Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Media Bureau Seeks Comment on DSTAC Report	)	MB Docket No. 15-64
	)	

To: The Commission

REPLY COMMENTS OF CISCO SYSTEMS, INC.

CISCO SYSTEMS, INC.

Jeffrey A. Campbell
Vice President, The Americas
Global Government Affairs
601 Pennsylvania Avenue, NW
North Building, 9th Floor
Washington, DC 20004
202.354.2920

November 9, 2015

TABLE OF CONTENTS

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Media Bureau Seeks Comment on DSTAC Report	)	MB Docket No. 15-64
	)	

REPLY COMMENTS OF
CISCO SYSTEMS, INC.

I. INTRODUCTION AND SUMMARY

Cisco Systems, Inc. ("Cisco") hereby responds to initial comments filed on the Media Bureau's above-captioned *Public Notice* ("*Notice*"),[1] which seeks comment on the work of the Downloadable Security Technical Advisory Committee (the "DSTAC Report").[2] Cisco has unparalleled expertise in video distribution security and has actively and consistently engaged in the Commission's proceedings regarding Section 629 of the Act. In particular, the company itself has extensive experience implementing a downloadable security system and deploying it at scale; it has closely followed the work of the DSTAC and presented to one of the DSTAC working groups at the group's invitation.

After carefully reviewing the DSTAC Report in the context of Cisco's long history as a leading security provider, it is Cisco's conclusion that the "virtual headend" approach (the

[1] *Media Bureau Seeks Comment on DSTAC Report*, Public Notice, MB Docket No. 15-64, DA 15-982 (MB rel. Aug. 31, 2015).

[2] FCC Chairman Tom Wheeler "established the DSTAC, a federal advisory committee made up of 'technical experts representing a wide range of stakeholders,' under Section 106(d) of the Satellite Television Extension and Localism Act Reauthorization Act of 2014 ('STELAR') … [which] required the DSTAC 'to identify, report, and recommend performance objectives, technical capabilities, and technical standards of a not unduly burdensome, uniform, and technology- and platform-neutral software-based downloadable security system designed to promote the competitive availability of navigation devices in furtherance of section 629 of the Communications Act [(the "Act")] …." *Notice* at 1 (internal citations omitted).

"Device Proposal")[3] simply is insufficient to protect against current and future security risks. As such, it is not suited for the realities of today's video distribution marketplace and should not serve as the foundation for any Commission rulemaking that may follow from the instant proceeding.

The industry, not the Commission, is best positioned to consider how the deeply-flawed Device Proposal could affect future development. For example, four years ago, Cisco urged caution in the Commission's AllVid proceeding based on innovation and deployment projections that since have generally come to fruition.[4] At that time, Cisco shared its vision of software-based multichannel video programming distributor ("MVPD") security (the Videoscape product, for which development then was well underway). Cisco explained that Videoscape, cloud-based technology and security that would allow consumers to watch MVPD and other video offerings from any device, anywhere, without being tethered to a set-top box, could not survive if the Commission imposed the proposed regulatory constraints. Cisco's vision has unfolded consistent with its predictions, thanks in part to the Commission's retreat from its AllVid proposal that would abruptly have curbed the evolution of Videoscape.

Today, as Cisco plans to largely exit the set-top box market through sale of its connected devices unit,[5] the company projects continued development of its software-based security. (This Cisco product is called VideoGuard Everywhere and is built-upon the world's most secure

[3] DSTAC Report at 4. The WG3 Virtual Headend System proposal recommends that network security and conditional access be performed in the cloud and the security between the cloud and retail navigation devices be a well-defined, widely used link protection mechanism such as DTCP-IP. *Id.*

[4] Letter from Natalie G. Roisman, Wilkinson Barker Knauer, LLP, Counsel to Cisco, to Marlene H. Dortch, Secretary, FCC, MB Docket No. 10-91, CS Docket No. 97-80, PP Docket No. 00-67 (Feb. 2, 2011) ("Cisco 2011 AllVid Ex Parte").

