

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of)
)
Expanding Consumers' Video Navigation Choices) MB Docket No. 16-42
)
Commercial Availability of Navigation Devices) CS Docket No. 97-80

To: The Commission

**COMMENTS OF
CISCO SYSTEMS, INC.**

CISCO SYSTEMS, INC.

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

April 22, 2016

TABLE OF CONTENTS

I. INTRODUCTION AND SUMMARY	1
II. APPS HAVE ENABLED MORE CHOICES IN CONTENT, DISTRIBUTION, AND DEVICES THAN EVER BEFORE, AND WILL CONTINUE TO DO SO IF NOT CONSTRAINED BY A SET-TOP BOX MANDATE	4
III. TODAY’S COMPETITIVE VIDEO MARKETPLACE IS ENABLED BY STRONG, VARIED SECURITY	6
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	7
B. The Dynamic and Competitive Video Distribution Marketplace is Reflected in the Similarly Dynamic and Competitive Market for Conditional Access and Digital Rights Management	7
C. The Commission Should Adopt Best Practices for Security Video Content.....	8
IV. THE PROPOSED SET-TOP BOX MANDATE WOULD HAMPER SECURITY AND STIFLE FUTURE INNOVATION	9
A. The Commission Should Not Mandate a Specific Deadline for the Development of the Proposed Open Standards	10
B. Any Rules Should Ensure a Diverse Ecosystem of Security Solutions Enabling Network, Device, and Content Diversity	11
V. CONCLUSION.....	13

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of)	
)	
Expanding Consumers' Video Navigation Choices)	MB Docket No. 16-42
)	
Commercial Availability of Navigation Devices)	CS Docket No. 97-80

**COMMENTS OF
CISCO SYSTEMS, INC.**

I. INTRODUCTION AND SUMMARY

Cisco Systems, Inc. (“Cisco”) submits these comments in response to the above-captioned *Notice of Proposed Rulemaking* (“*NPRM*”).¹ Cisco is well respected for its unparalleled expertise in video distribution security, and the company has actively and consistently engaged in the Commission’s numerous proceedings regarding Section 629 of the Communications Act of 1934, as amended (the “Act”).² In particular, Cisco has extensive experience *actually* implementing a downloadable security system and deploying it at scale; most recently, it has closely followed the work of the Downloadable Security Technical Advisory Committee (“DSTAC”), presented to one of the DSTAC working groups at the group’s invitation, and commented on the final DSTAC Report. After careful review of the *NPRM*, it is

¹ *Expanding Consumers' Video Navigation Choices and Commercial Availability of Navigation Devices*, Notice of Proposed Rulemaking and Memorandum Opinion and Order, 31 FCC Rcd 1544 (2016) (“*NPRM*”).

² *See, e.g.*, Reply Comments of Cisco Systems, Inc., MB Docket No. 15-64 (Nov. 9, 2015) (“Cisco DSTAC Comments”); 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”); Reply Comments of Cisco Systems, Inc., MB Docket No. 10-91, CS Docket No. 97-80, PP Docket No. 00-67 (Aug. 12, 2010) (“Cisco Video Navigation Reply Comments”); Comments of Cisco Systems, Inc., MB Docket No. 10-91, CS Docket No. 97-80, PP Docket No. 00-67 (July 13, 2010).

Cisco's conclusion that the "Via Media Proposal"³ simply is insufficient to protect against current and future security risks and that it thus would be irresponsible for the Commission to mandate this approach. Specifically, the introduction of a mandatory standard would *reduce* both device and content diversity, contrary to the public interest and the stated goals of the *NPRM*.

