DOCKET FILE COPY ORIGINAL

TITAN
BROADCAST COMMUNICATION SYSTEMS

RECEIVED BY
FEB 16 1994
FCC · MAIL ROOM

Federal Communication Commission
1919 N. Street N.W.
Washington, D.C. 20554

Subject: Federal Communication Commission ET Docket No. 93-7

To the Secretary,

Please accept these comments pursuant to the Federal Communications Commission (FCC) Notice of Public Rule Making (NPRM) on compatibility between cable decoders and consumer electronics equipment. Titan looks forward to assisting the FCC in their mission to define compatibility in this crucial area in hopes of establishing a framework for standards-based consumer electronics development in the digital video age.

Respectfully yours,

Charles F. Newby, Director
Broadcast Communications Systems
Titan Information Systems Incorporated

RECEIVED BY
FEB 16 1994
FCC · MAIL ROOM

No. of Copies rec'd 0+10
List ABCDE

DOCKET FILE COPY ORIGINAL

Before the

FEDERAL COMMUNICATIONS COMMISSION

Washington, D.C. 20554

In the Matter of	)	
	)	
Implementation of Section 17 of the Cable Television Consumer Protection and Competition Act of 1992	)	ET Docket No. 93-7
	)	
Compatibility Between Cable Systems and Consumer Electronics Equipment	)	

REPLY COMMENTS OF THE TITAN CORPORATION

RECEIVED BY
FEB 16 1994
FCC - MAIL ROOM

February 16, 1994

The Titan Corporation
3033 Science Park Road
San Diego CA 92121
Telephone (619) 552-9797
Fax (619) 597-9055

RECEIVED BY
FEB 16 1994
FCC - MAIL ROOM

TABLE OF CONTENTS

1 INTRODUCTION.....1

2 REPLY TO THE COMMENTS BEFORE THIS NPRM.....3

2.1 The Standards Setting Plan as Envisioned by the Cable-Consumer Electronics Advisory Group Does Not Address the Fundamental Issues Relating to Equipment Compatibility and Thus Will Not Succeed In Protecting the Public Interest.....3

2.2 The Commission Has Not Only the Authority but the Obligation to Protect the Public By Mandating Standards.....4

2.3 Adoption of a Replaceable Security Interface Standard Will Allow Competition in the Supply of Conditional Access/Encryption Without Any of the Side-effects Claimed By the Cable Industry.....6

3 THE COMMISSION SHOULD CLEARLY UNDERSTAND THE TECHNICAL AND OPERATIONAL ISSUES RELATING TO THE ADOPTION OF A REPLACEABLE SECURITY INTERFACE STANDARD.....9

4 THE COMMISSION SHOULD COMMENCE WITH AN INQUIRY AND RULEMAKING PROCEEDING FOR THE ADOPTION OF A REPLACEABLE SECURITY INTERFACE STANDARD WITHOUT DELAY.....12

5 CONCLUSION.....14

DOCKET FILE COPY ORIGINAL

Before the

FEDERAL COMMUNICATIONS COMMISSION

Washington, D.C. 20554

In the Matter of	)	
	)	
Implementation of Section 17 of the Cable Television Consumer Protection and Competition Act of 1992	)	ET Docket No. 93-7
	)	
Compatibility Between Cable Systems and Consumer Electronics Equipment	)	

REPLY COMMENTS

1 INTRODUCTION

The Titan Corporation ("Titan"), hereby respectfully submits Reply Comments to the Federal Communications Commission's ("Commission") Notice of Proposed Rule Making (NPRM) in the above-captioned proceeding. Titan has a strong interest in the Commission's implementation of the Cable Television Consumer Protection and Competition Act of 1992[1] ("Cable Act") in general and Section 17 in particular, because of its substantial involvement in and familiarity with the development, manufacture, and sale of the conditional access/encryption (scrambling) technologies that are so intertwined with the compatibility issues that the Commission is concerned with in this proceeding.

The Titan Corporation, through its Linkabit Division, was the inventor of the de facto U.S. industry standard conditional access/encryption technology for satellite television known as VideoCipher®[2]. This technology is used today by the cable industry to meet its obligations to the copyright-holder to protect from theft programming that it is transmitted via satellite to the cable headend, but more importantly, it is this very technology that General Instrument Corporation (GIC) is currently using with its DigiCipher™ I digital satellite television transmission system and will certainly use with its DigiCipher II and DigiCable products when they are fielded later this year. It is the fact that the Linkabit Division of Titan invented the VideoCipher conditional access/encryption system and the fact that it owns the patented, unpatented, and copyrighted intellectual property along with the knowledge of specific trade-secrets and know-how that makes these new products possible, that gives Titan the unique ability to comment with authority on

[1] Pub. L. No. 102-385, 102 Stat. 1460 (1992).
[2] VideoCipher, DigiCipher, and DigiCable are trademarks of General Instrument Corporation.

security issues relating to equipment in use and planned for use by the cable television industry.

Titan's recent investment and experience in efforts to introduce competition in the supply of VideoCipher compatible conditional access/encryption equipment for use in the satellite television industry, uniquely qualifies it to provide an important perspective on the rules proposed by the Commission.

Titan has recently formed a new corporation called Titan Information Systems Corporation, that will, taking advantage of its unique technology position, play an increasingly important role in the development and supply of conditional access/encryption equipment for satellite, cable, multi-point microwave, and cellular television systems used in this country and worldwide. As it will be explained below, through this new corporation Titan offers the Commission sound technical and market-driven solutions to the problems relating to the incompatibility of cable and consumer electronic equipment which will allow, to the extent required, the synchronization of the product development cycles of these two industries.

Finally, Titan certainly applauds the efforts of the cable and the consumer electronics industries but it is clear from the Comments submitted by the Cable-Consumer Electronics Compatibility Advisory Group ("C3AG") that the standards setting process started by this group is not moving forward quickly enough. It is clear that the cable and the consumer electronics industries each recognize the need to establish some form of standards but it is also clear from the Comments that the approach preferred by each of these industries is very different. This outcome was quite predictable given the narrow focus that the Commission gave the NPRM. Titan understands the rationale that the Commission used when developing the rules[3] that it proposes in order to achieve the compatibility goals sought by Congress when it enacted Section 17 of the Cable Act. After replying to the Comments submitted to the Commission in this proceeding, Titan will present a solution to the equipment compatibility problems that not only satisfies the intent of Congress, but also allows the Commission to discharge its duty to protect the public from the future equipment incompatibilities that will most certainly be created if the cable industry equipment suppliers are permitted to promulgate their proprietary conditional access/encryption systems into the National Information Infrastructure (NII).

[3] "Report To Congress On Means Of Assuring Compatibility Between Cable Systems and Consumer Electronics Equipment", adopted October 5, 1993.