[5] Technicolor, Press Release, *Technicolor to Acquire Cisco Connected Devices Division for €550M in Stock and Cash* (July 23, 2015), http://www.technicolor.com/en/who-we-are/press-news-center/press-releases/technicolor-acquire-cisco-connected-devices-division-eu550m-stock-and-cash; *see also* Hilton Romanski, *Technicolor Acquires Cisco's Connected Devices Division*, CISCO THE PLATFORM BLOG (July 22, 2015, 9:29 PM), http://blogs.cisco.com/news/spvideocpe.

content security technologies formerly developed by NDS.) Cisco again urges the Commission to allow the marketplace to continue to develop to allow industry-based innovation, not government-mandated technology. The marketplace for video distribution and video distribution security is competitive and flourishing – at most, the Commission should issue a Notice of Inquiry ("NOI") to consider as an open question whether any steps are necessary beyond review of the DSTAC Report. If the Commission nevertheless determines that it should proceed with a rulemaking and issue a Notice of Proposed Rulemaking ("NPRM"), it should tentatively conclude that MVPDs and online video distributors ("OVDs") should adopt the security Application Program Interfaces ("APIs") in HTML5 as a non-exclusive security system interface with consumer electronics and customer premises equipment manufacturers. This is a common, open, established standard for the delivery of streaming media via Internet Protocol ("IP") and is the most appropriate approach for today's marketplace.[6]

II. CISCO HAS UNPARALLELED EXPERTISE IN VIDEO DISTRIBUTION TECHNOLOGY AND SECURITY

Cisco is well-known as a global leader in building intelligent networks that transform how people connect, communicate, and collaborate, and it has been on the front lines as networks of all kinds converge into IP-based communications. With video at the center of it all, the company is a leading innovator in video distribution technology that offers greater choice and

[6] DSTAC Report at 3-4. The WG3 HTML5 Security APIs proposal recommends that MVPD/OVDs and consumer electronics/customer premise equipment companies adopt the security APIs in HTML5 as a non-exclusive security system interface between MVPD/OVD services and consumer electronic devices. As the DSTAC Report notes, HTML5 is the 2014 standard defined by the World Wide Web Consortium (W3C) as a common and open approach to deliver IP streaming media based on IP. It is a full application foundation, supporting both security elements and non-security elements. HTML5 and its Encrypted Media Extensions ("EME"), Media Source Extensions ("MSE"), and Web Cryptography extensions are being deployed across the Web by multiple vendors on hundreds of millions of devices and are widely supported by all major browsers. EME "operates as a bridge" to allow competing digital rights management ("DRM") security systems to operate on multiple platforms; the EME extensions defines standard APIs that permit HTML5 to support media under common encryption, even while protected by a variety of DRMs. By not mandating a single system, EME "avoids creating a single point of attack for hackers." W3C APIs are used in Web browsers but can also be used outside of a browser on other device platforms. This approach makes for a competitive market for security systems. It is technology- and platform-neutral, royalty free, and open source.

convenience to consumers, working to make video content much easier to find, navigate, interact with and enjoy, on any device and network. Cisco's unique security expertise encompasses the particular experience of NDS (acquired by Cisco in 2012) with downloadable security on both managed and unmanaged devices.

Cisco consistently has shared its technical and business expertise with the Commission as the agency has grappled with the complex issues surrounding compatibility between MVPD networks and retail consumer electronics products. For example, in 2009, Cisco described to the Commission its work with MVPD customers to define the architecture and a variety of potential products for Cisco's Next Generation Video Delivery service, an IP video delivery system envisioned to allow Internet connectivity.[7] At that time, Cisco explained that the fundamental components of the architecture had been established and that Cisco and its customers had begun developing related products. Cisco urged the Commission to refrain from mandating Internet video capability in set-top boxes because consumer demand for advanced, IP-based access to Internet video was being met. Indeed, in the years to follow, consumers grew to regularly access Internet video of all types through their set-top boxes, television sets, and other equipment.

Subsequently, in 2010, Cisco explained that its Next Generation IP video platform and other similar industry initiatives would integrate video into consumer home networks without the need for regulation.[8] The platform focused on the future of consumer networks, with video as an integral component of services to a consumer's personal network of entertainment, information, and communications devices. The goal was to cost-effectively merge on a single platform MVPD managed video, managed and unmanaged broadband video, high speed data services, in-

[7] Comments of Cisco Systems, Inc., GN Dockets No. 09-47, 09-51 (NBP PN #27), and 09-137, CS Docket No. 97-80 (Video Device Innovation) (Dec. 22, 2009).