Companies, by their very nature, must consistently be looking years into the future. So it is the industry, not the Commission, that is best positioned to consider how the deeply-flawed Via Media Proposal could affect future development in the video distribution marketplace. Cisco correctly predicted five years ago that software-based multichannel video programming distributor ("MVPD") security would allow consumers to watch MVPD and other video offerings from any device, anywhere, without being tethered to a set-top box.⁴ Today, a vibrant "TV Everywhere" marketplace exists, thanks in part to the Commission's retreat from its AllVid proposal that would abruptly have curbed the evolution of downloadable security systems.⁵ The Commission was right to avoid regulation at that time, and Cisco again urges the Commission to allow industry-based innovation, rather than stifling, government-mandated technology to dictate the future.

The marketplace for video distribution and video distribution security already is competitive and flourishing, and the Commission's premise for the *NPRM* proposal thus is unfounded. Consumers have incredible choices available to them every day, on multiple

³ *NPRM*, 31 FCC Rcd at 1568-69 ¶ 50 (dubbing the *NPRM*'s security proposal the "via media" approach). The *NPRM* proposes that MVPDs make available three "Information Flows" in their entirety subject to a "compliant" content protection system that is "licensable on reasonable and non-discriminatory terms, and must not be controlled by MVPDs." *Id.* at 1572 ¶ 58.

⁴ Cisco 2011 AllVid Ex Parte.

⁵ *Video Device Competition; Implementation of Section 304 of the Telecommunications Act of 1996: Commercial Availability of Navigation Devices; Compatibility between Cable Systems and Consumer Electronics Equipment*, Notice of Inquiry, 25 FCC Rcd 4275 (2010).

platforms. By using an apps-based approach, the MVPD industry can continue to make such options available for consumers to enjoy on devices, and through software, of their choosing. The Commission should refrain from adopting its Via Media Proposal and allow MVPDs' and online video distributors' ("OVDs") continued adoption of the generic security Application Programming Interfaces ("APIs") as a non-exclusive security system interface with consumer electronics and customer premises equipment manufacturers. This would satisfy the requirements of Section 629.⁶ HTML5 is a common, open, established standard for the delivery of streaming media via Internet Protocol ("IP") and is one of the options appropriate for today's dynamic marketplace.⁷ If the Commission nevertheless determines that it should proceed with the proposal in the *NPRM*, any new rules must include protections to ensure a marketplace for strong security by, in particular, reforming the proposed standards-setting process to ensure that it allows for sufficient deliberation and effectively enables security best practices.

⁶ 47 U.S.C. § 549; *NPRM*, 31 FCC Rcd at 1547 ¶ 5 (observing that Section 629 directs the Commission "to adopt regulations to assure the commercial availability of devices that consumers use to access multichannel video programming and other services offered over multichannel video programming networks" while prohibiting the Commission "from adopting regulations that would 'jeopardize security of multichannel video programming and other services offered over multichannel video programming systems, or impede the legal rights of a provider of such services to prevent theft of service'" (quoting 47 U.S.C. § 549(b)).

⁷ Downloadable Security Technical Advisory Committee Report, 30 FCC Rcd 15293, 15297-98 (2015) ("DSTAC Report") (attached to *Media Bureau Seeks Comment on DSTAC Report*, Public Notice, 30 FCC Rcd 15293 (2015)). 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.

II. APPS HAVE ENABLED MORE CHOICES IN CONTENT, DISTRIBUTION, AND DEVICES THAN EVER BEFORE, AND WILL CONTINUE TO DO SO IF NOT CONSTRAINED BY A SET-TOP BOX MANDATE

The future of television is bright with possibility, due to innovative new technologies introduced on a daily basis. In particular, the advent of a multiplicity of Apps, including HTML5 Apps, is driving substantial increases in consumer choice by facilitating MVPD content on consumers' televisions (through Roku boxes, game consoles, and more), mobile devices, and PCs.⁸ As one analyst recently observed, “[j]ust as consumers buy drill bits because they want the holes they make, true [set-top box] demand is for the features and functionality the devices provide and not the box itself...”⁹ Cisco’s security and solutions are key to consumers’ ability to access the features and functionality of the MVPD and OVD set-top boxes and other consumer electronics (“CE”) devices through Apps, as Cisco builds the world’s most robust security technologies for broadcast and internet-delivered television.