2 REPLY TO THE COMMENTS BEFORE THIS NPRM

It is clear from the Comments submitted in this NPRM that there are deep divisions between the cable equipment and consumer electronics industries. Of course both of these industries are vitally important to the current and future economic health of the country. Through the significant investments by corporations in both industries, the U.S. enjoys a commanding lead in many of the key technologies relating to the transmission of television signals by digital means. In addition, the convergence of technologies from these and other industries, the U.S. will in the near future begin to reap the benefits of competition in the a broad array of information delivery services. For the first time the integration of: television, audio, telephone, fax, data, and new information services not even thought of yet, will be both technically and economically feasible. Today several important industries stand together at the crossroads of this new era in information delivery services -- sound public policy requires that careful consideration be given to all aspects of these newly emerging technologies and services. Fortunately, through the efforts of enlightened leaders in the consumer electronics, cable, computer, and telephone industries, public policy makers are beginning to heed the call for interopertability and compatibility. U.S. Representative Edward Markey put the situation very well at a recent hearing of the House Telecommunications and Finance Subcommittee when he described the set-top converter as "the consumer's on-ramp to the information superhighway" and then warned that it should not become "a roadblock."[4] It is with these considerations in mind that Titan replies to the Comments before the Commision in this NPRM.

2.1 The Standards Setting Plan as Envisioned by the Cable-Consumer Electronics Advisory Group Does Not Address the Fundamental Issues Relating to Equipment Compatibility and Thus Will Not Succeed In Protecting the Public Interest

While the work of the C3AG is quite laudatory, the standards setting plan as envisioned by it does not address many of the fundamental requirements of a viable solution to the problems of compatibility. As described in the Decoder Interface Subcommittee's "Interim Report" issued January 20, 1994, the Interim Standard (IS-105), is very complex in its present form yet does not even begin to satisfy the requirements for digital interactive services. It should be clear to anyone skilled in communication systems engineering, that the proposed standard will add significantly to the cost of both cable and consumer electronics equipment even before it begins to address the requirements of newly emerging information services.[5]

---

[4] See "Markey Pushes for Interoperability" by Vincente Pasdeloup, Cable World, February 7, 1994, page 10.

[5] Contrary to a suggestion by a party to this proceeding, for the digital modulation schemes contemplated by all digital transmission proposals, a video baseband interface cannot be used.

Specifically, the proposed standard does not specify the following important interface requirements: the AGC requirements of the IF and baseband signals, the AFC requirements of the IF and baseband signals, the requirements for the control signals, the requirements for the interface protocol, video Y/C signal specifications, audio signal specifications, and the audio signal processing requirements, to name just the most important requirements. And importantly the proposed standard does not allow the cable television decoder function to be built into the consumer electronics equipment if the consumer electronics equipment manufacturer finds a reason to do so.

Additionally, the schedule that the C3AG hopes to adhere to is hopelessly unrealistic. The Interim Report predicts that a Decoder Interface Standard will be in place by Spring of 1995. It is much more realistic to assume, and experience shows, that a standards setting process as complicated as this one will be, will take at least four years and probably longer.

Therefore, since the proposed Decoder Interface will be expensive, cumbersome, late, and will not solve the fundamental causes for the equipment incompatibility problems that consumers face today, it will not succeed. Even though the Commission is obligated to implement the legislative intent of Congress, it cannot ignore the serious flaws in the standard setting process that it has began. Fortunately, Titan will describe an alternative standards approach that addresses the problems of compatibility in a most cost-effective and timely fashion.

2.2 The Commission Has Not Only the Authority But the Obligation to Protect the Public By Mandating Standards

Some of the Comments now before the Commission in this NPRM assert that the Commission has no legal authority to require the adoption of a Decoder Interface Standard by arguing that the adoption of such a standard would amount to "the imposition of a technological moratorium on emerging cable services and technologies... [that is] ...beyond the Commission's authority...".[6] The nation's largest MSO comments that, "While the adoption of such standards may ultimately prove to be worthwhile, TCI notes that the imposition of standards by the Commission would be contrary to congressional intent."[7]

Home Box Office asserts that "...whatever standardization process proves necessary for widespread deployment of digital transmission systems will be accomplished most efficiently through normal marketplace evolution."[8] Home Box Office, as an early adopter of digital transmission, also asserts that "The development of the MPEG-2 standard has been done in the marketplace without government regulation. HBO believes that market forces will create widespread utilization of the MPEG-2 standard."[9]

---

[6] See the NPRM Comments of General Instrument Corporation at page 20.
[7] See the NPRM Comments of Tele-Communications, Inc. at page 31.
[8] See the NPRM Comments of Home Box Office at page 3.
[9] See the NPRM Comments of Home Box Office at page 4.

The argument that it was not the intent of Congress that a Decoder Interface Standard be mandated by the Commission, uses the give-and-take of the legislative process to support a legal theory that is irrelevant. Congress has spoken through the law and the law is quite clear in the requirement that cable and consumer electronics equipment incompatibilities must be eliminated.

Additionally, participants in this NPRM must realize that the adoption of a standard is not the same as the imposition of a standard. The standardization process by its very nature cannot be forced. As Home Box Office notes, the standardization process can work well when conditions are right and cites the MPEG standards setting process as an example of the marketplace at work.

However, arguments that urge the Commission to let the natural forces of the marketplace set the standards, ignore the several important factors, the most important of which, is that there is no open "marketplace" when it comes to the development and procurement of cable television equipment. There is no vigorous competition among cable equipment suppliers -- equipment development and purchasing decisions are controlled by a few powerful MSOs who favor inside suppliers such as Jerrold (GIC) and Scientific-Atlanta to the exclusion on all others even when those suppliers' equipment provides more features at a lower cost.

Furthermore, Home Box Office's use of the assertion that equipment complying with the MPEG-2 standard will be widely adopted by the cable industry, in an attempt to convince the Commmission that the marketplace is at work in the cable industry, is misleading. Home Box Office and all other cable MSO's transmitting digital signals (with the exception of Viacom) have adopted GIC's DigiCipher I system for the transmission of their digital television feeds. DigiCipher I is not MPEG compatible but the statement is frequently made that it will be replaced with DigiCipher II equipment that is MPEG-2 compatible as soon as that equipment is available. Cable industry executives point to this commitment by the MSOs to show that the marketplace is working to evolve digital television standards. The fact is, it does not matter what compression technology is used by the system(s) that the cable industry uses, as long as the conditional access/encryption system that is used by the equipment is proprietary, the equipment suppliers favored by the cable industry (in this case GIC) will have a monopoly on the supply of these critical information delivery system components.

In fact, the situation that will result if the Commission fails to eliminate these equipment supply monopolies through the adoption of a conditional access/encryption standard, will be far more serious. If the Commission fails to act, GIC will be poised, using the proprietary position of the DigiCipher conditional access/encryption system, to extend its de facto monopoly of video transmission equipment from the 100 plus satellite systems now using VideoCipher equipment to the home through the use of the "pass-through" of Access Control Messages originating at a National Authorization Center that it controls.[10] By urging the Commission to let the marketplace

[10] Viacom in is anti-trust law suit against Tele-Communications Inc. described the situation in that "Defendant TCI, through the above-described conduct, has conspired and combined with GI in a plan, common design and understanding with the specific intent, to eliminate competitors and

work, the cable industry hopes to delay the adoption of a comprehensive standard that includes conditional access/encryption until it has a de facto standard, that is its DigiCipher system, and with it a continuing monopoly on the supply of cable television equipment and a new monopoly on the critical components required to build compatible consumer electronics equipment -- these are the proprietary integrated circuits and Smart Cards that must be purchased from GIC in order to decompress and decrypt the DigiCipher digital video datastream (be it MPEG-2 compatible or not). GIC has maintained for many months that it will freely license this technology on a fair basis. But those companies who have inquired as to the licensing fees, and we have, do not see GIC's fees and other terms and conditions as fair, and know that, if we were to become a DigiCipher licensee, we would always be at an economic disadvantage vs GIC and that GIC would, as a supplier of this critical technology, always have control of our businesses. Fortunately, the stakeholders in this process have began urging Congress to act in order to foreclose the continuing development of this situation.

