**Before the**
**FEDERAL COMMUNICATIONS COMMISSION**
**Washington, D.C. 20554**

| | | |
|---|---|---|
| In the Matter of<br><br>Authorizing Permissive Use of the "Next Generation" Broadcast Television Standard | )<br>)<br>)<br>)<br>) | GN Docket No. 16-142 |

**REPLY COMMENTS OF ATSC 3.0 SECURITY AUTHORITY LLC ("A3SA")**

Gerard J. Waldron
Kiara Ortiz
Covington & Burling, LLP
850 Tenth Street, N.W.
Washington, D.C. 20001

*Counsel for ATSC 3.0 Security Authority LLC*

February 18, 2026

## Summary

The ATSC 3.0 transition is reaching a critical moment and the record now makes clear that content protection, which includes tools such as encryption and digital rights management ("DRM"), is a necessary component of the NextGen TV framework. Premium sports, live events, and marquee programming increasingly require content protection as a condition of distribution. If over-the-air ("OTA") broadcasting is to remain a viable platform for this high-value content, broadcasters must be able to deploy the same standards-based security tools that competing Internet Protocol-based ("IP-based") platforms have used for years.

The record reflects broad consensus among broadcasters, networks, and content owners – including the National Association of Broadcasters, Gray Local Media, E.W. Scripps Company, Sinclair, and the Motion Picture Association – that content protection is essential to deterring escalating piracy threats and securing the programming that anchors the value of television broadcasting. Without it, broadcasters face a growing risk that premium programming will migrate to platforms better equipped to meet content-owner requirements. The ATSC 3.0 Security Authority ("A3SA") submits these comments to urge the Commission to recognize content protection as a core element of the ATSC 3.0 ecosystem.

Today, *more than 18 million ATSC 3.0-capable receivers are in the market, and nearly all of them are able to successfully receive and display encrypted broadcasts, without requiring an Internet connection*. Claims that content protection restricts consumer access are inconsistent with this real-world experience. Some individual commenters focused on isolated, outdated, or device-specific examples but these anecdotes do not reflect current receiver performance or the operation of the ATSC 3.0 security system as deployed today.

A3SA's reply comments also clarify some glaring flaws in certain comments filed in response to the *Fifth Further Notice of Proposed Rulemaking*. First and foremost, content protection does not impede the delivery of Emergency Alert System or public-safety messaging. ATSC 3.0 was designed to support enhanced emergency alerting across protected and unprotected streams alike. Content protection also does not alter broadcasters' obligation to provide a free, OTA programming stream or change the statutory character of broadcasting under the Communications Act.

Finally, completing the ATSC 3.0 transition requires certainty across the broadcast ecosystem. A3SA – acting in its limited, neutral role as administrator of the ATSC 3.0 security policy – has nonetheless enabled millions of devices to implement the security features embedded in the ATSC 3.0 standard. Thus, we urge the Commission to recognize that content protection is integral to ATSC 3.0 and provide the certainty needed to accelerate device availability, encourage broader manufacturer participation, and ensure the long-term competitiveness and sustainability of free, OTA television.

## TABLE OF CONTENTS

**Before the**
**FEDERAL COMMUNICATIONS COMMISSION**
**Washington, D.C. 20554**

| | | |
|---|---|---|
| In the Matter of<br><br>Authorizing Permissive Use of the "Next Generation" Broadcast Television Standard | ) | GN Docket No. 16-142 |

**REPLY COMMENTS OF ATSC 3.0 SECURITY AUTHORITY ("A3SA")**

## I. Introduction

Free, over-the-air ("OTA") television remains an essential source of premium sports, entertainment, news, and emergency information for many American households, and the ATSC 3.0 (or NextGen TV) transition will ensure broadcasters can use Internet Protocol-based ("IP-based") technology to deliver this high-value content and succeed in today's vibrant media marketplace. As ATSC 3.0 Security Authority's ("A3SA") initial comments explain, broadcasters are competing with Big Tech platforms for high-value content and content owners increasingly demand suitable content protection from their distribution partners. In this environment, where the largest U.S. pay-TV provider (YouTube TV) is owned by one of the largest technology companies in the world, broadcasters must be able to compete to preserve high-value programming on free, OTA television. The ATSC 3.0 standard approved by the Federal Communications Commission ("Commission" or "FCC") in 2017 provides broadcasters with the same security capabilities long used by streaming platforms to combat piracy and protect premium content.[1] The threat of piracy is greater today than ever, and even more so for

[1] *Authorizing Permissive Use of the "Next Generation" Broadcast Television Standard*, Report and Order and Further Notice of Proposed Rulemaking, 32 FCC Rcd 9930, 9931 para. 1 (2017) ("*NextGen TV First Report and Order*").

live events such as the Super Bowl or March Madness. To keep broadcast television a viable distribution mechanism for this programming and combat the associated piracy, broadcasters need the same tools used by Big Tech. In adopting rules to facilitate the final transition to ATSC 3.0, the Commission must preserve the ability of broadcasters to use content-protection technology and facilitate its incorporation in the broadcast experience.