When assessing the market for competitive devices, the Commission must recognize the increasing importance of MVPD traffic delivered using IP, including through CE device Apps.¹⁰ Internet video to television grew 47 percent in 2014 alone.¹¹ In fact, *all* IP traffic is bending towards video.¹² Consumer video-on-demand “will nearly double by 2019” to the equivalent of

⁸ See, e.g., DSTAC Report, 30 FCC Rcd at 15333-34, 15342-45 (listing numerous OTT and MVPD-provided apps and internet-delivered video options).

⁹ Frank G. Louthan IV *et al.*, *TMT: FCC Set Top Box Proposal Commentary: Not the BYOB Party the Commission Envisions*, at 2, Raymond James U.S. Research (Apr. 11, 2016) (“Raymond James Research”) (attached to Letter from Frank Louthan *et al.*, to Tom Wheeler *et al.*, Chairman, FCC, MB Docket No. 16-42 & CS Docket No. 97-80 (Apr. 11, 2016)).

¹⁰ See DSTAC Report, 30 FCC Rcd at 15322 (describing current MVPD distribution technologies and platforms such as Quadrature Amplitude Modulation for broadcast signals while over Hybrid Fiber Coax or Broadband-/Gigabit-capable Passive Optical Networks, MPEG-2, MPEG-4 AVC, MPEG HEVC, as well as IP).

¹¹ Cisco, *The Zettabyte Era: Trends and Analysis*, White Paper, at 2 (May 2015), http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/VNI_Hyperconnectivity_WP.pdf.

¹² *Id.*

7 billion DVDs per *month*.¹³ Based on the number (and projected growth) of MVPD-leased set-top boxes compared to other consumer electronics, the predicted growth of video and IP traffic means that consumers will be consuming video content – very often MVPD content – more than ever through Apps on competitive devices in the future.

One needs to look no further than mobile video consumption to see the impact of Apps. For example, “[m]obile video traffic now accounts for more than half of all mobile data traffic,” and Cisco estimates that three-fourths of the world’s mobile data traffic will be video by 2020.¹⁴ Although the *NPRM* appears to discount the importance of video accessed on streaming and mobile devices,¹⁵ Cisco’s research demonstrates that “[mobile v]ideo usage tends to occur during the evening hours and has a ‘prime time,’ unlike general web usage that occurs throughout the day,” indicating that, to some extent, consumers are using mobile video to increasingly augment their traditional television viewing.¹⁶ The current Apps model allows MVPDs, security providers, and device manufacturers to use common approaches, but with the flexibility to update their systems on a continuing basis when service and security dictate it.¹⁷

Further, Cisco’s VideoGuard content security product illustrates industry accomplishments in fully downloadable security without a regulatory mandate. As deployed

¹³ *Id.*

¹⁴ Cisco, *Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update: 2015-2020*, White Paper, at 2-3 (Feb. 3, 2016) (“VNI 2016”), <http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.pdf>.

¹⁵ *NPRM*, 31 FCC Rcd at 1552 ¶ 14.

¹⁶ VNI 2016 at 26; *see also* Raymond James Research at 3 (discussing changing viewer habits, including a migration away from MVPD-provided set-top boxes). In other contexts – namely accessibility – the Commission has recognized this “second screen” effect. *See, e.g., Accessible Emergency Information, and Apparatus Requirements for Emergency Information and Video Description: Implementation of the Twenty-First Century Communications and Video Accessibility Act of 2010*, Second Report and Order and Second Further Notice of Proposed Rulemaking, 30 FCC Rcd 5186 (2015).

¹⁷ Raymond James Research at 4 (noting that pay-TV providers make hundreds of updates and patches per month).

today in the United States,¹⁸ 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. This architecture 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. Cisco's "Infinite" platform solutions and VideoGuard security 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. Cisco's service provider video solutions all are pre-integrated with VideoGuard video content security technologies, including DRM as well as downloadable conditional access system ("CAS"). As discussed in more detail in the next section, dynamic and diverse security is essential to today's video ecosystem.

