Requirements for the Protection of
Unencrypted Digital Terrestrial Broadcast Content
Against Unauthorized Redistribution[1]

Discussion Draft
[THE CHANGES SHOWN IN THIS DRAFT ARE PART OF A PROPOSAL, BY COMPUTER INDUSTRY GROUP COMPANIES, 5C COMPANIES AND MPAA MEMBER COMPANIES, WHICH ALSO INCLUDES PROPOSED CRITERIA FOR AUTHORIZING TECHNOLOGIES ON TABLE A]
April ~~14~~25, 2002

[X.] Requirements.

X.1 Definitions.

"Authorized Digital Output Protection Technology" means a technology listed on Table A, as such list may be amended from time to time pursuant to Section [] [anticipates section (to be discussed by the parallel group in accordance with the "Notes" to the "Proposal to BPDG for Table A Criteria") that would specify~~, in a manner consistent with the enforcement structure,~~ how ~~other~~ technologies would be added to and removed from the list of Authorized Digital Output Protection Technologies].

"Authorized Recording Method" means a recording method listed on Table A, as such list may be amended from time to time pursuant to Section [] [anticipates section (to be discussed by the parallel group in accordance with the "Notes" to the "Proposal to BPDG for Table A Criteria") that would specify~~, in a manner consistent with the enforcement structure,~~ how ~~other~~ recording methods would be added to and removed from the list of Authorized Recording Methods].

"Broadcast Flag" means the ATSC Redistribution Control descriptor described in ATSC Standard A/65A: Program and System Information Protocol for Terrestrial Broadcast and Cable, 31 May 00, Amendment 3, 15 October 01[2].

---

[1]This draft sets forth requirements to be imposed on certain products that receive unencrypted digital terrestrial broadcast content to protect such content against unauthorized redistribution outside of the home or personal digital network environment. (A request has been made by MPAA member companies to discuss the meaning of the phrase "home or personal digital network environment" in the parallel group.) The draft assumes that the requirements will apply in the United States, although we anticipate that the requirements could be modified, as necessary, for use in other jurisdictions.

"Circumvention Devices" means devices or technologies that are designed and made available for the specific purpose of bypassing or circumventing the protection technologies used to meet the requirements set forth in this Section X.

"Compliance Requirements" means the requirements set out in Sections X.3 through X.6.

"Computer Product" means a product that is designed for or permits the end user to install a wide variety of commercially available software applications thereon, such as a personal computer, handheld "Personal Digital Assistant" and the like, and further includes a subsystem of such a product, such as a graphics card.

"Covered Product" means a product (whether a physical device, software or combination thereof) that is required under Section X.2 to comply with the Compliance Requirements, and to be manufactured in accordance with Robustness Requirements, prior to being sold or distributed.

"Demodulation Function" means a component, or set of components, that is specifically designed to perform 8-VSB, 64-QAM or 256-QAM demodulation of Unencrypted Digital Terrestrial Broadcast Content and thereby produce a data stream consistent with ATSC Standard A/53 Annex C[3] (e.g., a demodulation chip or demodulation software) [, where "8-VSB" means vestigial sideband modulation with 8 discrete amplitude levels, as described in ATSC Standard A/53, and "64-QAM" and "256-QAM" mean Quadrature Amplitude Modulation with 64-point and 256-point constellations, respectively, both as described in "Digital Video Transmission Standard for Cable Television", ANSI/SCTE 07 2000].

"Downstream Product" means a product (whether a physical device, software or combination thereof) that is capable of accessing in usable form[4] Unscreened Content or Marked Content passed to such product via a Robust Method, where the manufacturer of such product has committed in writing[5] that such product will comply with the

---

[2] Where the requirements set forth in this document are implemented in jurisdictions outside the United States, the definition of Broadcast Flag would need to be revised to reflect the appropriate location for the flag in the applicable digital broadcast television standard for each such jurisdiction.

[3] We anticipate that these requirements would need to be amended if, in the future, new modulation standards replace those listed.

[4] The fact that a stream containing Unscreened Content or Marked Content has not been altered following demodulation does not mean in and of itself that such content is not in "usable form".