[8] Comments of Cisco Systems, Inc., MB Docket No. 10-91, CS Docket No. 97-80, PP Docket No. 00-67 (Video Navigation Devices) (July 13, 2010).

home routing, and wired and wireless voice services both at the hardware/software layer and at the services layer, enabling devices to connect to a host of MVPD- and third-party-provided services. In that filing, Cisco demonstrated that industry was able to achieve FCC goals (*e.g.*, providing expansive choice in the video device retail market, stimulating broadband adoption, promoting a competitive MVPD marketplace, and creating economic growth) without a mandate.

Shortly thereafter, Cisco observed that requiring disaggregation could force MVPDs to violate many of their legally-binding agreements with content producers, ratings agencies, and channel guide providers, a concern that remains valid today.[9] Security measures are crucial to ensure effective protection of content; as Cisco explained then and continues to believe now, "Content producers secure protection for their video works through distribution contracts that detail permissible uses. MVPDs effectuate these contractual responsibilities through binding contracts with equipment manufacturers, or through binding industry standards, creating a chain of contractual obligations to protect content."[10]

In 2011, Cisco introduced the Commission to Videoscape, its vision and platform for creating and consuming visual, mobile, and social video entertainment experiences through the convergence of digital TV, online content, and social media and video communications applications.[11] Cisco's service provider video solutions offerings today are a direct outgrowth of the "real, not speculative"[12] vision shared in 2011, and Cisco similarly is concerned that many of the same threats posed by AllVid also would arise from the Device Proposal.

[9] Reply Comments of Cisco Systems, Inc., MB Docket No. 10-91, CS Docket No. 97-80, PP Docket No. 00-67 (Video Navigation Devices) (Aug. 12, 2010).

[10] *Id.* at 21.

[11] Cisco 2011 AllVid Ex Parte.

[12] *Id.* at 3.

Today, Cisco's service provider video solutions include Infinite Home, Infinite Video, Infinite Broadcast, and VideoGuard Everywhere. As deployed today in the United States, Cisco's service provider video solutions comprise a comprehensive digital television architecture that benefits consumers by enabling service providers to integrate linear television delivery with an ever-growing set of Cisco, as well as third-party-provided, television applications including on-demand access to online content, download-to-go viewing of offline content, navigation to previously played linear content (Reserve EPG), Cloud DVR playback of recorded programs on any device at any time, as well as user-generated content and social media. It is an open platform utilizing the cloud and network to allow consumers to access content from multiple sources of their choice via multiple devices of their choice, with the security and premium quality of service that consumers expect from MVPDs. The Infinite and VideoGuard applications are already being downloaded to most popular consumer devices on the market today and are therefore already independent of any service provider's access technology – indeed, Cisco's confidence regarding video in the cloud is illustrated through the pending sale of its connected device business unit to Technicolor.[13] The NDS acquisition was specifically intended to accelerate Cisco's video entertainment strategy and has done so;[14] among other developments, Cisco's service provider video solutions all are pre-integrated with VideoGuard video content security technologies, including DRM as well as downloadable conditional access

[13] Cisco's interest in this proceeding is not in maintaining the leased device model, as it is largely exiting that business. *See supra* n.5.

[14] Cisco, Press Release, *Cisco Announces Intent to Acquire NDS* (Mar. 15, 2012) http://newsroom.cisco.com/press-release-content?articleId=712002 ("Cisco's open, standards-based Videoscape platform, which spans the cloud, the network, and end-user clients, is a key part of the company's overall video strategy …. The addition of NDS's leading software solutions, such as the end-user viewing client and content security solutions, combined with its systems integration expertise, will accelerate the delivery of the Cisco Videoscape platform. This acquisition reflects Cisco's increased strategic focus on video … and its investment in software and services revenue streams and competencies.").

system ("DCAS") VideoGuard is used by more than 85 leading pay TV operators around the world.[15]

III. CISCO'S VIDEOGUARD CONTENT SECURITY PRODUCT ILLUSTRATES INDUSTRY ACCOMPLISHMENTS IN FULLY DOWNLOADABLE SECURITY WITHOUT A REGULATORY MANDATE

Cisco was pleased to assist the DSTAC's Working Group 3[16] by delivering, upon the group's request, a detailed technical presentation on the VideoGuard Everywhere content protection platform.[17] The full presentation is available in the DSTAC docket, and highlights include the following:

- VideoGuard is the brand name for Cisco's service provider video content security products that enable monetization of video services by supporting a wide range of purchase models and preventing theft of service and fraud. VideoGuard safeguards the MVPD content and services on all devices used for video delivery associated with a subscriber's home or account.