We therefore urge the Commission to immediately begin the process that will set standards governing the transmission and compression of digital television information and include in the process the requirement for a standard conditional access/encryption interface. The cable industry has shown that it will not release its grip upon this critical conditional access/encryption technology, therefore the Commission must act for the Public and mandate an interoperable, open-systems architecture through the adoption of a Replaceable Security Interface Standard.

2.3 Adoption of a Replaceable Security Interface Standard Will Allow Competition in the Supply of Conditional Access/Encryption Without Any of the Side-effects Claimed By the Cable Industry

The feasibility of an open-architecture, interoperable, Replaceable Security Interface standard is a critical issue that must be examined thoroughly by the Commission. GIC states that it is "...particularly troubled by ¶ 34's reference to the adoption of a standard security system."[11], and also, "... a national scrambling/encryption standard would provide signal pirates with increased incentives to defeat the standard, since compromise of the standard would provide access to all cable programming nationally. Thus, national security standards in the cable industry could seriously undermine the ability of cable operators to protect their signals. By contrast, in a world of multiple scrambling/encryption techniques, if a signal pirate's efforts are "rewarded" by access to limited amounts of programming, incentives are significantly reduced to engage in the endeavor in the first place."[12]

---

monopolize the market for encryption systems in the United States." See, Viacom International Inc. vs Tele-Communications Inc., et. al., pages 51,52. And also, "The conduct of defendant TCI constitutes a contract, combination, or conspiracy with GI in unreasonable restraint of trade in the national market for digital compression systems...". See, same, pages 52,53.

[11] See the NPRM Comments of General Instrument Corporation at page 36.

[12] See the NPRM Comments of General Instrument Corporation at pages 36,37.

GIC's is correct -- there should not be *a national security standard*, however, there should be a *National Replaceable Security Interface Standard.* Such an interface will use a standard keystream interface giving a *common, standard access point* for multiple conditional access/encryption systems that each will employ proprietary security techniques for the generation, management, and delivery of the keys that are used to encrypt the secret portions of the Program Entitlement and various (User Identification, Program Cost, Viewing Time, etc.) Authentication Messages. Thus, as we have explained in previous comments in this NPRM, the security of systems that utilize this approach will be enhanced over time with the introduction of comptetion. Indeed, using a standard keystream interface will allow the cable operator more options if the security system used on his systems is pirated. It would be the security system supplier, not the pirate, who would be incentivized in this case because the cable equipment supplier would know that the cable operator can buy an interoperable conditional access/encryption system from his competitor.

GIC also states that, "A national video security standard would have a similarly deleterious impact on subscriber privacy. The emerging infomation superhighway will transmit sensitive personal data -- such as banking transactions, health records, a consumer's viewing habits and buying predilections, etc. -- the confidentiality of which subscribers will want to preserve. In such an environment, the publication of a national video security standard would increase not only the ease with which programmers' intellectual property rights are transgressed but also the facility with which subscriber privacy is invaded."[13]

Here again, GIC's comments are off the point, and there is no danger to personal privacy since the public, through the cable operator or other information superhighway provider, would have a choice of security systems. If, as is the case with most cable systems in operation today, a system's security becomes compromised in some way, the American consumer could demand, and the information provider could readily supply, a replacement security system by mailing the consumer a new Smart Card.

GIC further states, "...while the Commission has studied the question of the standardization of video scrambling/encryption on a number of occasions, in each instance it has found that imposition of such a standard would be contrary to the public interest. Moreover, in deleting the House Amendment's directive to consider the "cost and benefits of requiring cable operators to adhere to technical standards for scrambling or encryption of video programming," the Conference Committee clearly conveyed Congress' decision to avoid the imposition of such universal security standards on the cable industry".[14]

As the Commission knows, the Commission did not mandate a national security standard, not simply because it was not feasible, but because, among other considerations, GIC already had achieved a monopoly in the conditional access/encryption system used in the delivery of

---

[13] See the NPRM Comments of General Instrument Corporation at page 37.
[14] See the NPRM Comments of General Instrument Corporation at pages 37,38.

programming via satellite (VideoCipher) and that to mandate anything at all would have meant disenfranchising millions of American consumers. The Titan Corporation was a party to a challenge of GIC's monopoly of the supply of satellite conditional access/encryption equipment and was not successful, not because of the lack of a sound technical and legal basis for the introduction of its equipment into the marketplace, but because the cable industry, who are the first users of conditional access/encryption technology, wished to maintain its monopoly of, through its favored equipment supplier, the supply of cable television equipment.

Additionally, GIC argues that, "...building the descrambling/decoding circuits into TV sets is too dangerous because it gives pirates single a technological design target to attack. Congress implicitly conveyed its recognition of this danger by deleting, in conference, a House amendment provision that would have required the Commission to consider "the potential for achieving economies of scale by requiring manufacturers of television receivers to incorporate technologies to achieve such compatibility in all television receivers." Moreover, as the Commission is well aware, existence of a single security target in the home satellite industry, i.e., VideoCipher II, contributed to its compromise.

Accordingly, if security standards are ultimately implemented, both the descrambling/decoding and the entitlement functions should be handled in a device external to the TV. Under this approach, the Decoder Interface would pass scrambled/encrypted programming out to this device and descrambled/decoded programming back in. Separating all security elements from the consumer electronics has significant benefits in the event the security is breached and must be replaced. By keeping the security system separate, the cable operator can replace/upgrade security without requiring replacement of the consumer electronics hardware by the consumer."[15]

GIC's argument that the descrambling/decoding must always be performed external to the consumer electronics equipment, is based upon the false construction that descrambling and decoding are equivalent and that they are both equivalent to security. The facts are that, descrambling, as in the descrambling of an analog signal scrambled using video inversion and synchronization pulse denial, is not equivalent to decoding, as in the decoding of an MPEG datastream. More properly, we define scrambling/descrambling to be invertible analog processess and encryption/decryption to be invertible digital processess. Furthermore we assert that, the final step in the descrambling or decryption process may indeed be performed in the consumer electronics equipment with no impact upon the security of the system. In addition the decoding, as in the decompression of an MPEG datastream, are functions that should be allowed to move to the consumer electronics equipment. The cost savings due to the economies of scale that would be realized by taking the open-architectural approach just described would be enormous. With this approach companies such as C-Cube Microsystems, AT&T Microelectronics, Toshiba, etc., will be able to produce the silicon required to do the video and audio decompression of a MPEG

---

[15] See the NPRM Comments of General Instrument Corporation at pages 38,39.

datastream and integrate this function with unique value-added functions such the graphical user interface that will allow the consumer to navigate the vast information superhighway. Consumer electronics manufacturers such as Zenith, Phillips, Sony, etc., would be allowed to build systems that integrate these systems on silicon in entirely new ways in response to consumer demand and the competitive process.