III. TODAY'S COMPETITIVE VIDEO MARKETPLACE IS ENABLED BY STRONG, VARIED SECURITY

Security underpins all of the distribution systems for MVPDs and OVDs, and distributors lacking high-quality security are disadvantaged in acquiring content, in turn adversely impacting consumers who are deprived of must-have programming. Any Commission action must allow security providers to continue to adhere to security best practices in order to ultimately benefit consumers.

¹⁸ 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. More than 85 leading pay-TV operators around the world use VideoGuard. Cisco maintains the longest record in the industry for unhacked pay-TV security services. 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 subscribers' set-top boxes (both service provider- and consumer-owned set-top boxes), mobile devices, game consoles, and smart TVs.

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

Security challenges and opportunities arise continuously through daily environmental interactions, including technological innovations, commercial or political mandates, as well as industry standardization and consolidation. Security measures are crucial to ensure effective protection of content; as Cisco previously has explained, "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."¹⁹

For any necessary change in technology, the security platform provider is responsible for deployment in an optimal fashion that continues to secure existing business models and enables the rapid introduction of new business models. Cisco fully expects industry change – technology, business models, and participants – to accelerate over the next decade at a pace even more rapid than has been experienced by the television industry over the last decade. A decade ago, few envisioned the ubiquitous delivery of high-quality linear and on-demand television over the top; today we can hardly imagine what types of television consumers will be experiencing a decade from now.

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

The CAS/DRM market is dynamic and competitive. This diversity of options makes sense, given that the safest ecosystem is one with multiple security solutions, each of them regularly evolving. A government-mandated, monolithic security requirement like the *NPRM*

¹⁹ Cisco Video Navigation Reply Comments at 21 (footnotes omitted).

contemplates is directly contrary to the nimble quality of the highest-level security.²⁰ DRMs evolve quickly against moving targets of attackers and to support moving evolving business models. There will have to be new industry standards that simplify integration between these different device models, even as today's video standards and security frameworks are enabling a variety of existing devices. Simultaneously, security changes cannot wait for a standard to change; indeed, some innovations will leapfrog existing standards and technologies.

Organically-evolved, diverse security models reduce the risks of a single point of attack.²¹

Although a single, mandated standard would risk security, Cisco recognizes that standards provide an important common language that can prevent equipment obsolescence and increase competition. For example, Cisco has taken the lead in introducing standards that enable a loose coupling of content encryption from the key management and license delivery systems, including SimulCrypt, which enables MVPDs to rapidly introduce new services without being tied to any particular security provider.²²

C. The Commission Should Adopt Best Practices for Security Video Content

As a security platform provider to MVPD and media companies, Cisco urges that any Commission rules should permit Cisco and the industry to continue to adhere to security best practices for video delivery, including:

²⁰ See, e.g., Harold Furchtgott-Roth, *The FCC Should Drop Its Proposed Rules For Set-Top Boxes*, Forbes, at 2 (Apr. 12, 2016) (“With proprietary devices outlawed, only generic set-top boxes would be lawful... [M]anufacturers that specialize in customizable proprietary software and ever better security systems would have a diminished market.... The range of video options would be diminished, and the security and privacy currently afforded by set-top boxes would be lost.”), <http://www.forbes.com/sites/haroldfurchtgottroth/2016/04/12/the-fcc-should-drop-its-proposed-rules-for-set-top-boxes/2/#256a977b188b>.

²¹ See Cisco DSTAC Comments at 9.

²² See Tony Wasilewski, *Simulcrypt: May They Live Happily Ever After*, Cisco SP360: Service Provider Blog, May 30, 2008 (noting that Simulcrypt can bridge legacy and new network equipment and set-top boxes, increasing vendor competition for MSOs and IPTV providers), http://blogs.cisco.com/sp/simulcrypt_may_they_live_happily_ever_after.