Parties who are committed to the continuation of free, OTA broadcasting have embraced this point. Major broadcasters and content owners – including the National Association of Broadcasters ("NAB"), Gray Local Media, Inc. ("Gray Media"), E.W. Scripps Company ("Scripps"), Sinclair Inc. ("Sinclair") as well as the Motion Picture Association ("MPA") – confirm that content protection is critical to securing premium programming and are being deployed in a manner that renders free, OTA service.[2] They emphasize that content protection is needed to deter escalating piracy threats and support the continued viability of local broadcasting.

Experience shows that over 99% of the 18.5 million NextGen receivers in the market today – including receivers from Samsung, Sony, TCL, Hisense, Panasonic, and several small device manufacturers – have implemented A3SA content-protection technology and receive and display protected ATSC 3.0 signals. Some commenters misleadingly highlight the one percent

[2] *See* Comments of the National Association of Broadcasters, GN Docket No. 16-142 (Jan. 20, 2026), https://www.fcc.gov/ecfs/document/10120155408928/1 ("NAB Comments"); Comments of Gray Local Media, Inc., GN Docket No. 16-142 (Jan. 20, 2026), https://www.fcc.gov/ecfs/document/10121298925745/1 ("Gray Media Comments"); Comments of the E.W. Scripps Company, GN Docket No. 16-142 (Jan. 20, 2026), https://www.fcc.gov/ecfs/document/10120254696497/1 ("Scripps Comments"); Comments of the Motion Picture Association, Inc., GN Docket No. 16-142 (Jan. 20, 2026), https://www.fcc.gov/ecfs/document/101202454406914/1 ("MPA Comments"). *See also* Comments of Sinclair Inc., GN Docket No. 16-142 (May 7, 2025), https://www.fcc.gov/ecfs/document/1050739202137/1.

of the 1% - the edge cases where a small number of devices from smaller manufacturers of "accessory" devices (e.g., set top boxes, DVRs, and home gateways) have experienced isolated difficulties that have since been corrected. As we explain below, some of the examples cited are obviously from a few years ago and do not reflect the software iteration and update process that manufacturers use to bring a product to market. And some claims reflect a misunderstanding of how ATSC 3.0 content protection functions. Thus, the overwhelming majority of devices in the market today - over 99% - work for consumers and demonstrate full compatibility with longstanding expectations for free, OTA broadcasting. A3SA stands ready to support the ecosystem by quickly addressing any future technical issues that might arise.

Deployment of ATSC 3.0, with its IP foundation, is a major undertaking for broadcasters, and as noted above it brings major benefits. Unlike Big Tech companies, which have been using IP-based content protection for *decades,* broadcasters did not have the same IP-based content-protection infrastructure available to them until relatively recently. Then in 2019, to fill that gap, A3SA was formed by Pearl TV (a coalition of the largest owners of affiliated stations) and the major broadcast networks, to develop a content-protection solution to protect ATSC 3.0 broadcast signals across both connected (Internet-connected) and unconnected (non-Internet-connected) devices. A3SA's role is narrow and serves simply to facilitate the use of content protection for both broadcasters and device manufacturers. As explained in A3SA's initial comments, A3SA provides neutral verification tools and credential administration so that broadcasters and device makers can implement ATSC 3.0's security features. It bears emphasis that A3SA has a limited scope: it does *not* require encryption, it does *not* dictate broadcaster content protection deployment decisions, and does *not* pick marketplace outcomes. Indeed, A3SA actively encourages device manufacturers to enter the ATSC 3.0 market, recognizing that

broader participation benefits consumers and broadcasters alike and, in a robust marketplace, creates meaningful revenue opportunities for manufacturers.

In sum, the Commission should recognize content protection as an essential part of the NextGen TV framework for the broadcast industry to succeed. Below, we address some points that were raised in comments submitted in response to the *Fifth Further Notice of Proposed Rulemaking* ("*Fifth Further Notice*")[3] and reiterate the request that the Commission adopt a unified encryption approach using the existing ATSC 3.0 standards to ensure a secure, interoperable, and future-proof environment for broadcasters, device manufacturers, and viewers.

## II. Content Protection Strengthens Broadcast Programming and Works Well with Consumer Access

### A. Content Protection Is Essential to Securing High-Value Programming

As several parties commented, content protection as part of ATSC 3.0 rests on two well-established technical components used by many IP-based technologies today: encryption and digital rights management ("DRM").[4] Encryption defeats unauthorized interception or redistribution by mathematically scrambling the broadcast content into unreadable data, whereas the integrated DRM system supplies authorized devices with the keys needed to reverse that process to present the content to the viewer. When an A3SA-compliant device receives encrypted OTA content, it automatically uses its built-in DRM keys to decrypt and display the programming, without any change in picture or sound quality, and without requiring an Internet connection. Put simply, these technologies work together to provide the ATSC 3.0 signal with a

[3] *Authorizing Permissive Use of the "Next Generation" Broadcast Television Standard*, Fifth Further Notice of Proposed Rulemaking, GN Docket No. 16-142, FCC 25-72, 90 FR 52327 (adopted Oct. 29, 2025) ("*Fifth Further Notice*").