Finally, GIC's argument that the use of a single security element would be unwise citing the rampant piracy of the VideoCipher II system as evidence to support this theory makes no sense whatever. The VideoCipher II system was widely pirated because of the lack physical security of the "secure microprocessor" that was used in its design and had nothing to do with being a single point of attack. All security systems are by definition "a single point of attack" and unless the system is designed to allow a flexible response to pirate attack, it will be extremely vulnerable. Titan is expert in the design of such flexible security systems and urges the Commission to consider the benefits of a system that, instead of the IF decoder interface, uses a low-speed keystream interface from the security Access Control Unit (typically a Smart Card) to the Video Decoder (Decompressor) in one direction and a low-speed serial interface for the flow of Access Control Messages in the other direction. This interface is simple and low-cost but does not subtract from the security of the system -- the security of the system rests upon the cryptographic design of the Access Control Message structures, the cryptographic strength of the keystream generator, and the physical security of the Smart Card. If any of these elements is found to be weak, the system can be repaired quickly by fielding a new Smart Card that repairs the weak element(s).

3 THE COMMISSION SHOULD CLEARLY UNDERSTAND THE TECHNICAL AND OPERATIONAL ISSUES RELATING TO THE ADOPTION OF A REPLACEABLE SECURITY INTERFACE STANDARD

We recommend that the Commission immediately prescribe standards governing transmission and compression and a "standard conditional access/encryption interface" that we will call the Replaceable Security Interface. Such standards should be based upon the configurations shown in Figure 1 (c) and (d). It is expected that time will ultimately lead to the dominance of configuration Figure 1(c). This interface is defined as a "keystream interface", since it provides a simple division between decoding hardware and the conditional access/encryption hardware. The advantages of the keystream interface over other signal interfaces such as IF or baseband interfaces are as follows:

- Expanding the scope of the hardware that becomes subject to competitive supply. This allows *unbundling* of reception-demodulation-decoding hardware from access control hardware.
- *Minimizing the redundancy* of costly subsystems such as demodulators, decoders and decompressors. These systems' costs may reach several hundred dollars at the retail level.

- Provide higher level of *security*, flexibility and deterrence to pirates. The operator's ability to replace low cost security modules removes the economic incentive for pirate R&D investments in security breaches.
- Allows *sharing* of most functions required for Advanced Television reception with those of digital 525 line systems.
- Unlike other interfaces, keystream interfaces can be easily expanded for the supply of *two* keystream signals for the *simultaneous decoding* of two channels for Picture-In-Picture ("PIP") or other advanced display functions. With one Access Control Unit providing dual keystream, this option will not require the provision of *two* decoders of the type shown in Figure 1(b) in every set or VCR designed with PIP features and the costly doubling of interface circuitry and sockets.[16]
- Allows multiple vendors for conditiona access/encryption systems.

Because the Access Control Unit interface information containing the interface protocol for the Access Control Messages (but not the meaning of the Access Control Messaages) and the Keystream signal interface specifications is a public standard, various vendors of conditional access/encryption systems can compete on the supply of such technology. These vendors may differ in their approach for supporting headend services and billing interface capabilities as well as the implementation strengths of their security modules. It is important to recognize that a breach of security in one vendor's Access Control Units, does not impact the security of the installed decoder base. Rather, the Access Control Units (smart cards or security modules) can be replaced either with new improved units from the same vendor or from a competing vendor. Hence, the threshold for the displacement of conditional access/encryption vendor's technology is much lower in configurations of Figures 1(c) and (d) than that of Figure 1(b). This competitive tension should be a welcome development as it leads to reduced costs and improved security performance by conditiona access/encryption vendors.[17]

Another significant factor that should be kept in mind regarding conditional access/encryption interface standardization is the fact that topologies of cable systems are evolving and that several architectures involving multiple program origination sources (possibly controlled by different entities) may well be applied. These distinct program encoding sources may require the control of program access for the same subscriber equipment. Thus, the standardization of the

---

[16] In digital TV applications, it may be possible to provide a PIP function without additional tuner by utilizing the channel multiplex and decompression capability within one carrier. Since only an infrequent still frame sample may be require in the PIP insert, sufficient buffering would allow both pictures to be processed and additional memory would be the only incremental costs for such "intracarrier" PIP modes.

[17] The suggestion that competitive access control suppliers might respond more rapidly to security breaches is offered by two other parties in connection with the satellite encryption proceeding. See In the Matter of Inquiry into Encryption Technology for Satellite Cable Programming, PP Docket No. 92-234; PrimeTime Comments at 4; Scientific-Atlanta Comments at 12-15.

conditional access/encryption interface as well as the transmission and compression standards will help guarantee the smooth transition from the architectures of Figure 2(a) to the type shown in Figure 2(b).

Let us review the operation of the operation of the Access Control Unit as shown in Figure 1 (c). The Access Control Unit within the decoder module receives from the demodulator the Access Control Messages. Those messages in turn are decrypted using the (unit specific and unique) secret information that is securely embedded within a secure enclosure, in order to produce the correct keystream for authorized *decoding* of the program. It should be clear that the Access Control Messages emanating from the demodulator contain *no useful information to would be pirates,* as these messages are encrypted under a key which resides or is produced within the Secret Information sector of the Access Control Unit. Moreover, the keystream signal supplied from the Access Control Unit is *equally useless to would be pirates*, as it contains rapidly changing *unpredictable* key signals that continuously become obsolete every small fraction of a second.[18] Thus, no unauthorized physical access, tampering or otherwise modifying of the demodulator-decoder and decompression unit (which contains a keystream controlled decoder) or the interfaces thereto, can result in any security compromise of the system. Such a breach of decoder security can only come from the compromise of the secure content or workings of the Access Control Unit. Thus, from the standpoint of security, in a properly designed system, one must make a distinction between the **decoding** functions (that are responsive to a *non-secure* decryption keystream) that may be performed in a *non-secure* demodulator-decoder-decompression unit and a **cryptographic** function (responsive to *secure* secret information which changes *very infrequently*) performed in a *secure* unit. The workings and operation of the demodulator, decoder (including its response to the keystream) and decompressor can be published, standardized and be supplied subject to genuine market competition.

Based on the above discussion, it should be clear that in new systems, there is no *security* reason for the functions of demodulation, decoding and decompression to be duplicated within the decoder and the consumer electronics appliance, just as there are no reasons that the tuner/converter functions be duplicated. Hence, the architecture of Figure 1(c) clearly emerges as optimal *from the subscriber's point of view*. Here, the Replaceable Security Interface is simply a keystream interface with an Access Control Unit that performs only the cryptographic functions in a secure enclosure such as a secure chip within a smart card or a Renewable Security module.[19] This

---

[18] Even if a pirate who electronically observes the rapidly changing keystream attempts to distribute it to others, he will require a clandestine real-time communication network to all other pirate locations. However, this approach will be unworkable for any practical application involving realistic distances due to propagation delays.

