

**Before the
Federal Communications Commission
Washington, D.C. 20554**

In the Matters of)	
)	
Amendment of Part 11 of the Commission's)	
Rules Regarding the Emergency Alert System)	PS Docket No. 15-94
)	
Wireless Emergency Alerts)	PS Docket No. 15-91

COMMENTS OF COMCAST CORPORATION

WILLKIE FARR & GALLAGHER LLP
1875 K Street, NW
Washington, DC 20006

Counsel for Comcast Corporation

Kathryn A. Zachem
Jordan B. Goldstein
James R. Coltharp
*Regulatory Affairs,
Comcast Corporation*

Francis M. Buono
Brian A. Rankin
Catherine Fox
*Legal Regulatory Affairs,
Comcast Corporation*

COMCAST CORPORATION
300 New Jersey Avenue, NW,
Suite 700
Washington, DC 20001

June 8, 2016

TABLE OF CONTENTS

I.	INTRODUCTION AND SUMMARY.....	1
II.	CERTAIN IP-BASED CABLE SERVICES ARE ALREADY SUBJECT TO EAS REQUIREMENTS, BUT THAT IS NO BASIS FOR APPLYING EAS REQUIREMENTS TO OTT SERVICES DELIVERED OVER THE INTERNET...4	4
III.	IT WOULD BE ARBITRARY AND CAPRICIOUS TO IMPOSE EAS OBLIGATIONS SOLELY ON THE OTT VIDEO SERVICES OF EAS PARTICIPANTS.....6	6
IV.	THE COMMISSION SHOULD REJECT ITS EAS SECURITY CERTIFICATION PROPOSAL.....10	10
V.	IP-FIRST DELIVERY IS THE LONG-TERM FUTURE OF EAS.....15	15
VI.	CONCLUSION	17

**Before the
Federal Communications Commission
Washington, D.C. 20554**

In the Matters of)	
)	
Amendment of Part 11 of the Commission’s Rules Regarding the Emergency Alert System)	PS Docket No. 15-94
)	
Wireless Emergency Alerts)	PS Docket No. 15-91

COMMENTS OF COMCAST CORPORATION

Comcast Corporation (“Comcast”) hereby responds to the above-captioned Notice of Proposed Rulemaking (“*Notice*”).¹ Comcast recognizes the vital importance of the emergency alert system (“EAS”) and looks forward to participating in the Commission’s efforts to ensure EAS remains effective, efficient, and secure as technologies evolve.

I. INTRODUCTION AND SUMMARY

The *Notice* appropriately looks to build a successful foundation for the long-term future of EAS. The Commission acknowledges the transformation of the video industry over the past several decades and seeks to “strengthen[] the nation’s public alert and warning systems” in the changed video landscape.² As an innovator in the dynamic video marketplace, Comcast welcomes the opportunity to share its insights into how the Commission can lead the way toward these goals.

The *Notice* invites comment on how EAS requirements should apply to IP-based platforms. As an initial and fundamental matter, the Commission should recognize that some

¹ *Amendment of Part 11 of the Commission’s Rules Regarding the Emergency Alert System; Wireless Emergency Alerts*, Notice of Proposed Rulemaking, 31 FCC Rcd. 594 (2016) (“*Notice*”).

² *Id.* ¶¶ 1, 88.

cable operators, such as Comcast, deliver Title VI *cable services* subject to EAS requirements using Internet protocol (“IP”) technology, and yet such IP cable services are distinct from IP video services *delivered over the Internet*. That EAS alerts are being delivered over IP cable services provides no basis for concluding that EAS requirements should be imposed with respect to *non-cable services delivered over the Internet*. Likewise, Comcast also believes that the Commission must continue distinguishing “programmed” channels subject to EAS obligations from other features and services offered by cable operators, such as interactive games, program guides, or Internet access, because this existing approach follows statutory language, tracks consumer expectations, and clearly delineates how EAS messages are to be delivered over cable systems.

The *Notice* also asks whether EAS obligations should apply to the over-the-top (“OTT”) video services offered by EAS Participants.³ It is far from clear whether the Commission has the authority to impose EAS requirements on OTT video services at all, but to the extent that the Commission believes it has jurisdiction to regulate the OTT video services of EAS Participants, it would be asserting jurisdiction to regulate *all* OTT video services, including those provided by edge providers. It would be arbitrary and capricious for the Commission to apply EAS obligations solely on OTT video services offered by EAS Participants. These OTT video services are edge services just like the OTT video services offered by Netflix, Hulu, and Amazon – services that the Commission has disclaimed any intent to regulate. In short, there is no sound legal or policy basis for imposing disparate alerting obligations simply because an edge service is affiliated with an EAS Participant. Adopting this approach would also create substantial consumer confusion by requiring EAS alerts over some OTT services but not others.