[5] Nature of written commitment to be discussed by parallel group.

Compliance Requirements and be manufactured in accordance with the Robustness Requirements [, such that such product shall be a Covered Product].[6]

"EIT" means Event Information Table as defined in ATSC Standard A/65A: Amendment No. 1 (2000) Program and System Information Protocol for Terrestrial Broadcast and Cable.

"Hardware" means a physical device, including a component, that implements in a Covered Product any of the content protection requirements set forth in the Compliance Requirements and that (i) does not include instructions or data other than such instructions or data that are permanently embedded in such Covered Product or (ii) includes instructions or data that are not permanently embedded in such Covered Product where such instructions or data have been customized for such Covered Product and such instructions or data are not accessible to the end user through the Covered Product.

"Marked Content" means, with respect to a Covered Product, Unencrypted Digital Terrestrial Broadcast Content that such product has (a) received and demodulated using its Demodulation Function and for which such product has inspected either the EIT or PMT and determined the Broadcast Flag to be present or (b) where such product is a Downstream Product, received via a Robust Method and accessed in usable form, and for which such product either inspected the EIT or PMT and determined the Broadcast Flag to be present or determined through information conveyed with such content (via such Robust Method) that another Covered Product had previously so screened such content and determined the Broadcast Flag to be present; provided, however, that, with respect to such Covered Product, "Marked Content" shall not include content that has been passed from such Covered Product other than pursuant to Section X.4(a)(3)~~X.4(a)(4)~~.

"PMT" means Program Map Table as defined in ISO/IEC IS 13818-1:1 2000 (E), International Standard, MPEG-2 Systems.

"Robust Method" means, with respect to the passing of Unscreened Content or Marked Content from one product to another, a method that complies with the robustness requirements set forth in Section X.10 and is designed to ensure that such content may be accessed in usable form by such other product only if the manufacturer of such other product has committed in writing[7] that such product will comply with the Compliance

[6] Note that Downstream Products would be required under Section X.2 to comply with the Compliance Requirements and Robustness Requirements prior to being sold or distributed (i.e., a failure to comply with such requirements would be a violation of, and subject to enforcement under, the instrument promulgating these requirements).

[7] Nature of written commitment to be discussed by parallel group.

Requirements and be manufactured in accordance with the Robustness Requirements ~~[~~, such that such product shall be a Covered Product~~]~~.[8]

"Robustness Requirements" means the requirements set out in Sections X.7 through X.11.

"Software" means the implementation in a Covered Product of any of the content protection requirements set forth in the Compliance Requirements through any computer program code consisting of instructions or data, other than such instructions or data that are included in Hardware.

~~[~~"Transitory Image" means data that has been stored temporarily for the sole purpose of enabling a function not prohibited by this Section X but that (a) does not persist materially after such function has been performed and (b) is not stored in a way that permits copying or storing of such data for other purposes.~~]~~

"Unencrypted Digital Terrestrial Broadcast Content" means ~~[the content of the [primary] video signal][[free over-the-air]~~ audiovisual content contained in the ATSC Transport Stream ~~and program-related data]~~ broadcast by a digital television station in compliance with the digital broadcast television transmission standard set forth in 47 C.F.R. Section 73.682(d)[9], without encrypting or otherwise making the ~~signal~~ content available through a technical means of conditional access, and includes ~~the content of~~ such ~~signal~~ content when retransmitted by a digital broadcast [or by a conditional access delivery system].

"Unscreened Content" means, with respect to a Covered Product, Unencrypted Digital Terrestrial Broadcast Content for which such product has inspected neither the EIT nor the PMT for the Broadcast Flag and that such product either (a) received and demodulated using its Demodulation Function or (b) where such product is a Downstream Product, received via a Robust Method and accessed such content in usable form and determined through information conveyed with such content (via such Robust Method) that such content was not previously so screened by another Covered Product; provided, however, that, with respect to such Covered Product, "Unscreened Content" shall not include content that has been passed from such Covered Product other than pursuant to Section X.3(a)(4).

