

18 December 2003

Charles Goldwater, CEO
Walt Ordway, Chief Technology Officer
Digital Cinema Initiatives LLC
6834 Hollywood Blvd., Suite 500
Hollywood, California 90028

Peter D. Symes
SMPTE Engineering Vice President
Thomson Broadcast and Media
Solutions, Inc.
400 Providence Mine Road
Nevada City, California 95959

Dear Digital Cinema Standardization Leaders:

On behalf of hundreds of cinema companies operating more than 50,000 movie screens in the two leading markets of North America and Europe, we write to object strongly to recent developments in the digital cinema standardization efforts of your two organizations. By copy of this letter, we also seek to inform the European Community's Commissioner of Culture, and our colleagues at the European Digital Cinema Forum, of our concerns.

Specifically, we are concerned that work undertaken, and draft specifications developed, in the area of cinema security suffer from three fundamental flaws. First, that work should be postponed until studios and cinema operators can answer fundamental business questions that must precede the adoption of any standards related to digital cinema security. Second, the work goes beyond the bounds needed to combat movie piracy. Finally, some suggested draft standards would interfere with normal business operations within cinema facilities.

Cinema operators around the world demand the development of fair business models as a necessary antecedent to the large-scale transition from film to digital cinema. We have also consistently supported the cause of global, uniform, open technical standards for the implementation of digital cinema, all of which are essential to open competition.

On 12 December 2001, cinema trade association executives from eighteen countries released a statement calling for the immediate development of global technical standards and setting forth a list of prerequisite technical standards demands. Then in February 2002, the National Association of Theatre Owners (NATO) published its Digital Cinema User Requirements in the United States. These two documents were complimentary and consistent. Both documents stressed the need for security provisions to combat movie piracy without interfering with normal business operations.¹

¹ The international letter of 12 December 2001 provided a list of cinema operator "needs", including "Rules for digital rights expression and for electronic methods of exhibitor authorization that duplicate the

Representatives of NATO and the Union Internationale de Cinemas (UNIC) have both worked to support the efforts of Digital Cinema Initiatives (DCI) by meeting with DCI executives on a regular basis and by providing input, suggestions and commentary on the DCI draft specifications when requested. In turn, DCI has been very responsive to the input of our industry and most solicitous of our suggestions. We are grateful for the important work performed to date by DCI and the spirit of partnership that has existed throughout the life of that venture.

Indeed, in most substantive areas other than security, DCI's technical specification work has progressed appropriately and has provided important leadership for the eventual transition to digital technologies. Technical specifications regarding cinema security, however, simply cannot be developed without guidance on important business decisions.

While DCI has made tremendous progress on technical specifications in many areas, DCI has not provided any guidance whatsoever on any important business issues. Nor are these issues being addressed in any other appropriate forum. Related specifically to the subject of this letter, no significant work has been undertaken to answer the important business questions that must precede and inform the development of digital cinema specifications related to security.

Some of the important questions include the following. Where do the trust relationships lie? When should we rely on machines and when should we rely on people? Who should control the security equipment contained within a cinema complex? When, if ever, should the digital distribution and exhibition of a movie be prevented and the movie screen left to go dark? What content (e.g., movies, trailers, shorts, etc.) should be included in an inviolate set of digital files that cannot be separated? Who should control the audit data and security logs produced by the system? For what universe of distribution (cinema circuit, cinema complex, or cinema auditorium) should a set of digital movie files be targeted? For what universe should a set of digital keys be targeted? How long should it take to replace dysfunctional equipment? Where can replacement equipment come from and go to? Who should maintain logs of equipment? What factors, if any, will hinder the movement of digital "prints" between auditoriums within a complex? When and how can content other than motion pictures be exhibited on the equipment? What relative role and emphasis should be placed on preventative technologies (e.g., encryption) versus forensic technologies (e.g., watermarking)?

On these and related questions, our respective members have strong beliefs regarding the appropriate answers. As partners with the studios in the digital cinema planning process, we believe we should answer these questions with DCI now.

The answers to these questions and many others dramatically affect the technical specification work being undertaken by DCI. The answers also have critical impact on

current rights and facilities existing in 35 mm technology." Similarly, the NATO User Requirements of February 2002 stated that "The mechanisms and processes that support content protection shall not interfere with normal business operation within the facility."

theatres as the issues are determinative of whether theatre operators continue to have control of their own operations. Yet DCI continues to move forward on those technical specifications with no answers, or insufficient answers to the questions. On issues related to security, the DCI “cart” is miles ahead of the “horse.”

Exhibitor representatives also continue to participate in the essential work of the Society of Motion Picture and Television Engineers (SMPTE). We are pleased that SMPTE’s DC28 Technology Committee has made tremendous progress developing digital cinema standards, and we are committed to seeing the process to completion. We are alarmed, however, at the direction work has taken on the important issue of cinema security. Specifically, some participants in SMPTE’s DC28 Technology Committee are pursuing draft security standards that exceed what is necessary to combat piracy. These suggested security provisions would also completely alter the existing relationship between movie exhibitor and movie distributor, and dramatically change the normal operations within the cinema.

Piracy constitutes a fundamental threat to the entire motion picture industry. Over the past few years, NATO and UNIC have raised the fight against piracy to a new level of priority within our organizations. Exhibitors seek a continuing and strong partnership with movie studios on this important battle.

Piracy occurs at every juncture in the movie production, distribution and exhibition process. Exhibitors have no say, and do not seek to control, the manner in which piracy is fought in the production and distribution segments of this industry. The SMPTE work does not address those segments. The SMPTE work, however, would dramatically affect the exhibition segment of the industry.

In many cases, the draft work on security suggested by some DC28 participants presumes answers to the many business questions listed above, and would significantly change the competitive balance between distributors and exhibitors. Yet DC28 is not the proper forum for the resolution of those business issues.

In sum, we will not support the continuing efforts of DCI or SMPTE to design specifications and standards related to security unless and until several actions take place. First, studios and exhibitors must find a way, through DCI or elsewhere, to answer the fundamental business issues that will control the manner in which security systems are deployed in cinemas. Second, all participants in your two organizations must agree to focus all security work on that which is necessary to combat piracy. Third, those participants must agree to design any security standards in a manner that will not interfere with normal business operations within a cinema complex or change the competitive balance between exhibitor and distributor.

Thank you for your consideration of these views.

Sincerely,

Jan van Dommelen, President
UNIC
On behalf of its member associations
15, rue de Berri
F-75008 Paris
France

John Fithian, President
NATO
On behalf of its members
4605 Lankershim Blvd, Suite 340
North Hollywood, California 91602
U.S.A.

Cc:

Vivian Reding, Commissioner of Culture
European Commission

Ase Kleveland, Chairman
European Digital Cinema Forum

Tom Scott
SMPTE Engineering Director of Motion Picture Technology

Curt Behlmer, Chairman
SMPTE DC28 Technology Committee