³ See 47 C.F.R. § 11.11(a) (defining “EAS Participant” by listing entities that must comply with EAS requirements).

Moreover, imposing EAS obligations on OTT video services is unwarranted. EAS alerts are not delivered via OTT video services today, so consumers have no expectation of receiving them in the online environment. And for those consumers who want to get alerts through online platforms, they already have a range of options to do so via social media and other online sources.

The Commission should reject the EAS security certification proposed in the *Notice*. As an initial matter, there is some question as to whether the anecdotal evidence cited in the *Notice* reveals industry-wide failures that would warrant such regulatory intervention. Moreover, the proposed certification regime would lock in a checklist of mandatory actions and impose significant costs on EAS Participants, thereby potentially *reducing* security as the mandatory actions become obsolete and overtaken by marketplace developments. The Commission should instead encourage EAS Participants to implement more flexible and appropriate risk-management strategies consistent with the Commission's broader approach to cybersecurity. To the extent the Commission nonetheless moves forward with the proposed certification regime, the Commission must afford strong confidentiality protection to all information collected through each certification.

The *Notice* also asks about the long-term future of EAS. The Commission should embrace an IP-first future for government delivery of EAS messages to EAS Participants over the Integrated Public Alert and Warning System ("IPAWS") and create a multi-stakeholder initiative to assist in finding solutions to issues raised by the migration to IP-first delivery. The broadcast daisy chain is a vital and needed EAS transmission line of defense, but it should be

considered a secondary line of defense with the primary focus on alert transmission via IP that offers many advantages over the daisy chain.⁴

II. CERTAIN IP-BASED CABLE SERVICES ARE ALREADY SUBJECT TO EAS REQUIREMENTS, BUT THAT IS NO BASIS FOR APPLYING EAS REQUIREMENTS TO OTT SERVICES DELIVERED OVER THE INTERNET.

The *Notice* correctly points out that there is a “wealth of video content . . . now available to consumers online” and that MVPDs “offer IP-based versions of their programming.”⁵ The *Notice* invites comment on the “potential issues with offering [EAS] alerts outside traditional broadcast or pay TV delivery mechanisms,” such as alternative means like “IP-based platforms.”⁶ In these and other references, the *Notice* does not appear to take into account the fact that many cable operators today deliver cable services using IP technology and that such IP-based cable services are distinct from “Internet-delivered” or “OTT” offerings. Nor does the *Notice* appear to take into account that, as detailed below, even where delivered in IP, digital cable services are already subject to and compliant with EAS requirements.

For example, Comcast today delivers its cable service in two formats: a QAM-based version that is accessed via set-top boxes and retail CableCARD devices; and an IP-based version that is currently accessed via its Xfinity TV app and portal running on tablets, smartphones, computers, and other customer-owned devices that are behind the customer’s in-home modem. This IP-based *cable service* is distinct from OTT services *provided over the Internet* and, like all of its QAM-based services, is delivered directly to customers exclusively

⁴ These comments address only a few of the many important issues raised in the *Notice*. Comcast associates itself with the comments filed by NCTA in this rulemaking, which address other issues of interest to the cable industry. See Comments of NCTA, PS Docket Nos. 15-94, 15-91 (June 8, 2016).

⁵ *Notice* ¶ 88.

⁶ *Id.* ¶ 89.

over Comcast’s private managed network facilities within its footprint using a closed transmission path that is distinct and separate from broadband Internet access service (“BIAS”).⁷ And, just like its QAM-based cable service, Comcast’s IP cable service complies with all applicable Title VI requirements, including EAS.⁸ However, simply because EAS alerts are currently being provided over IP cable services is no basis for concluding that EAS requirements should be imposed with respect to *non-cable services delivered over the Internet* (a topic further discussed in Section III below).