[19] We note that the economics and security advantages of such an approach have been recently utilized in the VideoCipher access control system used on C-band. The system has been recently converted to employ a Renewable Security Unit within the decoder module in order to predominantly perform cryptographic functions requiring security. See "Showtime Sets Commercial Upgrade" by Tom Middleton, Satellite Business News, Mar. 24, 1993, pp. 1, 22.

interface approach for pay television has been successfully deployed for some 3.5 million subscribers of British Sky Broadcasting ("Sky") service in Europe[20] and is scheduled to be introduced in the U.S. on DirecTv's DBS system.[21] The ability to combine an Access Control *decoding* function within consumer electronics equipment without compromising the security of the *cryptographic* system is evidenced by the fact that such TV sets, VCR's and stand-alone decoders from competing vendors with smart card interfaces have been produced and made available to Sky subscribers in Europe.

4 THE COMMISSION SHOULD COMMENCE WITH AN INQUIRY AND RULEMAKING PROCEEDING FOR THE ADOPTION OF A REPLACEABLE SECURITY INTERFACE STANDARD WITHOUT DELAY

The record in this proceeding is replete with explanations and historical accounts of the reasons for the present situation of access control equipment incompatibilities with consumer electronics. Titan believes that a significant contributor to the current situation is the long history of bundling the access control equipment supply with cable services. We submit that decoder interfaces that allow the furtherance of such bundling by the nature of the proprietary systems they require would be against the public interest. If security and cost considerations are satisfied, the public interest requires that factors relating to subscriber interests should weigh more heavily than the fact that there might be an accord between the cable and consumer electronics industries who both benefit from selling more costly hardware by agreeing on a compromise of configurations such as that of Figure 1(b).

There is strong evidence on record in this proceeding to support Titan's recommendations. Circuit City recognizes that if the Decoder Interface, as presently constituted is adopted, the cable industry, through the equipment that the local cable company provides, "...will be granted a monopoly on providing both the service and the consumer electronics. If every information and media distributor is encouraged to furnish unique hardware that is non-standard and not competitively available, the National Information Infrastructure ("NII") cannot be achieved."[22] Circuit City recognizes that, "What is at stake for consumer electronics retailers is nothing other than survival. As consumer electronics product categories converge, the functions of many or most may be folded into an all-important "set-top" interface. As decoder interface TVs and VCRs appear, and cable operators are required to provide descrambler/decoder modules, they may (despite the rate disincentive) seek to extend their monopoly of the "set-top" market by building as many functions and features as possible into these decoder/descrambler devices. Rather than set a

---

[20] See Comments and Reply Comments of News Datacom, In the Matter of Inquiry into Encryption Technology for Satellite Cable Programming, PP Docket No. 92-234, December 24, 1992; January 26, 1993.

[21] See Comments of DirecTV, Inc., In the Matter of Inquiry into Encryption Technology for Satellite Cable Programming, PP Docket No. 92-234, December 24, 1992.

[22] See the NPRM Comments of Circuit City Stores Inc. at page 3.

bad precedent and risk failure through indirection, the Commission should take clear, affirmative action to limit potential monopolies over both set-top and decoder/descrambler devices."[23]

Similarly, Mitsubishi Electronics America Inc. recognizes the serious implications of adopting a Decoder Interface Standard that does not eliminate proprietary cable industry conditional access/encryption systems when it states, "Despite the progress represented by the decoder interface, this standard is not sufficient to assure that cable operators will encourage movement from set-top to decoder interface connections, or that their "security" hardware supplied through the decoder interface will allow real competition in offering product features to consumers. Unless the Commission goes further now, program distributors will retain powerful incentives and means to keep features, and hardware, proprietary, nonstandard, and noncompatible."[24]

The Hewlett-Packard Company recognizes some of the serious problems that will arise unless the Commission takes a more comprehensive approach to the standards setting process began by this NPRM. The Hewlett-Packard Company points out that, "Going forward, cable systems will continue an evolutionary process. One such process is toward multiple program origination sources. There is no assurance that all programs will use the same encipherment process and cryptographic key information. There exists the undesired possibility of multiple decoders to receive programs from multiple origination sources. For digital systems the decoder interface is an incomplete solution and furthermore the compatibility problem may be compounded by future delivery systems."[25] The Hewlett-Packard Company goes on to say, that it "...believes the following principles are applicable to Digital video systems:

3.1 Adequate security can be achieved with a Digital video system which incorporates standard interfaces.

3.2 Adequate security can be achieved with a Digital video system which separates decipherment and access control functionality by standard interfaces.

3.3 Separation of decipherment and access control functionality is desirable in early development of Digital video systems. Such separation allows the most timely response and deployment of evolving technology advances."[26]

News Datacom is a company that has significant expertise in the supply of conditional access/encryption systems, they comment for this proceeding, "The conditional access portion of the cable system should be regarded as a detachable and replaceable subsystem capable of descrambling various types of scrambling techniques. Conditional access technology can be incorporated into a stand-along converter or directly into consumer electronics equipment, as the market dictates. Such flexibility will serve to preserve and even enhance the features and functions contained in consumer electronics equipment now and in the future. Moreover, this severablility

---

[23] See the NPRM Comments of Circuit City Stores Inc. at page 8.
[24] See the NPRM Comments of Mitsubishi Electronics America Inc. at page 7.
[25] See the NPRM Comments of the Hewlett-Packard Company at page 3.
[26] See the NPRM Comments of the Hewlett-Packard Company at page 4.

ensures that compatibility can be mandated and signal security preserved without interference to present or future functions of television receiver or VCRs. Descrambling hardware, if licensed in an open architecture, will quickly respond to market demands, and compatibility issues will diminish over time if conditional access is supported in a renewable and replaceable manner."[27] We could not have said it better ourselves.

Furthermore, there is a clear trend toward replaceable security as an cost-effective means of combating piracy. Attachment A shows only a few of the many fully developed conditional access/encryption products that are in use around the world today. The three we cite here are: 1) Scientific-Atlanta (cable set-top decoder), 2) Thomson Consumer Electronics/News Datacom (DirecTv receiver decoder), and General Instrument Corporation (VideoCipher II Plus RS descrambler module). All of these security products use either Smart Cards or Security Modules as replaceable security elements (GIC's VideoCipher II Plus RS system uses a replaceable module as well as a replaceable Smart Card as its replaceable security elements).

Finally, Attachment B is a fax of the progress report of the National Replaceable Security Subcommittee of the JEC. Importantly, the report states that, "On January 11, [1994] the NRSS co-chairmen presented the new concept of a Conditional Access Card. This card can provide security for digital consumer electronics. This card isolates all the security elements into one removable medium, is inexpensive, and uses an existing form factor. It will allow all types of digital consumer electronics to be developed independent of the conditional access system. This card meets all of the system attributes required by the committee. The committee is drafting a straw man specification which will be ready by March 8[, 1994]. The target date to complete this specification is April 15, 1994."[28] We point out that this Smart Card approach can be applied to *any analog scrambling system* with equal success.

5 CONCLUSION

For the foregoing reasons, Titan respectfully recommends that the Commission adopt rules consistent with the Comments herein in order to assure the expansion of competitive forces into the conditional access/encryption market sector and in order to assure compatibility between cable systems and consumer electronics equipment.

---

[27] See the NPRM Comments of the News Datacom at page 5.
[28] See NRSS Progress Report, January 19, 1994, attached.