---

[8] Note that ~~P~~products manufactured under such commitment would be required under Section X.2 to comply with the Compliance Requirements and Robustness Requirements prior to being sold or distributed (i.e., a failure to comply with such requirements would be a violation of, and subject to enforcement under, the instrument promulgating these requirements).

[9] Definition to be revised where the instrument promulgating these requirements applies in jurisdictions outside the United States.

~~[“User” means a consumer of a Covered Product but not a professional trained to repair, build or service a Covered Product.]~~

“User Accessible Bus” means a data bus that is designed for end user upgrades or access, such as an implementation of a smartcard interface, 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 usable by end users.

X.2

[Note to BPDG: it is assumed for purposes of technical evaluation that the instrument promulgating the Compliance Requirements and Robustness Requirements below would include provisions that specify the circumstances under which the Compliance Requirements and Robustness Requirements would apply. This Section X.2 is a placeholder for such provisions. Please see separate documents, prepared by studio representatives to the drafting committee, on the one hand, and CE and IT representatives to the drafting committee, on the other hand, reflecting concepts that such representatives assume would be included in such provisions. Note that such separate document prepared by studio representatives may require certain updates in light of changes made in this document.]

X.3 Compliance Requirements: Unscreened Content.[10]

(a) A Covered Product shall not pass, or direct to be passed, Unscreened Content to any output except

(1) to an analog output;

[add consumer modulators with appropriate conditions]

(2) to a digital output protected by an Authorized Digital Output Protection Technology, in accordance with any obligations set out on Table A applicable to such Authorized Digital Output Protection Technology;

(3) where ~~[~~the stream containing such content has not been altered following demodulation and~~]~~[11] such Covered Product outputs, or directs to be output, such

[10] No requirements or limitations are imposed by this Section X with respect to the output, recording, or other handling of content other than Unscreened Content and Marked Content.

[11] ~~Consensus was not reached within the drafting committee as to whether the bracketed language should be included or omitted.~~

content to a Downstream Product solely within the home or ~~[personal digital network][~~other, similar local~~]~~[12] environment, using a Robust Method;

(4) where such Covered Product outputs, or directs to be output, such content to another product and such Covered Product exercises sole control (such as by using a cryptographic protocol), in compliance with the Robustness Requirements, over the access to such content in usable form in such other product;

(5) where such Covered Product outputs, or directs to be output, such content for the purpose of making a recording of such content pursuant to Section X.3(b)(2), where such content is protected by the corresponding recording method[13]; or

(6) ~~[~~where such Covered Product is incorporated into a Computer Product and passes, or directs to be passed, such content to an unprotected DVI output as an image having ~~[no more than 30 frames per second and]~~ the visual equivalent of no more than (a) 350,000 pixels per frame (e.g. an image with resolution of 720 x 480 pixels for a ~~3:2~~4:3 (non-square pixel) aspect ratio) and (b) 30 frames per second. Such an image may be attained by reducing resolution, such as by discarding, dithering or averaging pixels to obtain the specified value, and can be displayed using video processing techniques such as line doubling or sharpening to improve the perceived quality of the image.~~]~~

(b) A Covered Product shall not record or cause the recording of Unscreened Content in digital form unless such recording is made using one of the following methods:

(1) ~~[~~a method that ~~uses an encryption protocol, or other means at least as effective, to~~ effectively and uniquely associates such recording with a single Covered Product (using a cryptographic protocol or other effective means) so that such recording cannot be accessed in usable form by another product except where such recording (or a copy thereof) is passed to another product as permitted under this Section X~~]~~ ~~[a method that uses an Authorized Recording Method for Removable Media technology, or other means at least as effective, to uniquely associate such recording with a single Covered Product so that such recording cannot be played on another~~

~~[12] The second alternative was raised, but the drafting committee did not reach consensus regarding which of the two alternatives should be adopted.~~

[13] For example, a protected recording made onto storage media located in an external drive, where the recorder first encrypts the content and then passes it to the drive via an output.