The *Notice* also asks whether there is a technical basis to continue distinguishing “programmed” channels subject to EAS obligations from other features and services offered by cable operators (e.g., interactive games, program guides, or Internet access).⁹ The Commission’s

⁷ The Commission has previously recognized the distinction between IP cable and OTT services. *See Promoting Innovation and Competition in the Provision of Multichannel Video Programming Distribution Services*, Notice of Proposed Rulemaking, 29 FCC Rcd. 15995 ¶ 74 (2014) (noting “an entity that delivers cable services via IP is a cable operator to the extent it delivers those services as managed video services over its own facilities and within its footprint” while services like “TV Everywhere” do not qualify as cable services because “they are not managed video services”); *Closed Captioning of Internet Protocol-Delivered Video Programming: Implementation of the Twenty-First Century Communications and Video Accessibility Act of 2010*, Report and Order, 27 FCC Rcd. 787 ¶ 11 (2012) (stating that “[a]ll video programming that is available on the Internet is IP-delivered, but not all video that is delivered via IP is Internet programming”); *Accessible Emergency Information, and Apparatus Requirements for Emergency Information and Video Description: Implementation of the Twenty-First Century Communication and Video Accessibility Act of 2010*, Second Report and Order and Second Further Notice of Proposed Rulemaking, 30 FCC Rcd. 5186, ¶¶ 9-15 (2015) (applying emergency information requirements to MVPD-supplied apps delivered in IP but not to MVPDs’ linear programming accessed via the Internet). *See also* Public Knowledge Reply Comments, MB Docket No. 16-42 at 12 (May 23, 2016) (noting that “use of the Internet Protocol does not mean programming is being delivered over the ‘Internet’”).

⁸ *See, e.g.*, Comcast Comments, MB Docket No. 15-64 at 10 (Oct. 8, 2015) (noting that “[t]he Xfinity apps used to deliver Comcast’s Title VI cable service are designed to fully implement all applicable Title VI protections,” including EAS alerts). The *Notice* suggests in a footnote that a new Comcast offering, Stream TV, is an OTT service. *See Notice* ¶ 88, n.209. That is incorrect. Stream TV is an IP cable service that is delivered to customers’ homes over Comcast’s private managed network facilities within its footprint utilizing dedicated bandwidth; it does not traverse the Internet or use BIAS in any way. *See* Comcast Corp. Opposition, MB Docket No. 10-56, GN Docket No. 14-28 at 8-9, 11 (Mar. 14, 2016) (“Comcast Opposition”). Stream TV complies with all applicable Title VI requirements, including EAS; Stream TV customers get all EAS alerts today – when an EAS alert is issued while the customer is watching video on the Stream TV app, the customer is force-tuned to a channel that displays the EAS alert.

⁹ *Notice* ¶ 86.

current EAS rules apply to channels that are used to deliver video programming,¹⁰ but not to cable capacity used for other purposes, such as interactive games or Internet access service.¹¹ Comcast believes that the current approach should be maintained because it follows unambiguous statutory language, tracks consumer expectations regarding the receipt of EAS alerts, and clearly delineates how EAS messages are to be delivered over cable systems. In contrast, adopting a model based on “channels that are made available for consumer use” could be construed as broadly expanding the scope of EAS requirements to non-cable services, raising a host of policy and jurisdictional issues discussed further below. It is also important to note that cable operators’ networks are engineered to only pass through EAS alerts on “programmed” channels, and implementing any changes to expand the scope of EAS obligations beyond the current approach would require significant re-engineering of those networks at substantial cost and for little consumer benefit.

III. IT WOULD BE ARBITRARY AND CAPRICIOUS TO IMPOSE EAS OBLIGATIONS SOLELY ON THE OTT VIDEO SERVICES OF EAS PARTICIPANTS.

The *Notice* seeks comment on “whether consumers have any expectation that EAS would be available over EAS Participant OTT offerings, and what technical, policy or jurisdictional issues would need to be addressed in order to make EAS available over such services.”¹² As a threshold matter, it is debatable whether the Commission has the authority to impose EAS obligations on OTT video services *at all*. It is unclear whether the Communications Act

¹⁰ 47 U.S.C. § 522(20) (“[T]he term ‘video programming’ means programming provided by, or generally considered comparable to programming provided by, a television broadcast station.”).

¹¹ 47 C.F.R. § 11.11, Table 2 n.3, Table 3 n.4, & Table 4 n.4; *Amendment of Part 73, Subpart G, of the Commission’s Rules Regarding the Emergency Broadcast System*, Second Report and Order, 12 FCC Rcd. 15503 ¶ 38 (1997) (“Programmed channel means a channel carrying video programming.”).