[4] Comments of the ATSC 3.0 Security Authority, GN Docket No. 16-142 at 7-8 (Jan. 20, 2026), https://www.fcc.gov/ecfs/document/10121096038274/1 ("A3SA Comments"); *See also* Gray Media Comments at Part VI; Scripps Comments at Part III; NAB Comments at Part IV.

modern, IP-based content protection system comparable to what streaming platforms have used for decades, while still preserving free, OTA access and safeguarding premium content with and without an Internet connection.

The record reflects broad agreement that broadcasters need content protection to continue securing high-value programming for delivery to the large number of consumers who continue to rely on OTA signals. NAB explains that encryption "protects the core business model of broadcast television and the principles inherent in Congress's retransmission consent regime."[5] Scripps emphasizes that DRM requirements "are increasingly required in licensing terms between local broadcast stations and their programming partners, including major networks, sports-rights holders, syndicators, and others who want to ensure that their programming is delivered and received securely across varied platforms – including via free, over-the-air broadcasting."[6] Gray Media adds that "getting DRM right is critical to the ability of Gray and other broadcasters to secure the content their viewers want to see."[7] These statements reflect a clear consensus that without reliable, interoperable content protection, broadcasters risk losing access to the premium programming that anchors the value of local and free, OTA broadcasting.

#### i. The Rising Threat of Digital Piracy Highlights Need for Broadcasters to Use Robust Content-Protection Tools

The rising threat of digital piracy highlights the need for broadcasters to use robust content-protection tools. The MPA explains that "sports, premium episodic television, and live events are high-value targets for piracy because they air first in broadcast windows and have

[5] NAB Comments at 16.

[6] Scripps Comments at 11.

[7] Gray Media Comments at 18.

*immediate* viewing demand."[8] Live sports – such as the Super Bowl, March Madness, Major League Soccer, PGA tournaments, and other high-profile events – are among the most heavily-pirated programming.[9] The MPA explains that piracy "devalues programming not only for purposes of distribution via broadcast television, but also when it is subsequently distributed via streaming or traditional pay-TV services."[10] In light of this ever-present threat, content owners by necessity "consider the content protection available on a given platform in determining where to air valuable programming."[11] According to Gray Media, "an *estimated 17 million people watched the 2024 Super Bowl via pirate streams,*" and Gray Media further notes that, according to major sports leagues (NFL, NBA, and UFC), "piracy costs the sports industry $28 billion per year."[12] A 2025 study further highlights the severity of the trend: 69% of sports fans in the United States and Europe now report turning to illegal streams, driven in part by fragmented access to live events on streaming platforms.[13] The Commission should understand that the harm extends beyond lost revenue. Consumers who turn to illicit streaming sites face significant

[8] MPA Comments at 3 (emphasis added).

[9] *See e.g.* Larissa Knapp, *The Hidden Cost of Live Sports Piracy – and how we fight back*, Alliance for Creativity and Entertainment (Sept. 9, 2025), https://www.alliance4creativity.com/blog/the-hidden-cost-of-live-sports-piracy-and-how-we-fight-back/; *See also* Brett Danaher, Michael D. Smith, and Rahul Telang, *Pro Sports Has a Piracy Problem*, Harvard Business Review (Feb. 14, 2024), https://hbr.org/2024/02/pro-sports-has-a-piracy-problem.

[10] MPA Comments at 3.

[11] *Id*.

[12] Gray Media Comments at 18-19 (emphasis added). *See also* Danaher, et al., *Pro Sports Has a Piracy Problem*.

[13] In 2025, 4.7 million U.K. adults used illegal sports streams, which drew 1.6 billion views in the first half of the year, while 58% of fans deemed the practice socially acceptable. Erik Gruenwedel, *Illegal Live Sports Streaming Flourishing Despite Industry Crackdowns*, Media Play News (Jan. 27, 2026), https://www.mediaplaynews.com/illegal-live-sports-streaming-flourishing-despite-industry-crackdowns/.

security risks. OpenText Security Solutions found that nearly every illegal streaming service exposes users to malicious or misleading content, including "malware, spyware, phishing [attacks], junk security software, explicit content, fake operating systems, and related online scams."[14]

The threat of piracy to broadcasters has long been recognized and has caused significant harm to the industry, resulting in long and expensive (yet successful) litigation. NAB explains that "services such as Aereo and Locast," which unlawfully retransmitted local broadcast stations over the Internet, "were built on the premise that broadcast signals, because they were unprotected, could be captured, repackaged, and redistributed without authorization or compensation."[15] Why could Aereo and Locast so brazenly break the law, as determined by multiple courts? Because high-value broadcast content was not protected. NAB persuasively argues that "encryption would have prevented these services from launching in the first place, avoiding disruption to viewers and preserving the integrity of local broadcast."[16]

These pressures are compounded by rapid shifts in the modern media marketplace. High-value programming that once aired exclusively on free, OTA television is increasingly migrating to Big Tech platforms. The Oscars will be carried exclusively on YouTube beginning in 2029; live sports now routinely appear on Amazon Prime Video, Apple TV, and YouTube TV; and many Emmy award-winning programs premiere solely on subscription services. If the Commission seeks to preserve the value and long-term viability of free, OTA broadcasting, it

[14] *Id*. *See also The Hidden Threats Lurking on Illegal Streaming Sites*, OpenText Security Solutions, https://www-cdn.webroot.com/9516/6265/6764/Webroot-Report-The-Hidden-Threats-Lurking-on-Illegal-Streaming-Sites_2.pdf.