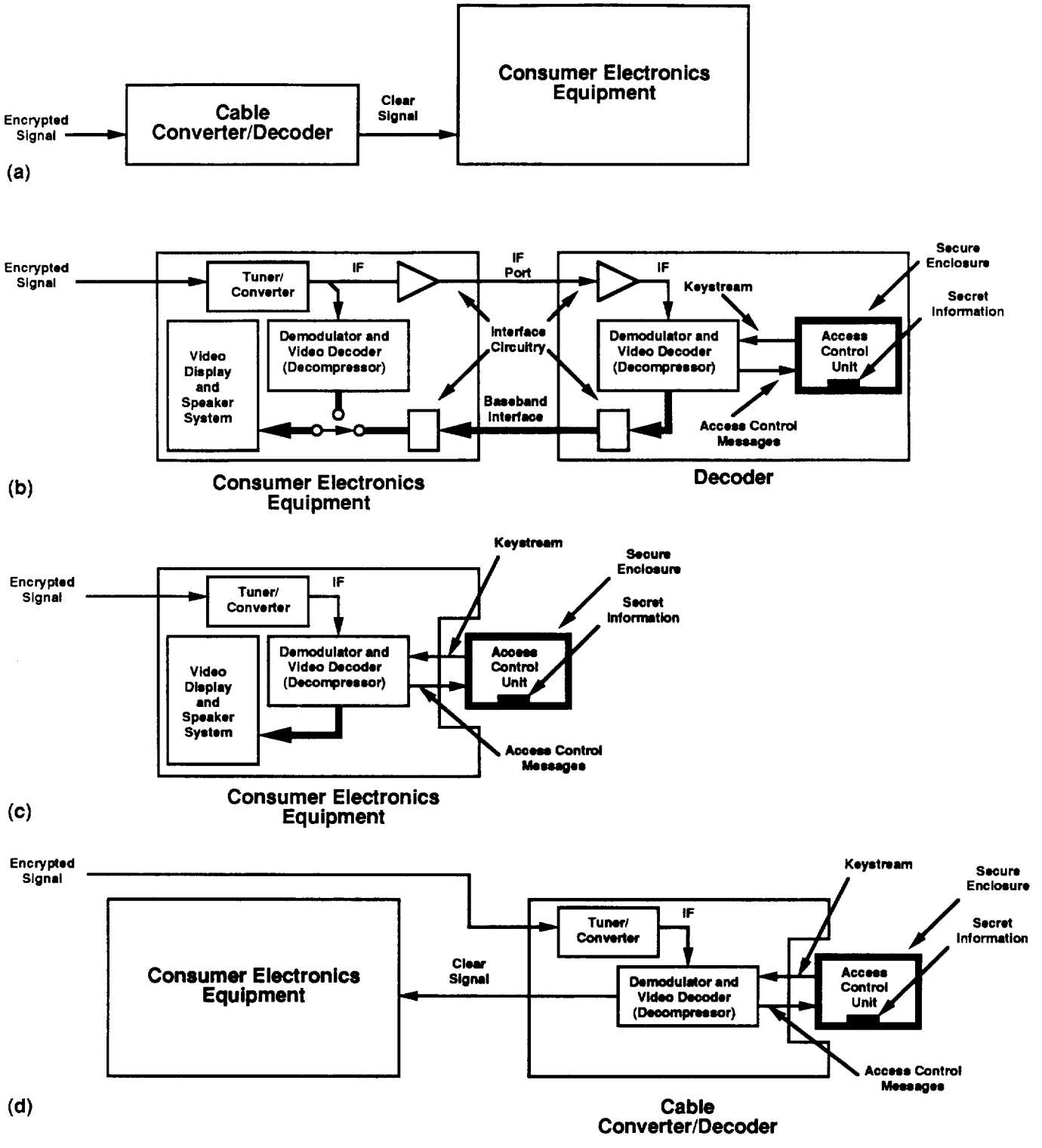
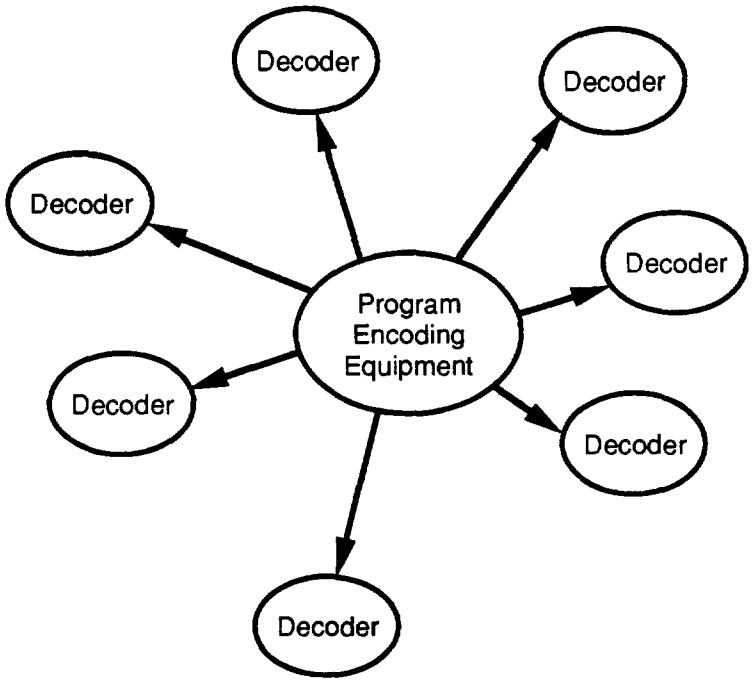
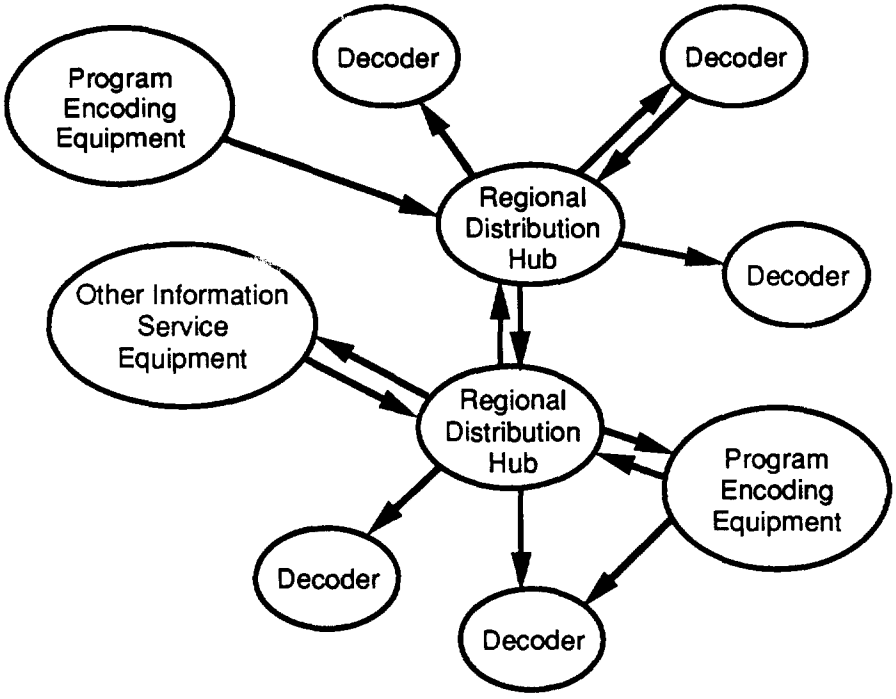