~~product and that no further usable copies may be made thereof except by such Covered Product]~~[14] or

(2) an Authorized Recording Method, in accordance with any obligations set out in Table A applicable to such Authorized Recording Method ~~[~~(provided that for recordings made on removable media, only Authorized Recording Methods expressly identified on Table A for use in connection with removable media may be used)~~][, or [,where the stream containing such content has not been altered following demodulation,] other method that …[track three alternatives from X.10]]~~[15].

~~[~~This Section X.3(b) does not impose restrictions regarding the storage of Unscreened Content as a Transitory Image.~~]~~

X.4 Compliance Requirements: Marked Content.

(a) A Covered Product shall not pass, or direct to be passed, Marked Content to any output except

(1) to an analog output;

[add consumer modulators with appropriate conditions]

(2) to a digital output protected by an Authorized Digital Output Protection Technology, in accordance with any obligations set out on Table A applicable to such Authorized Digital Output Protection Technology;

~~(3)[where such Covered Product outputs, or directs to be output, such content to a Downstream Product solely within the home or personal digital network environment, using a Robust Method;]~~[16]

~~(4)~~(3) where such Covered Product outputs, or directs to be output, such content to another product and such Covered Product exercises sole control (such as by using a cryptographic protocol), in compliance with the Robustness Requirements, over the access to such content in usable form in such other product;

---

[14] ~~The drafting committee has been discussing the bracketed alternatives but has not reached consensus regarding the adoption of either one of the alternatives.~~

[15] ~~Consensus was not reached within the drafting committee as to whether this provision should be included or omitted.~~

[16] ~~Consensus was not reached within the drafting committee as to whether this provision should be included or omitted.~~

~~(5)~~(4) where such Covered Product outputs, or directs to be output, such content for the purpose of making a recording of such content pursuant to Section X.4(b)(2), where such content is protected by the corresponding recording method[17]; or

~~(6)~~(5) ~~[~~where such Covered Product is incorporated into a Computer Product and passes, or directs to be passed, such content to an unprotected DVI output as an image having ~~[no more than 30 frames per second and]~~ the visual equivalent of no more than (a) 350,000 pixels per frame (e.g. an image with resolution of 720 x 480 pixels for a ~~3:2~~4:3 (non-square pixel) aspect ratio) and (b) 30 frames per second. Such an image may be attained by reducing resolution, such as by discarding, dithering or averaging pixels to obtain the specified value, and can be displayed using video processing techniques such as line doubling or sharpening to improve the perceived quality of the image.~~]~~

(b) A Covered Product shall not record or cause the recording of Marked Content in digital form unless such recording is made using one of the following methods:

(1) ~~[~~a method that ~~uses an encryption protocol, or other means at least as effective, to~~ effectively and uniquely associates such recording with a single Covered Product (using a cryptographic protocol or other effective means) so that such recording cannot be accessed in usable form by another product except where such recording (or a copy thereof) is passed to another product as permitted under this Section X~~]~~ ~~[a method that uses an Authorized Recording Method for Removable Media technology, or other means at least as effective, to uniquely associate such recording with a single Covered Product so that such recording cannot be played on another product and that no further usable copies may be made thereof except by such Covered Product]~~[18] or

(2) an Authorized Recording Method, in accordance with any obligations set out in Table A applicable to such Authorized Recording Method ~~[~~(provided that for recordings made on removable media, only Authorized Recording Methods expressly identified on Table A for use in connection with removable media may be used)~~] [, or other method that …[track three alternatives from X.10]]~~[19].

[17] For example, a protected recording made onto storage media located in an external drive, where the recorder first encrypts the content and then passes it to the drive via an output.

~~[18] The drafting committee has been discussing the bracketed alternatives but has not reached consensus regarding the adoption of either one of the alternatives.~~

[19] Consensus was not reached within the drafting committee as to whether this provision should be included or omitted.