[15] NAB Comments at 16.

[16] *Id*.

must ensure that broadcasters have the tools needed to compete for and retain this content. Content protection is one of those tools.

One commenter, Mr. Tyler Kleinle (a YouTube blogger who bills himself as "Antenna Man") claims that DRM is "unnecessary" because certain sports leagues currently have multi-year broadcast agreements.[17] This is simplistic and misses the point. His assertion does not appear to be based on any real-world experience with such agreements, instead relying on press announcements.[18] This unfounded claim ignores clear trend lines showing the migration of sports rights to digital platforms and overlooks the contractual expectations in those same broadcast agreements that require, encourage, or anticipate that broadcasters will protect content when capable of doing so. When ATSC 3.0 was first proposed, sports events on streaming platforms were the outlier; today they are the norm.

The real question is not whether broadcasters carry premium content today, but whether they will be able to keep it in the near future. As major sports league renewals approach, including portions of the current NFL rights expiring as early as 2029, it is necessary for broadcasters to use content protection tools when transmitting high-value programming.[19] Far

---

[17] Comments of Tyler Kleinle, Antenna Man LLC, GN Docket No. 16-142 at 10 (Jan. 20, 2026), https://www.fcc.gov/ecfs/document/10116201806975/1 ("Antenna Man Comments").

[18] *Id*. *See also* Reply Comments of Lon Seidman, GN Docket No. 16-142 at 4 (Jan. 30, 2026), https://www.fcc.gov/ecfs/document/1013019127432/2. ("Seidman Reply Comments") (claiming in paragraph V that "[a]ll of these [new broadcast deals with major sports leagues] were made with no encryption mandate or certainty that ATSC 3.0 will be mandated during the length of those agreements.").

[19] *See* Mike Florio, *Report: NFL Could Attempt to Extend Media Deals Before 2029*, NBC Sports: ProFootballTalk (July 8, 2025), https://www.nbcsports.com/nfl/profootballtalk/rumor-mill/news/report-nfl-could-attempt-to-extend-media-deals-before-2029. *See also NFL Considers Early Broadcast Deal Renegotiation Before 2029 Opt-Out*, RealGM: Football Wiretap (July 8, 2025), https://football.realgm.com/wiretap/53021/NFL-Considers-Early-Broadcast-Deal-Renegotiation-Before-2029-Opt-Out.

from being speculative or optional, these measures respond directly to documented, rapidly escalating threats to the economic viability of broadcasting and to consumer safety alike. The Commission should be skeptical of claims that content protection is "unnecessary" for premium sports programming coming from persons who have no knowledge beyond limited trade press reports and instead should credit those on the front-line of these discussions.

### B. Claims That Content Protection Blocks Consumer Access Are Out of Touch With the Current Reality

There are 18.5 million ATSC 3.0 receivers in the market today, a number that is growing every day, and over 99% are capable of receiving and displaying protected ATSC 3.0 content for the enjoyment of consumers. Ignoring this overwhelming majority of devices, a few commenters seek to get the Commission to focus on the corner cases – the one percent of 1% that arguably experienced technical issues. Broadcasters want to reach 100% of the audience, so we will address those claims, though many are outdated or simply wrong. But the Commission should view these claims in the context of the 99% of devices that are working for consumers, just as expected.

One individual commenter claims that ATSC 3.0's content protection system "locks" viewers out from accessing free, OTA television.[20] That is simply not true. The comments rely on outdated information and misconstrue how the A3SA system works. Specifically, the comments use outdated screenshots to suggest that encryption blocks reception today.[21] For example, the commenter presents a screenshot of a ZapperBox device running software from 2023. This ignores the fact that ZapperBox implemented support for protected ATSC 3.0 content in late 2023, and the on-screen message referenced in the filing was subsequently removed from

[20] *See* Antenna Man Comments at 10.

[21] *Id*. at 6-10.

ZapperBox software via routine update in 2024 in version 2.7. The current software version of ZapperBox is 3.5.2. The representation of ZapperBox in these comments do not reflect current device operation.[22]

The same pattern appears in other examples this individual raises, including with the Zinwell ZAT-600b. The Zinwell set top box issue referenced has already been resolved. Gray Media and Channel Master engineers investigated the issue and resolved it promptly in 2024. The other devices cited similarly rely on outdated information; those manufacturers have since issued firmware updates and released new devices that fully address the earlier problems.