Encrypted Signal
Cable Converter/Decoder
Clear Signal
Consumer Electronics Equipment
(a)
Encrypted Signal
Tuner/ Converter
IF
IF Port
IF
Keystream
Secure Enclosure
Secret Information
Video Display and Speaker System
Demodulator and Video Decoder (Decompressor)
Interface Circuitry
Demodulator and Video Decoder (Decompressor)
Access Control Unit
Baseband Interface
Access Control Messages
(b)
Consumer Electronics Equipment
Decoder
Encrypted Signal
Tuner/ Converter
IF
Keystream
Secure Enclosure
Secret Information
Video Display and Speaker System
Demodulator and Video Decoder (Decompressor)
Access Control Unit
Access Control Messages
(c)
Consumer Electronics Equipment
Encrypted Signal
Consumer Electronics Equipment
Clear Signal
Tuner/ Converter
IF
Keystream
Secure Enclosure
Secret Information
Demodulator and Video Decoder (Decompressor)
Access Control Unit
Access Control Messages
(d)
Cable Converter/Decoder

Figure 1


Decoder
Decoder
Decoder
Decoder
Program
Encoding
Equipment
Decoder
Decoder
Decoder

(a)


Program
Encoding
Equipment
Decoder
Decoder
Regional
Distribution
Hub
Decoder
Other Information
Service
Equipment
Regional
Distribution
Hub
Program
Encoding
Equipment
Decoder
Decoder

(b)

Figure 2

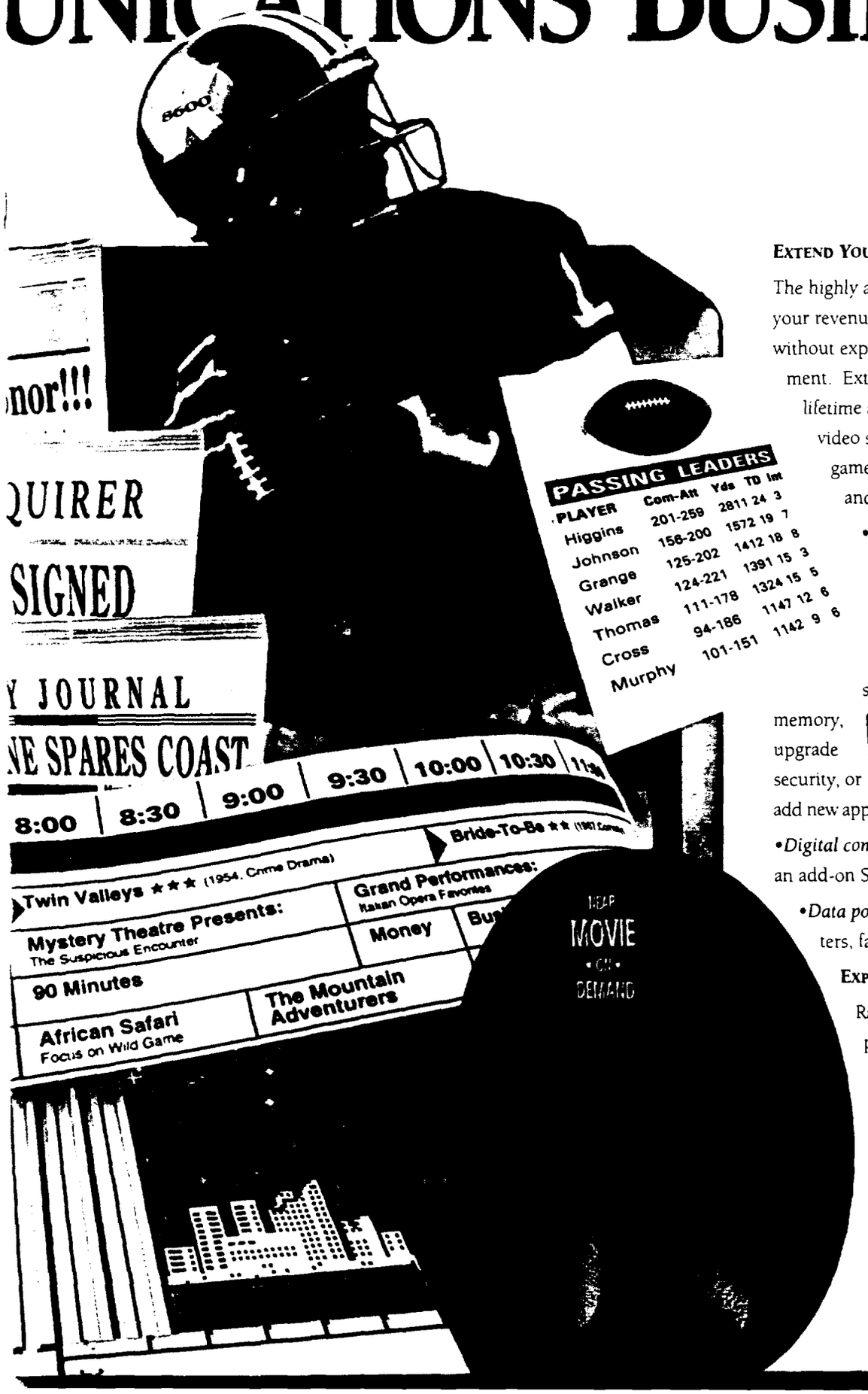
Attachment A

1. Sales brochure from Scientific-Atlanta, Summer 1993.

2. Sales brochure from DirecTv, Summer 1993.

3. Advertisement by Showtime Satellite Networks in Satellite Business News, January 13, 1993, page 2.

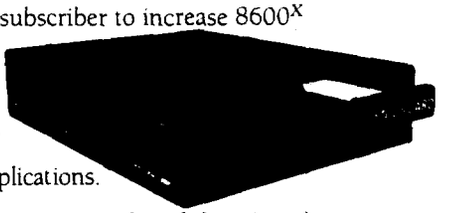
UNICATIONS BUSINESS.



EXTEND YOUR POTENTIAL TOMORROW

The highly adaptable 8600^X is ready to raise your revenues to the "X" power...upgradable without expensive truck rolls or new equipment. Extend your equipment investment lifetime and add virtually any electronic or video service imaginable, such as video games, catalog services, travel services and multimedia applications via:

- *Downloadable software.* Addressably change screens, add features and upgrade security.
- *A slide-in Genius Card.*™ Mail a Genius Card to the subscriber to increase 8600^X memory, upgrade security, or add new applications.



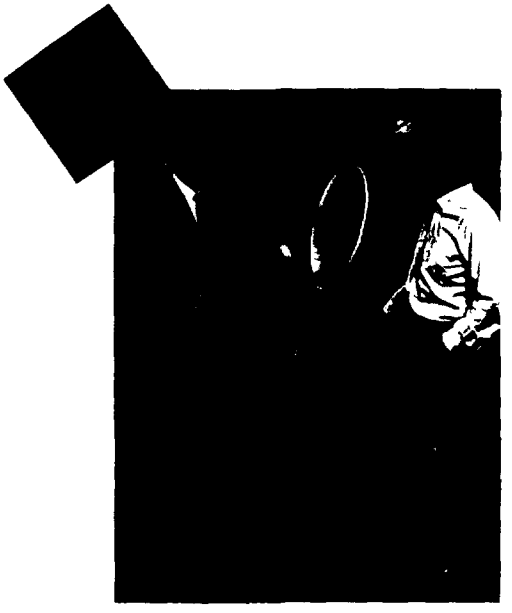
- *Digital compression adaptability.* Simply use an add-on Scientific-Atlanta decompressor.
- *Data port availability.* Connect computers, fax machines, and other devices.