- VideoGuard is unique in the industry for utilizing custom-built security profiles that are specialized for each customer. Rather than a one-size-fits-all MVPD content security solution, VideoGuard offers a large variety of solutions in response to the operational requirements of, and the particular, business-model-specific security threats to, each of Cisco's MVPD customers. No two MVPD customers have the same security needs – for example, direct broadcast satellite ("DBS"), cable, and telecommunications provider systems often have different security threats based on characteristics such as the size of the subscriber base, network attachment interfaces, and regulatory requirements.

- VideoGuard solutions may include standard and proprietary as well as downloadable and removable elements. A key reason for VideoGuard's success is the use of MVPD-

[15] U.S. customers of VideoGuard include Cablevision, Charter, Cox, and DirecTV, who are delivering linear, on-demand, broadcast, over-the-top streaming, as well as download-to-go content to their subscriber's service provider and consumer owned set-top boxes, mobile devices, game consoles, and smart TVs. International customers of VideoGuard include Sky, Vodafone, Astro, and Tata Sky.

[16] Working Group 3 ("WG3") ultimately submitted a report covering two approaches for addressing the security elements of a downloadable security system, including performance objectives, technical capabilities, and industry standards. DSTAC Report at 2.

[17] Cisco Systems, Inc., VideoGuard Everywhere: Overview of Downloadable Security Solutions, MB Docket 15-64 (dated June 2, 2015). The DSTAC "undertook extensive surveys and studies (including 50 technical presentations from 33 industry experts) of various security systems, of the trust infrastructure used for the secure delivery of commercial content and multichannel service, the variation in current video providers' distribution technologies and platforms, and the capabilities of various original equipment manufacturers and retail devices used with video services." DSTAC Report at 1.

specific security technologies (*e.g.*, customized algorithms and secure micro-processor designs); Cisco VideoGuard customers have never suffered from a "domino attack," where a successful attack on one customer propagates to another customer.[18]

- VideoGuard Everywhere is the cloud deployment version of the VideoGuard security solution, which provides security for services on both MVPD managed (or leased) devices such as set-top boxes and gateways, as well as on consumer-owned devices such as tablets and "smart" (Internet-connected) TVs. For securing broadcast content (*e.g.*, MPEG2 transports delivered over QAM), with rapidly changing crypto-periods (*e.g.*, descrambling keys that change every couple of seconds), VideoGuard Everywhere includes DRM or digital rights management as well as DCAS or downloadable CAS functionality. For all other content (*e.g.*, Adaptive Bitrate transports pulled or pushed over IP), VideoGuard Everywhere includes a flexible Multi-DRM framework.

- There are many different downloadable security software implementations currently deployed in the market. The VideoGuard Everywhere conditional access solution currently supports downloadable clients in native C code (*e.g.*, DLL like environments), in Java code (GEM/OCAP/ACAP like environments), as well as JavaScript (for HTML5-like environments).

- Cisco (and NDS, pre-acquisition) has worked for many years to strengthen device security at the fundamental security foundation: hardware. The MVPD "chain of trust" extends from a device's hardware, through to that device's software, and then through to a device application's ability to attach to the MVPD network. In the case of an MVPD-owned set-top box, this foundation is typically provided by a set-top box "system on chip" manufacturer. Cisco works to reduce the threat of piracy to its MVPD customers by evaluating and providing input to the underlying hardware device's security capabilities, such as use of "One-Time-Programmable" memory, as well as implementation of secure keys, certificates, and bootloaders.

IV. SECURITY IS AN INTEGRAL COMPONENT OF ALL SUCCESSFUL VIDEO DISTRIBUTION SYSTEMS

A. Security is Critical to Video Distribution and to Consumers' Ability to Enjoy High-Value Content at the Time, Place, and Platform of Their Choice

The distribution of high-quality video content depends in substantial part on the confidence of content owners and distributors that revenues flowing from distribution of such content will not be jeopardized by weak security. Security is the underpinning that enables all of

[18] Even in the most challenging one-way threat environments, VideoGuard has been uncompromised for over a decade, due not only to MVPD-specific technologies but also to Cisco's world-leading operational security team.

the distribution systems for MVPDs and OVDs, and distributors lacking high-quality security are disadvantaged in acquiring content. It is security that enables creative, consumer-friendly offerings, including secure home recording, video on demand ("VOD") (and subscription VOD), viewing expiration times, rental windows, device- and household-level entitlements, and multi-device policies. Cisco has built its video distribution technology business with a primary focus on security because the video distribution ecosystem simply cannot operate without strong security. Cisco's VideoGuard content security products protects over $100 billion of service provider revenue annually, and Cisco's VideoGuard has 32% of the service provider content security market share. Cisco thus has the expertise and experience to identify the substantial flaws in the Device Proposal, which would compromise security and, necessarily, jeopardize the foundation of the video distribution ecosystem.