As a general matter, newly introduced consumer electronics devices are well known to exhibit more issues during the early stages of market introduction, which are subsequently addressed by manufacturers, and this naturally applies equally to television receivers as well. Manufacturers have continued to harden and refine their ATSC 3.0 implementations generally, including their implementation of A3SA's content-protection solution. Receiver reliability has improved over time as integrations mature, and firmware updates continue as part of standard lifecycle management, with the release frequency of these updates slowing compared to earlier deployment phases.

Some individual commenters make similar incorrect claims, but the Commission should not allow itself to be misled. For example, two individuals falsely claim that "A3SA refuses to certify" HD HomeRun (the device manufactured by Silicondust).[23] That is not true. The process for A3SA approval is communicated clearly in writing to device manufacturers promptly upon becoming an A3SA licensee, and Silicondust received that as an A3SA licensee. Here is the

[22] *See* ZapperBox Release Notes, https://zapperbox.com/pages/release-notes.

[23] Antenna Man Comments at 5. *See also* Lon Seidman Reply Comments at 4.

process. First, device manufacturers develop a product and conduct their own conformance testing to demonstrate that they meet the technical specifications. Second, the device manufacturers submit their test results to A3SA for verification confirming the device's compliance, which then results in approval to access production DRM services. Third, after the device has been introduced in the market, A3SA purchases a device at retail and spot checks the device for compliance. While A3SA cannot speak to what internal product development they have or have not done, Silicondust has certainly not completed submission of test results. Silicondust has never requested A3SA verification or approval for their HD HomeRun device, despite having been a licensee of the A3SA technology since March of 2022. And Silicondust clearly has never released a product with A3SA content protection to consumers. A3SA wishes it were otherwise, since A3SA worked closely with Silicondust through February 2024, and they contributed meaningfully to the A3SA Local Content Protection ("ALCP") specifications, which specifically address concerns raised by Silicondust. Until recently, Silicondust was also a member of the A3SA Technical Contributors Working Group ("TCWG") – a collaborative forum chaired by an A3SA-licensed device manufacturer and composed of at least a dozen TV and device manufacturers who help shape A3SA's technical specifications. Whenever Silicondust is ready to move forward, A3SA stands ready to work with them, and is eager to engage with other manufacturers to review test results and support the development of A3SA-compliant solutions that expand the ATSC 3.0 ecosystem and benefit consumers.

Contrary to the isolated claims by some commenters, the real-world experience is that early device quirks have been resolved through firmware updates or new models, and A3SA has seen no significant wide-spread non-compliance among A3SA-enabled devices available today in the market. Scripps describes the situation accurately: "failures in some early models of

consumer devices to properly implement DRM should therefore not be treated as an inherent issue with DRM itself."[24] Moreover, Scripps is right to point out the issues cited in the record stem from how content protection has been implemented in certain devices – particularly by smaller manufacturers – rather than from any deficiency in the content-protection solution itself: "DRM should not be conflated with DRM implementation in consumer devices."[25]

As A3SA and others explained in the initial comments, the content-protection mechanisms are designed to work with all devices right out of the box, whether they are connected to the Internet or not. Public Knowledge suggests that viewers need an active Internet connection to receive "DRM updates or access important features,"[26] falsely implying that DRM updates with an Internet connection or another connectivity method are unique to DRM. The A3SA content-protection solution was deliberately developed, using creative engineering solutions, so that it would display protected OTA signals in receivers with, and without, an Internet connection. It should be noted the ATSC 3.0 specification allows software updates to occur OTA in a non-real-time data stream for software updates, consumer enhancements, and DRM updates, and the Commission can expect this functionality to develop further as the ATSC 3.0 market matures. Receivers and set top or converter boxes supporting content protection are being built and sold today with A3SA credentials pre-installed, ensuring that they work without

[24] Scripps Comments at 12.

[25] *Id.*

[26] Comments of Public Knowledge, Consumer Reports, Electronic Frontier Foundation, Electronic Privacy Information Center, Media Council Hawaii, Open Technology Institute at New America Comments, GN Docket No. 16-142 at 6 (Jan. 20, 2026), https://www.fcc.gov/ecfs/document/101202300720591/1 ("Public Knowledge Comments").

an Internet connection.[27] In sum, households without broadband receive the same protected programming as connected homes.

As part of ongoing monitoring, A3SA has been assessing ATSC 3.0 televisions from major manufacturers to confirm they receive and can display encrypted signals out of the box. All the tested models have received and displayed live A3SA-protected ATSC 3.0, broadcasts OTA both with and without an Internet connection. These results confirm that content protection does not impede reception on modern A3SA-compliant receivers and that any remaining issues are attributable to device-specific implementation, not encryption.