~~[~~This Section X.4(b) does not impose restrictions regarding the storage of Marked Content as a Transitory Image.~~]~~

X.5 ~~[~~Audio. Except as otherwise provided in Sections X.3(a) or X.4(a), Covered Products shall not output the audio portions of Unscreened Content or of Marked Content in digital form except in compressed audio format (such as AC3) or in Linear PCM format in which the transmitted information is sampled at no more than 48 kHz and no more than 16 bits.~~]~~

X.6 ~~Integrated~~ Add-in Covered Products.[20] Where a Covered Product passes Unscreened Content or Marked Content from such Covered Product to another product, other than where such Covered Product passes, or directs to be passed, such content to an output (e.g., where a demodulator add-in card in a personal computer passes such content to an associated software application installed in the same computer), it shall so pass such content ~~[~~(a) protected by an Authorized Digital Output Protection Technology, in accordance with any obligations set out on Table A applicable to such Authorized Digital Output Protection Technology or (b)~~]~~ using a Robust Method. Neither Unscreened Content nor Marked Content may be so passed in unencrypted, compressed form via a User Accessible Bus.

X.7 Robustness: Construction

(a) Covered Products shall be manufactured in a manner clearly designed to effectively frustrate ~~[User]~~ attempts to modify such Covered Products to defeat the Compliance Requirements.

(b) Covered Products shall not include:

(1) switches, buttons, jumpers or software equivalents thereof,

(2) specific traces that can be cut, or

(3) functions (including service menus and remote-control functions),

in each case by which the Compliance Requirements can be defeated, or by which compressed unencrypted Marked Content or compressed unencrypted Unscreened

[20] It is not the intent of the drafting committee to generally incorporate Downstream Products into X.4(a)~~X.4(a)~~ or to override the limitations of X.3(a)(3)~~X.3(a)(4)~~.

Content in such Covered Products can be exposed to output, interception, retransmission or copying, in each case other than as permitted under this Section X.[21,22]

(c) Covered Products shall be manufactured in a manner that is clearly designed to effectively frustrate attempts to discover or reveal any secret keys or secret algorithms used to meet the requirements set forth in this Section X.

X.8 Robustness: Data Paths. Within a Covered Product, neither Unscreened Content nor Marked Content shall be present on any User Accessible Bus in unencrypted, compressed form.

[*Note to reader: The instrument promulgating these requirements could also address the issues raised in Section 2.2 of the Robustness Rules for DTCP (alerting manufacturers that the robustness requirements may be modified in the future to require the protection of uncompressed data on a User Accessible Bus, when it is technically feasible and commercially reasonable to do so.)*]

X.9 Methods of Making Functions Robust. Covered 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~~]~~.

(a) Distributed Functions. Where compressed Unscreened Content or compressed Marked Content is delivered from one portion of the Covered Product to another portion of such Covered Product, whether among integrated circuits, software modules, a combination thereof, or otherwise, such portions shall be designed and manufactured in a manner associated and otherwise integrated with each other such that such Unscreened Content or Marked Content, as the case may be, in any usable form flowing between such portions of such Covered Product shall be reasonably secure from being intercepted or copied ~~[by a User]~~ except as permitted under the Compliance Requirements.

(b) Software. Without limiting the requirements of Sections X.7 and X.8, portions of a Covered Product that implement in Software the content protection requirements set forth in the Compliance Requirements shall:

---

[21] See italicized note at the end of Section X.8~~X.7~~. It is anticipated that if the Robustness Requirements are modified in the future to require protection of uncompressed data on a User Accessible Bus, the requirements of Section X.7(b)~~X.6(b)~~ would also then be modified to apply to uncompressed unencrypted content.

[22] For avoidance of doubt, the provisions of X.7(b)~~X.6(b)~~ prohibit inclusion of such means by which such defeating or exposure can occur through modification of the state of the Broadcast Flag.

(1) Comply with Section X.7(c) by a reasonable method including but not limited to: encryption, execution of a portion of the implementation in ring zero or supervisor mode (i.e. in kernel mode), and/or embodiment in a secure physical implementation; and, in addition, using techniques of obfuscation clearly designed to effectively disguise and hamper attempts to discover the approaches used.

