documentation is required.]* Note: Examples of such methods are provided in Section 3.3.2 of Exhibit C Part 2.	
4.5.5	Which is used for implementation in Hardware? (Check all that apply): ☐silicon circuitry ☐firmware that cannot be reasonably read, with hardware root of trust ☐firmware employing the techniques described for Software with hardware root of trust ☐other method providing equivalent level of protection *[Documentation is required.]*	

4.5.6	Have you determined the methods used to enforce a secure hardware boundary for DTCP2 functions (such as by isolating or protecting execution environment used to execute software)? By way of example, a secure allocation and/or encryption of memory space, clearing of memory space as a final operation, whenever possible, if clearing of the memory space is not achievable the memory space contents are unusable, and authentication of software and/or firmware that can and cannot execute herein. It will provide secure interfaces to these functions, while creating a secure boundary. *[Documentation is required.]*	
4.5.7	If hardened execution environment is used for your Implementation, have you documented how such hardened execution environment is established, such as with descriptions of the hardware root of trust and secure software loading mechanism? *[Documentation is required.]*	
Section 3.3.2 of Exhibit C - Part 2		
#		Y/N
4.5.8	Do attempts to remove, replace or reprogram Hardware elements that would compromise the content protection requirements of DTCP2 (including compliance with the Compliance Rules and DTCP2 Specification) in your product pose a serious risk of rendering the final product unable to receive, decrypt, or decode DT Data? *[Documentation is required.]* Note: Examples of such methods are provided in Section 3.3.2 of Exhibit C Part 2.	

4.6 Level of Protection (L2 Level)

DTCP2 Core Functions, Section 3.5 of Exhibit C - Part 2		
#		Y/N
4.6.1	Are all of the DTCP2 Primary Core functions in your Implementation implemented in Hardware as required in Section 3.5 of Exhibit C Part 2? Note: DTCP2 Primary Core Functions are defined in Section 3.5 of Exhibit C Part 2. Hardware is defined in Section 3.3 of Exhibit C Part 2.	

4.6.2	Have you identified the Other DTCP2 Core Functions in your product? *[Documentation is required.]* Note: Other DTCP2 Core Functions are defined in Section 3.5 of Exhibit C Part 2.	
All DTCP2 Core Functions, Section 3.5.1 of Exhibit C - Part 2		
#		Y/N
4.6.3	Have you identified threats from the use of "Widely Available Tools" in the context of Section 3.5.1 of Exhibit C – Part 2? *[Documentation is required.]* Note: Widely Available Tools are defined in Section 3.5.1 of Exhibit C Part 2.	
4.6.4	Have you identified threats from the use of "Specialized Tools" in the context of Section 3.5.1 of Exhibit C - Part 2? *[Documentation is required.]* Note: Specialized Tools are defined in Section 3.5.1 of Exhibit C Part 2.	
4.6.5	Have you identified threats from the use of "Professional Software Tools" in the context of Section 3.5.1 of Exhibit C - Part 2? *[Documentation is required.]* Note: Professional Software Tools are defined in Section 3.5.1 of Exhibit C Part 2.	
4.6.6	Does implementation of DTCP2 Primary Core Functions and Other DTCP2 Core Functions meet the requirements of Section 3.5.1 concerning attacks using Widely Available Tools, Specialized Tools and Professional Software Tools? Note: DTCP2 Primary Core Functions and Other DTCP2 Core Functions are defined in Section 3.5 of Exhibit C Part 2.	
All DTCP2 Core Functions, Section 3.5.2 Exhibit C - Part 2		
#		Y/N
4.6.7	Have you identified threats from the use of "Professional Hardware Tools" in the context of Section 3.5.2 of Exhibit C - Part 2? *[Documentation is required.]* Note: Professional Hardware Tools are defined in Section 3.5.2 of Exhibit C Part 2.	
4.6.8	Does implementation of DTCP2 Primary Core Functions and Other DTCP2 Core Functions meet the requirements of Section 3.5.2 of Exhibit C Part 2 concerning attacks using Professional Hardware Tools? Note: DTCP2 Primary Core Functions and Other DTCP2 Core Functions are defined in Section 3.5 of Exhibit C Part 2.	

Section 3.6 of Exhibit C - Part 2		
#		Y/N
4.6.9	Have you identified threats from the use of "Widely Available Tools"? *[Documentation is required.]* Note: Widely Available Tools are defined in Section 3.5.1 of Exhibit C Part 2.	
4.6.10	Does your implementation meet the requirements of Section 3.6(i) of Exhibit C - Part 2 about protection of delivery of Decrypted DT Data to outputs specified in such section?	
4.6.11	If a Common Device Key and corresponding Common Device Certificate is used, does your Implementation meet the requirements of Section 3.6(ii) of Exhibit C - Part 2 about protection of the method by which the DTCP2 functions are designed to cease to function in case of an attempt to defeat such functions?	