One final note: while it is convenient to blame any glitch in a device on DRM or encryption, the reality is that content protection frequently has nothing to do with the typical software issues users experience in many new devices, particularly from innovative manufacturers. It is not unusual for software-based devices (e.g., smart TVs with or without ATSC 3.0 functionality, set top boxes, cell phones, computers), especially new ones, to require occasional software updates for bug fixes, product enhancements, and security improvements. When these devices fail to render protected broadcasts correctly, the cause is almost always manufacturer-specific implementation rather than the underlying content protection. Because there is no end date for ATSC 1.0, the ATSC 3.0 accessory device market-segment in particular remains small – perhaps as many as 100,000 devices (less than 1% of all 18.5 million ATSC 3.0 capable devices) – and includes manufacturers with limited engineering resources who face various implementation challenges unrelated to content protection. Even today, A3SA recognizes that some devices currently in the market continue to undergo routine software

[27] It bears mention that many of these devices are designed specifically to utilize an Internet connection to populate program guides and to access streaming services that also reside on the device as well as to provide necessary software updates and to improve the user experience.

refinement, including improvements to content protection support and other non-content protection functionality. We recognize that such disruptions are frustrating for affected consumers and also for broadcasters, and A3SA's goal is that all A3SA-compliant devices work at all times.

A3SA has monitored manufacturer performance and provides guidance where helpful, but the recent implementation issues reinforce the broader point: manufacturers, especially smaller manufacturers entering a new technical space, need resources and predictable regulatory frameworks to refine their engineering processes and ensure consistent performance. As Scripps correctly notes, "DRM hinges on successful implementation by device manufacturers."[28] While the overwhelming 99% of devices are working today, more clarity around the NextGen TV framework will encourage smaller manufacturers to focus their engineering resources on resolving any outstanding issues.

### C. Addressing Key Considerations Related to Content Protection

#### i. Emergency Alerts and Public Safety Information Work Seamlessly with Content Protection

Local news, weather information and emergency alerts are central to the broadcast industry's public interest mission and ATSC 3.0 content protection works seamlessly with that mission. ATSC 3.0 was designed to support and enhance public safety capabilities, including advanced emergency alerting features. *The Commission should be clear that: content protection works seamlessly with the emergency alerting systems and it does not impede, limit, or affect the reception of Emergency Alert System messages or other critical public-safety information*. In fact, the Advance Warning and Response Network ("AWARN") Alliance confirms that content

[28] Scripps Comments at 2.

protection "does not in any way impede the delivery" of emergency alerting or public-safety messaging, and that more than 18 million households with NextGen TV receivers can access "all NEXTGEN TV content, whether encrypted or not, without needing an Internet connection or subscription."[29] And beyond this technical reality, broadcasters have every incentive – both legal and reputational – to ensure that emergency alerts remain universally accessible across every stream, protected or not.

**ii. MVPD Claims Misunderstand How ATSC 3.0 Signals Are Delivered**

Concerns raised by the pay-TV industry are similarly misplaced. The American Television Alliance ("ATVA") asserts that A3SA's role in an encryption scheme would introduce "additional technical challenges" and "increase the costs of consumer devices by about $10 to $20 for each A3SA-capable unit."[30] ATVA further claims that "A3SA encryption prevents MVPDs from passing through broadcast signals because the encrypted signals cannot travel through untrusted headend equipment," that MVPDs would need to "completely redesign their hardware systems," and that A3SA encryption "adversely impacts" MVPD features such as "DVR functionality, multiscreen access, and network-based storage."[31] NCTA – The Internet & Television Association ("NCTA") similarly argues that encryption "adds further complexities and costs," asserting that MVPDs would need access to decryption keys and additional information in order to process the signal.[32]

---

[29] Comments of AWARN, GN Docket No. 16-142 at 2 (Jan. 20, 2026), https://www.fcc.gov/ecfs/document/10120353825757/1.

[30] Comments of the American Television Alliance, GN Docket No. 16-142 at 7 (Jan. 20, 2026), https://www.fcc.gov/ecfs/document/101202352023382/1 ("ATVA Comments").

[31] *Id*. at 7-8.

[32] Comments of the NCTA – The Internet & Television Association, GN Docket No. 16-142 at 10 (Jan. 20, 2026), https://www.fcc.gov/ecfs/document/1012196557527/1.

These claims misunderstand how encrypted ATSC 3.0 signals are handled in MVPD environments. In practice, A3SA-encrypted broadcasts are demodulated and decrypted in an ATSC 3.0 edge cable headend receiver, such as the Synamedia MEG or the Wisi VMA-AT3 from Inca networks (both A3SA-compliant devices), upon OTA reception. After this point, the signal is no longer encrypted. It then moves through the MVPD's network in the same unencrypted form that cable systems have used for many years when carrying decrypted satellite and IP-delivered channels. As a result, by the time the signal reaches an MVPD subscriber's device, the content is already decrypted and the same consumer devices used today can receive the broadcast without incurring any additional device costs. Because MVPDs have access to decrypted broadcast signals, all existing MVPD service features should remain fully available, including DVR functionality, multiscreen access, and network-based storage. It is notable that ATVA objects to broadcasters delivering encrypted signals to viewers, even though cable operators routinely deliver the same broadcast signals to their subscribers in encrypted form.