- *Renewability.* Renewability, rather than standardization, avoids revocation of complete classes of consumer electronics.
- *Avoidance of fixed security elements.* Fixed keys and vulnerable security algorithms create a single point of attack for hackers.
- *Device integrity checking.* Strong device authentication and detection of tampering – such as device rooting and jail-breaking – leads to strong protection of user information, privacy, content/player output control, and additional App code (where, for example, applications must be signed in to run on a particular device).
- *Business rule security.* Correct measurement and accounting of content usage, event-based access, and concurrency checks prevent circumvention of usage. Such circumvention would prevent content and distribution companies from monetizing their offerings.
- *Appropriate for different business use cases.* Live TV, on-demand, streaming, download, and stored content must be secured across different networks.
- *Video format independent.* Security must be independent of the several video resolution, video compression, transcoding, and video streaming technologies.
- *Choice of technology appropriate to the current market conditions.* This ensures the best balance of security, complexity, and ultimately security costs.

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.

IV. THE PROPOSED SET-TOP BOX MANDATE WOULD HAMPER SECURITY AND STIFLE FUTURE INNOVATION

The government-mandated reduction to a single, regulated standard for security would create unacceptable vulnerabilities, prevent future innovations, and hamper the current, competitive marketplace.²³ This approach is risky and irresponsible. As explained above, absolute standards and frameworks provide a single point of attack and thus are easy targets for

²³ See *NPRM*, 31 FCC Rcd at 1572 ¶ 58 (defining a “compliant” system as one that is “licensable on reasonable and non-discriminatory terms, and must not be controlled by MVPDs”); *Ex Parte* Notice from Michael Romano, Senior Vice President – Policy, NTCA – The Rural Broadband Association, to Marlene H. Dortch, Secretary, FCC, MB Docket No. 16-42, CS Docket No. 97-80, at 2-3 (Apr. 12, 2016) (noting that very limited demand for third-party devices that are operable with “the diversity of small MVPD networks” means that “small MVPDs will ultimately be forced to adopt and implement the same standards as larger providers, resulting in a technology mandate by default for the former”).

malicious actors. Regulated standards that dictate what a security system can and cannot do will tie the hands of a security platform provider like Cisco, which needs the flexibility to adapt to every changing security circumstance. Only standards processes that provide time for sufficient deliberation, evaluation, and flexibility to accommodate changing security needs stand a chance of complying with Section 629’s prohibition against regulations that would “jeopardize security of multichannel video programming and other services offered over multichannel video programming systems, or impede the legal rights of a provider of such services to prevent theft of service.”²⁴

A. The Commission Should Not Mandate a Specific Deadline for the Development of the Proposed Open Standards

Through decades of participating in standards development processes, Cisco’s experience has been that a deliberative process, which allows standards bodies the time to evaluate and iterate multiple technical approaches, leads to more useful and widely adopted standards. A key component of such a process is the lack of a specific deadline. The *NPRM* proposes a two-year deadline for MVPDs to come into compliance,²⁵ meaning that the standards process will be afforded significantly less than two years to enable MVPDs and their partners, such as Cisco, time to develop compliant software and hardware. This tight deadline inevitably will lead to a rushed standards process, reducing the ability of the standards body to deliberate and develop a standard that will meet the needs of the covered entities and their partners. The Commission should not set a deadline for the development of open standards under any new rules. Artificial deadlines can create opportunities for poor decision-making and increase the risk of

²⁴ 47 U.S.C. § 549(b).

²⁵ *NPRM*, 31 FCC Rcd at 1565 ¶ 43 (“[W]e propose to require MVPDs to comply with the rules two years after adoption.”).

vulnerabilities to enter. Past experience with standards processes indicates that important standards often take far longer than two years to be completed.