AFFIRMATION OF
ADOPTER REPRESENTATIVE

A. Adopter Representative

The undersigned hereby affirms that he or she (a) has been designated by Adopter as having managerial responsibility for the design of the Implementation identified in Section 1.6 of this Robustness Verification List, (b) understands the requirements pertaining to robustness and the Robustness Verification List in accordance with the Procedural Appendix and Exhibit C of the DTCP2 Adopter Agreement, and (c) has reviewed Adopter's responses on the Robustness Verification List and finds them to be true and correct.

Date:_____

_____
(Signature)

Name:_____

Title:_____

Business Address:

Email:_____

EXHIBIT D: ACTIVATION NOTICE

The undersigned ("Adopter") having entered into a DTCP2 DIGITAL TRANSMISSION PROTECTION LICENSE AGREEMENT–Evaluation License Convertible to Product License (the "DTCP2 Adopter Agreement") with Digital Transmission Licensing Administrator, LLC ("DTLA") hereby activates its rights under the DTCP2 Adopter Agreement in accordance with Section 2.2 of the DTCP2 Adopter Agreement subject to the following:

(1) Adopter chooses to be a:

Component Supplier	☐
Adopter- Small	☐
Adopter- Large	☐

(choose only one category)

(2) The fees to be paid in connection with the: (i) activation of the DTCP2 Adopter Agreement and selection of an Adopter category; and (ii) issuance, shipping and handling of DTCP2 Device Certificates and DTCP2 Device Keys, are set forth on Exhibit A to this Activation Notice, which may be amended by DTLA in accordance with the terms of the DTCP2 Adopter Agreement.

(3) The evaluation fee paid by Adopter shall be credited against the fees associated with the chosen Adopter category.

(4) Adopter acknowledges and agrees that DTLA shall ship all orders for DTCP2 Device Certificates and DTCP2 Device Keys in electronic form using Pretty Good Privacy (PGP) as described in the DTLA DTCP2 Keying Material Order Guide.
If Adopter does not have or is unable to provide DTLA its PGP public key, Adopter shall, at its own cost and expense, with each order placed with DTLA, designate an agent who shall pick up the generated DTCP2 Device Certificates and DTCP2 Device Keys at a location designated by DTLA.

(5) All capitalized terms not otherwise defined herein shall have the meanings set forth in the DTCP2 Adopter Agreement.

Please make checks payable to "DTLA" and send such check, together with an executed copy of this Activation Notice and, if available, a CD-ROM containing Adopter's public key, to the following address:

Digital Transmission Licensing Administrator
c/o License Management International, LLC
380 Tennant Ave., Unit 4
Morgan Hill CA 95037-5478

Please call for wire information.

_____
Company Name
By:_____
Name:_____
Title:_____
Date: _____

EXHIBIT 1
TO THE
ACTIVATION NOTICE

ADOPTER CATEGORY ADMINISTRATION FEES

Component Supplier:	$14,000
Small Adopter Fee:	$14,000
Large Adopter Fee:	$18,000

DTCP2 DEVICE CERTIFICATE AND DTCP2 DEVICE KEY FEES

Shipping and Handling - $200.00 / order

Category	Per Unique DTCP2 Certificate Fee (US $)
DTCP2 Adopter - Small	.07
DTCP2 Adopter - Large	.06

Per Common DTCP2 Certificate Fee
(DTCP2 Adopter - Large Only)

Unit Options

Up to a maximum of 4 keys/total 20,000 units or copies -- $1,000
Up to 100,000 units or copies -- $2,000
Up to 200,000 units or copies -- $4,000
Up to 500,000 units or copies -- $6,000
Up to 1,000,000 units or copies -- $10,000
Up to 2,000,000 units or copies -- $12,000
Up to 5,000,000 units or copies -- $15,000
Up to10,000,000 units or copies -- $25,000
Up to 30,000,000 units or copies -- $50,000

Blanket Option

Up to a maximum of 5 Common DTCP2 Device Keys and Common DTCP2 Device Certificates -- $100,000

Additional Common DTCP2 Device Keys and Common DTCP2 Device Certificates -- $1,000

OTHER FEES: • The fee for replacing a PGP key is $3000.00
• The fee for additional hardcopies of DTLA confidential or highly confidential specifications is $500.00