#### iii. Primary-Stream Protection is Consistent With How Broadcasters Deliver High-Value Content

Public Knowledge argues that content protection should not be permitted on the primary video stream.[33] But the notion that the most important, most valuable, and most widely viewed content – which almost always appears on the primary stream – should be the only content that cannot be protected would disadvantage consumers. The record shows that premium programming such as live sports and marquee entertainment increasingly require strong content protection tools. Allowing protection on secondary, less-watched streams while barring it on the very stream that carries the highest-value programming is backwards.

[33] Public Knowledge Comments at 10.

Moreover, there is no valid basis for treating the primary stream differently. If the concern is ensuring that viewers receive an accessible free, OTA service, the FCC already mandates that outcome, by requiring broadcasters to continue providing one free OTA video programming stream.[34] Content protection does not change that obligation. And if the concern is preserving the programming that consumers value most, then it is precisely the primary stream that reasonably requires content protections.

### D. Content Protection Does Not Change the Fundamental Nature of ATSC 3.0 Broadcasting

ATSC 3.0 transmissions that use content protection (encryption and DRM) are – and remain – "broadcasting" under the Communications Act. Broadcasting is defined as the dissemination of radio communications "intended to be received by the public," and the Commission has always applied that definition by examining whether programming is publicly receivable, not whether it incorporates modern content protection features.[35] The Commission has also identified three circumstances in which a service is not broadcasting: when (1) it requires specialized equipment; (2) encryption renders programming unusable by the public; or (3) it is delivered through a private contractual relationship with viewers.[36] As detailed in A3SA's initial comments, ATSC 3.0 with content protection satisfies the statutory definition because protected signals are received on ordinary, commercially available ATSC 3.0 televisions

---

[34] *See NextGen TV First Report and Order*, 32 FCC Rcd at 9935, para. 9 (". . . requiring Next Gen TV stations to provide one free, over-the-air video programming stream broadcast in ATSC 3.0").

[35] 47 U.S.C. § 153(7).

[36] *See NextGen TV First Report and Order*, 32 FCC Rcd at 9935, para. 9. *See also Subscription Video Services*, Report and Order, 2 FCC Rcd 1001, 1006 para. 41 (1987) (concluding that subscription TV and DBS services are not "broadcasting" within the meaning of the Communications Act), aff'd, *National Association for Better Broadcasting v. FCC*, 849 F.2d 665, 669 (D.C. Cir. 1988).

and set top boxes; no specialized equipment, subscription, or login is required; and viewers continue to receive one free, OTA program stream as the rules require.[37]

The Commission emphasized this point in 2017 when it concluded that NextGen TV stations "will be engaged in broadcasting" based on the expectation that ATSC 3.0-capable television receivers would become widely available. [38] Today's robust marketplace – with 18.5 million ATSC 3.0-capable devices sold at retail – only reinforces that finding. The Digital Television ("DTV") transition underscores this point. When broadcasters were operating in both analog and digital (ATSC 1.0 standard), the Commission classified DTV as broadcasting (in addition to analog television) and never treated ATSC 1.0 tuners as specialized equipment. Transitional device availability has never dictated whether a service qualifies as "broadcasting," and it does not do so in the ATSC 3.0 context.

Public Knowledge argues that "the use of DRM… render[s] encrypted ATSC 3.0 transmissions distinct from traditional broadcasting" in part because broadcasters "require viewers to use devices certified by the ATSC 3.0 Security Authority," which supposedly introduces "contractual conditions that broadcast participants must accept to access what has historically been a free and open medium."[39] That framing is mistaken. First, content protection is optional. It is each broadcaster's choice whether to encrypt its streams or not. Second, content protection does not render programming unusable by the public as more than 18 million compliant receivers – and counting – automatically decrypt protected signals without any viewer action, exactly as with unprotected broadcasts. Lastly, there are no "contractual conditions"

[37] *NextGen TV First Report and Order*, 32 FCC Rcd at 9935, para. 9.

[38] *Id*.

[39] Public Knowledge Comments at 27-28.

required of viewers.[40] A3SA is a technology licensing entity that provides optional content protection specifications and verification services for broadcasters and device manufacturers. The use of content protection does not in any way convert free, OTA television into a subscription service for which consumers must sign a contract. Therefore, content protection does not change the nature of ATSC 3.0 broadcasting, it simply provides the security capabilities needed to safeguard content against piracy while preserving universal public access.

### E. A Unified Encryption Approach is Necessary to Ensure Interoperability and Long-term Stability

A3SA reiterates its support for a unified, standards-based encryption approach within the existing ATSC 3.0 framework to promote interoperability, spectral efficiency, and consumer clarity. As explained in A3SA's initial comments, the ATSC DRM Recommended Practice (A/362) already provides a clear path forward through Common Encryption ("CENC"), which allows a single encrypted broadcast stream to utilize multiple DRM systems for decryption key delivery.[41] Absent a unified approach, broadcasters may be forced to transmit multiple encrypted versions of the same content to accommodate different devices, undermining the efficiency gains ATSC 3.0 was designed to deliver and increasing complexity for manufacturers. A unified encryption method, implemented through existing ATSC standards, ensures that protected ATSC 3.0 broadcasts remain broadly accessible, interoperable, and future-proof, while enabling broadcasters to meet content-owner requirements and preserve free, OTA service.