B. The Dynamic and Competitive Video Distribution Marketplace is Reflected in the Similarly Dynamic and Competitive Market for Conditional Access and Digital Rights Management

Today, there is a dynamic and competitive market in CAS/DRM. As just one example, over the last year every video service provider has been required to eliminate their plug-in based IP video technologies for Internet browsers and instead adapt to multiple native IP video formats (including specific DRM platforms) built-in to the major browser products (*e.g.* Google Chrome, Microsoft Explorer, Apple Safari). The safest ecosystem is one with multiple security solutions, each of them consistently evolving. A moving target is harder to hit, and, thus, a government-mandated, monolithic security requirement is directly contrary to the nimble quality of the highest-level security. DRMs evolve quickly against moving targets of attackers and to support moving targets of evolving business models. Security changes cannot wait for a standard to change. The industry also has organically evolved toward a diversity in security models, which reduces the risks of a single point of attack.

Cisco urges the Commission to give serious consideration to the importance of security and to the need for any such security to be both strong and nimble.

V. THE DEVICE PROPOSAL FAILS TO REFLECT TECHNICAL, LEGAL, AND PRACTICAL SECURITY REALITIES

The DSTAC Report offered two possible paths forward, and it is not surprising that comments in this proceeding have been divided, just as the work of the DSTAC was.[19] The key difference in the two proposals is that the Device Proposal does not include a security solution that meets the requirements of MVPDs and content providers. Many of these deficiencies were detailed in the DSTAC Report, and rather than comments supporting the Device Proposal addressing or correcting them, the issues have been magnified. The Commission should not move forward to a rulemaking proceeding, but if it does, the only appropriate course of action would be to adopt the HTML5 Security APIs Proposal.

The Commission has completed its responsibilities under STELAR by convening the DSTAC and reviewing its report. Congress did not direct the Commission to act on the DSTAC Report, there is significant disagreement as to the scope of the Commission's authority under Section 629, and (as reflected in the disparate proposals in the DSTAC Report), there is no industry consensus as to how to proceed. Launching a rulemaking proceeding – particularly one with the Device Proposal as a premise – is unnecessary and counterproductive, directing key industry resources away from development and deployment of new, consumer-friendly solutions toward a backward-looking regulatory mandate.

[19] The DSTAC did not reach a consensus recommendation but did have "major points of agreement," including that: (i) there is a "wide diversity in delivery networks, conditional access systems, bi-directional communication paths, and other technology choices across MVPDs"; (ii) it "should not be necessary to disturb the potentially multiple present and future CA/DRM system choices made by cable, DBS, and IPTV systems, which effectively leave in place several proprietary systems for delivering digital video programming and services across MVPDs"; (iii) it is "unreasonable to expect that retail devices connect directly to all of the various MVPDs' access networks"; and (iv) it is "unreasonable to expect that MVPDs will modify their access networks to converge on a single common security solution" or that "all MVPDs will re-architect their networks in order to converge on a common solution".

In any event, one need only look at comments in this proceeding to see that the goals of Section 629 have been realized: There is no question that video consumers have more choices in content, distribution, and devices than ever before. The Commission does not need to "commence a rulemaking to ensure that … consumers enjoy these sorts of options,"[20] because they already do. It is startling, given the wide array of choices in the video marketplace, that Consumers Union would say consumers "have no practical alternatives to renting set-top boxes that can access MVPD content" and that design and licensing of technology is controlled by "special interests."[21] In contrast, as AT&T aptly explains, "Dumbing down MVPD services and stripping out their features [under the Device Proposal] … is exactly the wrong approach in a marketplace where consumers already ubiquitously access MVPD and OVD content on a wide and growing array of retail devices."[22]

If it does move forward, the Commission must look more carefully at the practical weaknesses of the Device Proposal. There is insufficient, impractical information in the Device Proposal to formulate even an NPRM, so the most the Commission should do is move forward to an NOI. But the weaknesses of the Device Proposal are so significant that they should give the Commission pause as it considers next steps. For example, the Commission should carefully investigate whether the Device Proposal exceeds the bounds of its authority under STELAR and Section 629, and it should consider the practical and legal consequences of mandatory disaggregation of MVPD content.[23]

[20] Google Comments at 4.