(2) Be designed so as to perform or ensure checking of the integrity of its component parts such that unauthorized modifications ~~[by a User]~~ will be expected to result in a failure of the implementation to provide access to unencrypted Unscreened Content or unencrypted Marked Content. For purposes of this Section X.9(b)(2), a "modification" includes any change in, or disturbance or invasion of, features or characteristics, or interruption of processing, relevant to Sections X.7 and X.8. This Section X.9(b)(2) requires at a minimum the use of signed code or more robust means of "tagging" operating throughout the code. ~~[~~For purposes of this Section X.9(b), "signed code" means a method of achieving trusted distribution of Software by using public key cryptography, keyed hash, or other means at least as effective, to form a digital signature over Software such that its authenticity and integrity can be verified.~~]~~

(c) Hardware. Without limiting the requirements of Sections X.7 and X.8, the portions of a Covered Product that implement in Hardware the content protection requirements set forth in the Compliance Requirements shall:

(1) Comply with Section X.7(c) by any reasonable method including but not limited to (x) embedding any secret keys or secret cryptographic algorithms used to meet the content protection requirements set forth in the Compliance Requirements in silicon circuitry or firmware that cannot reasonably be read or (y) employing the techniques described above for Software.

(2) Be designed such that attempts ~~[by a User]~~ to remove, replace, or reprogram Hardware elements in a way that would compromise the content protection requirements set forth in the Compliance Requirements in Covered Products would pose a serious risk of rendering the Covered Product unable to receive, demodulate, or decode Unencrypted Digital Terrestrial Broadcast Content. By way of example, a component that is soldered rather than socketed, or affixed with epoxy, may be appropriate for this means.

(d) Hybrid. The interfaces between Hardware and Software portions of a Covered 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 that would be provided by a pure Software implementation.

X.10 Robust Methods. Where a Covered Product passes, or directs to be passed, Unscreened Content or Marked Content from such Covered Product to another product pursuant to Sections ~~X.3(a)(3), X.3(a)(4), [X.4(a)(3),] X.4(a)(4) or~~ X.6(b), it shall do so using[23]

~~[~~ a method designed to ensure that such content, in any usable form, shall be reasonably secure from being intercepted, redistributed or copied when being so passed to such other product~~]~~. Where a Covered Product passes, or directs to be passed, Unscreened Content or Marked Content to an output pursuant to Sections X.3(a)(3), X.3(a)(4) or X.4(a)(3), it shall do so using

~~[~~a method that ~~…technical criteria to be specified]~~

~~[an Authorized Digital Output Protection Technology or other means that~~ provides technological protection against unauthorized redistribution of such content that is at least as effective as such technological protection provided by any one of the Authorized Digital Output Protection Technologies~~]~~.

X.11 Level of Protection. ~~[Discuss relationship of X.11 to other robustness provisions.]~~ The content protection requirements set forth in the Compliance Requirements and the requirements set forth in Sections X.7(c) and X.8 shall be implemented in a reasonable method so that they:

(a) Cannot be defeated or circumvented ~~[by a User]~~ merely by using general-purpose tools or equipment that are widely available at a reasonable price, such as screwdrivers, jumpers, clips and soldering irons, 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, other than Circumvention Devices; and

(b) Can only with difficulty be defeated or circumvented using professional tools or equipment, such as logic analyzers, chip disassembly systems, or in-circuit emulators or any other tools, equipment, methods, or techniques not described in Section X.11(a) 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.

[*Note to reader: The instrument promulgating the Compliance Requirements and Robustness Requirements could include the "New Circumstances" concepts reflected in Section 3.7 of the DTCP Robustness Rules or Sections 6.2.4.3 and 6.2.5.5 of the CSS Procedural Specifications (addressing new circumstances that may arise which, had they existed at the time of design of a particular Covered Product, would have caused such product to fail to comply with the Robustness Requirements).]*

[23] The drafting committee has been discussing the various alternatives specified but has not reached consensus regarding the adoption of any one of the alternatives.

Table A

[Anticipates list setting forth specific technologies together with any language necessary to invoke such technologies.]

Authorized Digital Output Protection Technologies	Associated Obligations

Authorized Recording Methods	Associated Obligations