[40] *See Id*.

[41] *See* A3SA Comments at 13.

## III. A3SA's Provision of Technical Verification and Certificate Administration Does Not Constrain the Market But Rather Seeks to Maximize Participation

A small group of commenters suggest that A3SA's administration of certificates, DRM credentials, and compliance tests grants A3SA control over which devices function with protected ATSC 3.0 signals, or otherwise creates a central point of control over market access. These concerns misapprehend A3SA's role.

A3SA is comprised of broadcasters. The broadcast industry would be significantly better off if the TV receiver market were filled with a plethora of compliant receivers across a range of price points. The reason this would be good for broadcasters is that it would be good for consumers. Accordingly, A3SA has every incentive to encourage and facilitate the availability of compliant devices and actively works with a variety of manufacturers towards that goal. Commenters like Weigel and ATVA would have the Commission believe that A3SA is sabotaging its own goal.

As explained previously, A3SA stepped up to create a unified, neutral provider of standard tools, test suites, and certificate resources so broadcasters could protect their ATSC 3.0 broadcast signals because no one else was meeting the need. Weigel now complains that it wishes other entities would provide various ATSC 3.0 security components since A3SA "cannot easily be bypassed, because doing so would require working out separate agreements with every device manufacturer."[42] While A3SA spent significant time, money, and energy establishing a solution for licensing security technology components to device manufacturers and other industry participants, it would welcome new contributors of security components to the industry.

[42] Comments of Weigel Broadcasting Co., GN Docket No. 16-142 at 27 (Jan. 20, 2026), https://www.fcc.gov/ecfs/document/1012077377468/1 ("Weigel Comments").

Public Knowledge similarly errs in its claims that manufacturers "must obtain A3SA verification, comply with confidential licensing terms, pay fees, and implement Google's Widevine DRM" to manufacture an ATSC 3.0 device.[43] A3SA implementation (and therefore its verification) is not required to manufacture an ATSC 3.0 device; manufacturers are free to use alternative content protection technologies once they appear. In the same vein, Google's Widevine DRM was initially selected because it was the first widely deployed system capable of securely delivering and managing DRM licenses (with the associated CENC decryption keys) *without requiring an Internet connection*, thereby providing broadcasters with a reliable foundation for ATSC 3.0 content protection. As the market continues to mature, A3SA is now actively vetting additional DRM solutions beyond Widevine, including Apple FairPlay and Microsoft PlayReady.

What Weigel and others ignore is that some 18.5 million receivers have been sold by various manufacturers, which is evidence that the system is currently working well. Major global brands – including Sony, Samsung, Hisense, TCL, and Panasonic – and established new entrants such as BitRouter, ADTH, Zinwell, and GT Media already ship devices with factory-installed support for receiving A3SA credentials and decrypting protected ATSC 3.0 content out of the box. A3SA is also aware of several smaller manufacturers that have already developed ATSC 3.0-capable devices with A3SA compatibility, and they have expressed the need for Commission action in this proceeding to support their entrance into the market. This shows that the growing level of manufacturer engagement would not exist if A3SA were restricting access or imposing unreasonable requirements.

[43] Public Knowledge Comments at 32.

*Signal Security*. Weigel also lumps its objections to content protection with concerns about signal security.[44] For clarity, content protection and signal security (via signing) are two different and unrelated technologies. The ATSC 3.0 standard requires OTA signaling to be digitally signed (for example, via a certificate), which then enables a consumer's device receiver to confirm for the consumer that the signal is from a trusted source and has not been subjected to tampering or hijacking. Contrary to Weigel's suggestion, A3SA does not require receiver manufacturers to include a switch that causes the receiver to "go dark" if a non-signed signal is encountered. [45] To the contrary, devices may respond flexibly to incorrectly signed signals. [46] A3SA requires only that devices notify consumers that a signal is improperly signed, so the consumer may choose for themselves how to act.

Overall, broadcasters and consumers would benefit from greater participation by additional certificate suppliers and device manufacturers. The limited number of market participants today reflects the early stage of the ecosystem rather than any limitation in A3SA's framework, and increased device demand would naturally support greater entry, competition, and more tailored solutions.

## IV. Conclusion

To ensure broadcasters can continue securing high-value programming and delivering it to viewers at no cost, the Commission should permit the use of content protection within

[44] Weigel Comments at 27.

[45] *Id*.

[46] As A3SA mentioned in initial Comments, the deadline for implementing signal security (aka "High Noon") was postponed indefinitely by A3SA in March 2025 and assures the Commission that A3SA does not anticipate reintroducing any sort of signal security deadline until certain conditions are met. *See* A3SA Comments at 29.

ATSC 3.0, including a unified encryption approach that ensures long-term interoperability and stability across the ecosystem.

Gerard J. Waldron
Kiara Ortiz
Covington & Burling, LLP
850 Tenth Street, N.W.
Washington, D.C. 20001

*Counsel for ATSC 3.0 Security Authority LLC*

February 18, 2026