¹² *Notice* ¶ 3.

provisions discussed in the *Notice* would provide a legal basis for the Commission to assert jurisdiction over OTT video services, or whether any of the cited provisions create “statutorily mandated responsibilities” necessary for the Commission to invoke its ancillary authority.¹³

The *Notice* asserts that that “[t]he Commission’s regulation of emergency broadcasting, both of the EBS and EAS, has been grounded, in significant part, in Sections 1, 4(i) and (o), 303(r), and 706 of the Act,” as well as in its authority under Section 624(g) of the Cable Act of 1992, and certain provisions of the Twenty-First Century Communications and Video Accessibility Act of 2010 (“CVAA”).¹⁴ Some of those provisions, such as Section 1, “are statements of policy that themselves delegate no regulatory authority.”¹⁵ To the extent that other sections, such as Section 624(g), affirmatively grant rulemaking authority, those sections are limited to services that already are regulated by the Commission.¹⁶

Moreover, EAS obligations for OTT video services would appear to contradict repeated assurances that the Commission has no intention of regulating edge services or other Internet content.¹⁷ The Chairman and staff repeatedly have disavowed that the FCC will regulate edge services and edge providers,¹⁸ yet OTT video is an edge service and OTT video providers are

¹³ See *Comcast Corp. v. FCC*, 600 F.3d 642, 654 (D.C. Cir. 2010) (“[P]olicy statements alone cannot provide the basis for the Commission’s exercise of ancillary authority.”).

¹⁴ See *Notice* ¶ 184 (citing 47 U.S.C. § 544(g); 47 U.S.C. § 613).

¹⁵ *Comcast*, 600 F.3d at 652.

¹⁶ See 47 U.S.C. § 544(g).

¹⁷ See *Protecting and Promoting the Open Internet*, Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd. 5601 ¶ 282 n.725 (2015); see also *id.* ¶ 382 (stating that the Commission does not intend to “regulat[e] the Internet, *per se*, or any Internet applications or content”); *Consumer Watchdog Petition for Rulemaking to Require Edge Providers to Honor ‘Do Not Track’ Requests*, Order, 30 FCC Rcd. 12424 ¶ 1 (WCB 2015) (stating that the Commission “has been unequivocal in declaring that it has no intent to regulate edge providers”).

¹⁸ For example, when asked whether the FCC would investigate Netflix for throttling its video streams on mobile networks, Chairman Wheeler emphasized that “[w]e do not regulate edge providers,” and that the network

edge providers, *regardless of whether those services and providers are affiliated with an EAS Participant*. To the extent the Commission claims jurisdiction to impose EAS requirements on the OTT video services of EAS Participants, then it would have to also concede that such jurisdiction extends to regulate all OTT video services. With respect to the questions in the *Notice* about applying EAS obligations solely to the OTT video services of EAS Participants, such an approach would be arbitrary and capricious.¹⁹ There is no sound legal or policy basis for singling out these services for differential treatment, especially considering the reported growing use of OTT video services by consumers.²⁰ Such an approach would also be contrary to the Commission’s goal to make emergency alerts more consistent.²¹ Targeting only the OTT services affiliated with EAS Participants would work *against* this goal and create consumer confusion.²² If consumers can get EAS alerts on the OTT video services affiliated with EAS Participants, they will expect to get alerts on *all* OTT video services and will not understand why

management practices of online content providers are “outside of our jurisdiction.” See Jon Brodtkin, *Netflix Throttling Itself Isn’t a Net Neutrality Problem, FCC Chair Says*, ARS TECHNICA, (Apr. 1, 2016), at <http://arstechnica.com/business/2016/04/netflix-throttling-itself-isnt-a-net-neutrality-problem-fcc-chair-says/>; see also Testimony of Chairman Wheeler, Senate Subcommittee on Privacy, Technology and the Law, Examining the Proposed FCC Privacy Rules at 37:45 (May 11, 2016), <http://www.judiciary.senate.gov/meetings/examining-the-proposed-fcc-privacy-rules> (stating that the Commission’s broadband privacy proposal “only applies to network providers,” and that “we do not regulate those with whom the network terminates . . . and this includes network affiliates acting as edge providers”).

¹⁹ As a practical matter, such an approach would cover not only the TV Everywhere services offered by MVPDs, but also a wide variety of other OTT services offered by EAS Participants, such as YouTube (through its affiliation with Google Fiber), ESPN.com (through its affiliation with ABC’s broadcast stations), and Go90 (through its affiliation with Verizon FiOS).

²⁰ The average consumer’s viewing of video on the Internet increased by 36% from 2013 to 2014. See *Annual Assessment of the Status of Competition in the Market for the Delivery of Video Programming*, Seventeenth Report, DA 16-510 at ¶ 194 (May 6, 2016).

²¹ See *Notice* ¶ 89 (asking “[w]hat kind of strategies could be employed to standardize the availability of alerts across technologies, applications, and platforms?”).

²² It would also skew competition in the market for OTT video services by subjecting EAS Participants to regulatory mandates that would not apply to their OTT competitors.

alerts are not available on those other services, including popular services like Netflix, Hulu, and Amazon Prime.