[21] Consumers Union Comments at 1.

[22] AT&T Comments at 23.

[23] The Device Proposal breaks the necessary license relationships and chains of trust on which the secure distribution of programming is based. In contrast, the Device Proposal "makes no commitment to abide by content providers' licensing terms," and "[t]hird parties could potentially seek to disassemble the programming, features, and functions offered over distribution services and selectively reassemble some of them for their own commercial

From a technical perspective, the Commission cannot give credence to comments that downplay the integration and operational complexities of the Device Proposal. The Device Proposal relies on DTCP-IP link protection, with possible extensions, as a single solution for the proposed interface to all MVPDs. This monolithic security solution would present a single point of failure or attack – a step backward from the industry's existing approaches that layer link protection with additional protections such as DRM.[24] DTCP also has not changed quickly enough to support changing or differentiated business models, and the Device Proposal thus also represents a step backward in terms of its usefulness for a broad array of distribution services. Moreover, the Device Proposal does not adequately define device authentication, trust authority, trust infrastructure (issuance, injection, protection, propagating revocation lists and requirements to query CRLs), and any policies necessary to make the certificates useful (profile, fields and information), testing and certification, or renewal. Some commenters would have the Commission dismiss these concerns as those of policy, not content security,[25] but they miss the point that a policy decision in favor of the Device Proposal necessarily – and, perhaps, irreparably – directly and substantially compromises security. Amazon offers vague assurances that security concerns are "misplaced" – without the background to know whether this is the case. (In any event, Cisco notes that Amazon has deployed Amazon Prime Instant Video without a mandated regulatory solution.) Public Knowledge glibly suggests that the Device Proposal comes with security protections that are off-the-shelf and that it does "not require any compromises or changes to the MVPD's security mechanisms, systems, or standards."[26]

exploitation. This could interfere with contracts, upset copyright law, and run afoul of … [the] Constitution." MPAA Comment at 2.

[24] Even DRM alone is augmented in order to provide the service protection necessary in today's market.

[25] *See, e.g.*, Amazon Comments at 5.

[26] Public Knowledge Comments at 18.

Similarly, Hauppage opines that no new work is required to define the necessary API and that "the API and security would be the same and apps could be developed once and run on a wide range of devices on any TV system used in the United States."[27] These comments bear no basis in technical reality, go beyond even the security approach of the Device Proposal in the DSTAC Report, and demonstrate the danger and fallacy of a rushed, oversimplified, impractical call for rulemaking.

In contrast, EchoStar, a company with experience in retail devices and an association with a competitive entrant in the video distribution market, correctly warns that the FCC "must not oversimplify this complex technological and service delivery ecosystem, as doing so would likely lead to a regime that does not adequately reflect and protect the legitimate interests of all affected parties."[28] The American Cable Association, representing numerous small operators, urges the FCC to proceed with "great caution," given that the Device Proposal would require "millions of dollars of network upgrades in a short span of time."[29] These concerns are real, raised by parties with significant experience in video distribution security – both its possibilities and its vulnerabilities. The Commission cannot give them short shrift.

VI. CONCLUSION

For the reasons discussed herein, Cisco urges the Commission to refrain from a rulemaking proceeding premised on the Device Proposal for security. If the Commission does issue an NPRM, it should tentatively conclude that the HTML5 Security APIs Proposal is the only approach sufficient to protect the high-value content that consumers demand. Following its detailed presentation to Working Group 3, Cisco would be pleased to continue to assist the

[27] Hauppauge Comments at 2.

[28] EchoStar Comments at 1.

[29] American Cable Association Comments at 4, 14.

Commission if the agency proceeds to consider the complex technical issues of video distribution security.

Respectfully submitted,

CISCO SYSTEMS, INC.

By: *___/s/ Jeffrey A. Campbell_____*

Jeffrey A. Campbell
Vice President, The Americas
Global Government Affairs
601 Pennsylvania Avenue, NW
North Building, 9th Floor
Washington, DC 20004
202.354.2920

November 9, 2015