EXPERIENCE THE 8600^X

Raise your operation to the "X" power. Call 800-722-2009 or your Scientific-Atlanta representative. And get into the home communications business today.

Scientific Atlanta

of the Art



operate 27 of the 32 licensed DBS frequencies at this central orbit location. Employing circular polarization, the satellites will provide coverage over the contiguous United States and Canada.

DSS™ (Digital Satellite System)

The home receiving system will be manufactured and distributed by Thomson Consumer Electronics under the RCA brand name. DSS™ is a three component satellite receiving system consisting of an 18-inch satellite dish, an addressable digital receiver/decoder and a remote control unit. DSS will retail for less than $700 through satellite system dealers and consumer electronics retail outlets. The lightweight satellite antenna can be conveniently installed at a variety of exterior home locations, including a windowsill, roof line or porch railing.

Digital Compression

The satellite transmission system will employ the MPEG-2 standard for digital compression technology, provided by Thomson Consumer Electronics, to transmit multiple high-quality video and CD-quality audio channels through each satellite transponder. Compression ratios range from four-to-one for live video to eight-to-one for film.

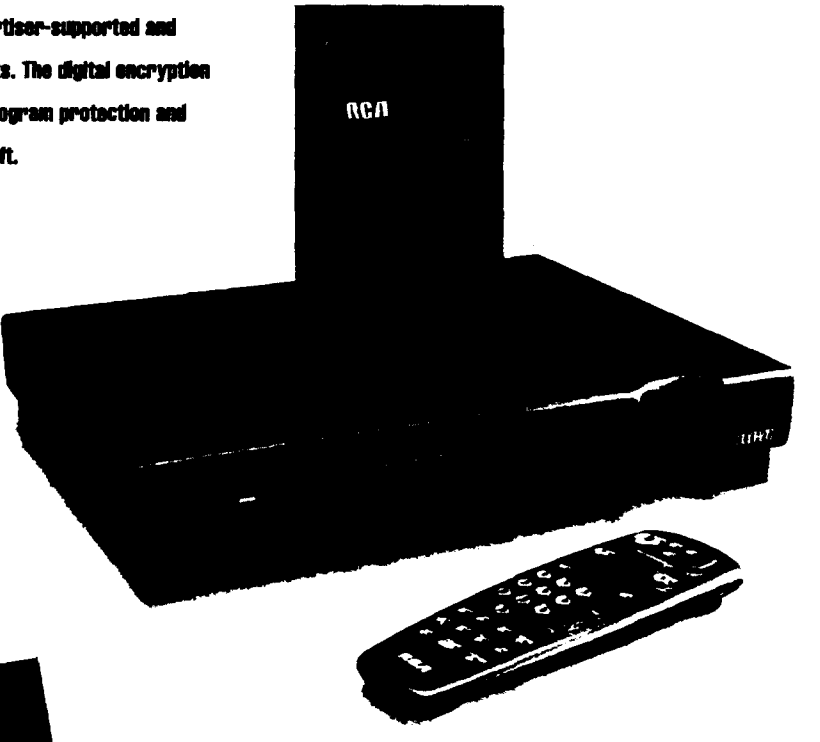
Conditional Access/Encryption

The conditional access system uses smart card technology provided by News Datacom for tracking subscriber service requests and providing authorizations for subscription, advertiser-supported and pay-per-view events. The digital encryption system ensures program protection and prevents signal theft.

Programming

DirecTv will offer television viewers over 150 channels of quality programming options. An innovative on-screen program guide provides viewers with automatic selection of their favorite channels, impulse pay-per-view movies, and enables scanning through the current program lineup. A-la-carte selection of programming or entertainment packages will provide unprecedented choice and convenience.

Program purchases are automatically billed to a major credit card or mailed monthly to DirecTv subscribers.



99.92

THE MOVIE CHANNEL™, FLIX™
EXPANDED ULTRAVIEW™

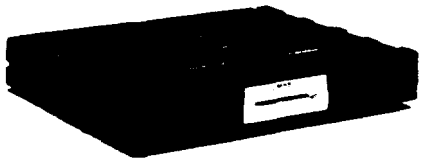
$539.92

PROGRAMMING PACKAGE AND
VCRS™ MODULE

SUPER LOW DEALS AND 2 SUPER HIGH REBATES!

gramming Package Deal op-rated SHOWTIME, THE MOVIE NNEL, FLIX and newly expanded ckage (now with 25 channels) is avail- d-time only at an annual dealer net cost 2. That means with the PercentagePlus ecial bonus rebate, you'll pocket a min-)0! And your customers will enjoy Television and KTLA which have just JLTRAVIEW...***at no extra charge.***

2 **Programming Package and VCRS Module Deal** Make the most of the conversion with our special combo package of a year of SHOWTIME, THE MOVIE CHANNEL, FLIX and ULTRAVIEW and a brand new VCRS Module for a dealer cost of just $539.92 (including shipping and handling)!



With the PercentagePlus rebate and special bonus rebate, your commission is at least $60! And ask about our module offer with monthly subscriptions.

PERCENTAGE*Plus*™ It's here! Showtime Satellite Networks' new profit-building rebate program now gives you our highest rebates ever on new and renewing customers. Earn from **17.5%** to **21%** on new subscrip- ions (plus rebates on active and passive renewals, upgrades and continuing nonthlies). Take advantage of this superb rebate opportunity today!

Call 1-800-422-9006

Attachment B

1. Progress Report of the National Replaceable Security Subcommittee of the JEC, January 19, 1994.

FAX

To: George Hanover, EIA, Washington, DC
Copy to: David Broberg, Mitsubishi, Cypress, CA
From: Jack Chaney, Thomson R&D, Indianapolis
Subject: NRSS Interim Report to the C^3AG
Wednesday, 5:00 PM EST, January 19, 1994

NRSS Progress Report to the C^3AG
by Co-Chairmen
Claude Raggett and Jack Chaney
January 19, 1994

The NRSS has made forward progress in the last three months. On November 3, the NRSS held a "Security Roundup" at EIA in Washington, DC. It was a good exchange of views. It was here that it became clear that there is a need to further isolate the security components in the designs of present consumer electronics systems. The program and cable providers consider signal scrambling technique, as well as entitlement management and purchase control, as a part of its security domain. As a result, the entire security system must be replaceable. On January 11, the NRSS co-chairmen presented the new concept of a Conditional Access Card. This card can provide security for digital consumer electronics. This card isolates all the security elements into one removable medium, is inexpensive, and uses an existing form factor. It will allow all types of digital consumer electronics to be developed independent of the conditional access system. This card meets all of the system attributes required by the committee. The committee is drafting a straw man specification which will be ready by March 8. This specification will specify the physical and electrical and software interface to the security system. The target date to complete this specification is April 15, 1994. It is this committee's goal to allow the application of this standard to Grand Alliance and MPEG2 systems level specifications and demonstrations.