B. Any Rules Should Ensure a Diverse Ecosystem of Security Solutions Enabling Network, Device, and Content Diversity

Consistent with security best practices, the Commission must ensure security diversity and avoid fixed security systems that lead to single points of attack. Focusing on security renewability, upgradeability, and device diversity – rather than absolute standardization – will enable the industry to adapt to evolving threats. Solutions that focus on renewability and upgradeability will stand the test of time and be able to sustain content businesses over many years. Indeed, for decades, Cisco has practiced what it has preached by focusing on renewable security with both hardware elements (such as smart cards) and software solutions (such as moving target-software for DRM), which has fueled its success. Any rules should ensure a diverse ecosystem of security solutions, as well as include support for renewability of security technologies in a competitive fashion.

Technology is rapidly changing the nature of content itself. Whether through adaptation to new applications, formats, or delivery technologies (*e.g.*, Virtual Reality, High-Dynamic Range, and Ultra-High Definition 4K and 8K formats), content is evolving. By choosing the technology most appropriate for current market conditions, industry can best balance security, complexity, and cost. In contrast, a one-size-fits-all standard has the potential to stifle new content diversity by limiting support for these evolving content formats.²⁶ For instance, regulated standards that mandate a particular encoding format will limit innovations in

²⁶ *See, e.g.*, Comments of AT&T, MB Docket No. 15-64, at 23 (Oct. 8, 2015) (“Dumbing down MVPD services and stripping out their features [under the similar DSTAC Media Server 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.”).

compression technology by dictating what formats could be included in the regulated standard.²⁷ Regulated standards that require MVPDs to expose a limited set of metadata will correspondingly limit innovations in new service deployments that require new metadata that are not included in the regulated standard. To ensure that any future standard promotes content diversity, standards must be permitted to evolve. Cisco recommends that any rules should ensure a diverse ecosystem of content types that supports the evolution of new content formats.

Any rules also must ensure a diverse ecosystem of network technologies that do not disadvantage any particular network topology. As acknowledged in the *NPRM* and *DSTAC* Report, every MVPD network is unique, and some MVPDs may even be unique from one division to another.²⁸ If it is not carefully crafted, a “one-size fits-all” standard could disadvantage a particular network topology. Content currently travels across many networks: broadcast, cable, Internet, cellular, in-home, other wireless networks, device-to-device, etc. The wrong approach on security standards could render content unavailable to certain segments of the population or on certain devices because industry will not be able to achieve a sufficient level of security. Equally problematic, an incentive to build solutions around a lowest common denominator would reduce the capabilities of any future video offerings as well as security across the board.²⁹

Likewise, any rules intended to increase device diversity must reflect that devices with varying capabilities – whether in processor speed, screen size, memory, or data storage – will

²⁷ See, e.g., Comments of EchoStar Corporation, MB Docket No. 15-64, at 1 (Oct. 8, 2015) (warning that the Commission “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 *NPRM*, 31 FCC Rcd at 1572-73 ¶ 59 (observing that MVPDs employ system-specific content security equipment in subscribers’ homes); *DSTAC* Report, 30 FCC Rcd at 15296.

²⁹ Because MVPDs do not only offer video services to their customers, but are often also telephony, Internet, and security providers, reducing *network* security may have consequences beyond theft of video service.

require unique implementations of any standard. These implementations require time, evaluation, and iteration. Cisco recommends that any rules should ensure a diverse ecosystem of device types that are not disadvantageous to any particular device type.

The security inherent in well-constructed Apps fulfils the criteria above. Indeed, the App approach – not the *NPRM*'s Via Media Proposal – accomplishes the dual commands of Section 629: (i) assuring the commercial availability of devices to access MVPD content and services and (ii) eschewing regulations that would risk security or enable theft of service.³⁰

V. CONCLUSION

Cisco urges the Commission to refrain from adopting the Via Media Proposal and instead allow the industry to continue work on the Apps approach, the only approach sufficient to protect the high-value content that consumers demand.

Respectfully submitted,

CISCO SYSTEMS, INC.

By: /s/ Jeffrey A. Campbell

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

April 22, 2016

³⁰ See *supra* note 6.