The *Notice* invites comment on whether consumers have an expectation that alerts will persist across different technology platforms.²³ If consumers have any such expectation today, it is on the TV set, where consumers get EAS alerts from cable, satellite, and other MVPD service providers, as well as via over-the-air broadcast stations. Yet even on the TV set, while consumers can receive EAS alerts from these providers, those alerts are not provided on the OTT video services available via the numerous applications running on the TV itself (such as Netflix, Hulu, or Amazon apps on smart TVs) or similar applications running on game consoles, streaming players, or other devices connected to the TV set.²⁴ Presumably, the Commission is comfortable with the fact that EAS alerts do not persist across these different services accessible on the TV set. Therefore, it is difficult to understand why the Commission believes there might be a problem if EAS alerts that are accessible via the customer's in-home MVPD service (or over-the-air broadcast service) do not persist on the OTT video services affiliated with those entities, particularly when customers do not get EAS alerts from *any* OTT video service today. It would be arbitrary for the Commission to conclude there is an issue that needs to be remedied in this latter situation, but not the former.

In all events, however, such discriminatory EAS treatment of OTT services need not arise, because pursuing such regulations is unwarranted. EAS alerts are not delivered via OTT video services today, so consumers have no expectation of receiving them in the online

²³ See *Notice* ¶ 90 (asking whether “consumers have an expectation that alerts provided with programming offered via traditional technologies would still be provided when programming is offered through some other means, such as through online offerings”).

²⁴ Consumers can access apps running on these TV-connected devices by toggling to different inputs on the TV set.

environment. It bears emphasis that EAS alerts typically address localized emergencies, such as a severe weather event or flash flooding. While consumers may expect to get those alerts while watching their MVPD or over-the-air broadcast television service in the home, there is no similar expectation to receive those alerts when using OTT video services, which are generally accessible on a nationwide basis via any Internet connection. For example, a customer who resides in Philadelphia would not expect to get an alert about severe weather in Philadelphia while traveling in Washington, Chicago, or elsewhere.²⁵ And even to the extent that consumers want to receive local alerts when online, there are numerous resources available today to meet that need in the absence of government mandates. As the *Notice* observes, “Twitter, Google, and Facebook . . . personalize alerting profiles for individual users, allowing them to opt-in to receiving emergency alert messages from only those emergency management agencies or friends that they affirmatively select.”²⁶

IV. THE COMMISSION SHOULD REJECT ITS EAS SECURITY CERTIFICATION PROPOSAL.

Citing certain EAS security incidents dating back to 2007, the *Notice* asserts that “there are significant vulnerabilities in the nation’s EAS infrastructure that must be addressed comprehensively” and proposes to require EAS Participants to submit an annual certification “that attests to performance of required security measures with a baseline security posture in four

²⁵ Further, OTT video services typically provide content on a nationwide basis without the geo-targeting made possible by the local service footprints of broadcasters and MVPDs, raising significant technical feasibility issues with localized delivery of emergency alerts over OTT services.

²⁶ *Notice* ¶ 11 (“In addition to regulated alerting tools (e.g., EAS and WEA), alternative alerting mechanisms such as social media platforms may offer benefits in appropriate situations.”). For example, Twitter offers an emergency alerts platform – Twitter Alerts – where a number of federal agencies, including FEMA, and alerting authorities from 15 states and the District of Columbia participate in disseminating emergency alerts via the social media platform. See Twitter Alerts, Participating Organizations, <https://about.twitter.com/products/alerts/participating-organizations> (last visited June 1, 2016).

core areas.”²⁷ Some 27,000 EAS Participants would be required to certify, under penalty of perjury, that they comply with specified security practices regarding (1) patch management, (2) account management, (3) segmentation, and (4) CAP digital signature validation.²⁸

Companies that follow other security practices would be required to disclose and explain “alternative measures or remediation to meet or exceed the security provided by” the specified practices.²⁹ The *Notice* suggests that such a certification regime would be “minimally burdensome” and would provide “ample flexibility” for EAS Participants’ individual circumstances.³⁰ Comcast respectfully submits that the Commission should refrain from imposing such a certification regime given the concerns detailed below.

As an initial matter, the anecdotal incidents cited in the *Notice* do not reveal industry-wide failures that would warrant regulatory intervention of the type proposed here.³¹ There were certainly errors and omissions leading to the February 2013 “zombie attack” hoax, the October 2014 “Bobby Bones Show” false alert, and the other cited events, but it does not appear that these events reflect lingering security vulnerabilities or a general lack of appropriate security practices among EAS Participants. Rather, several of the incidents appear to involve simple human error beyond the scope of any of the four “core areas” identified in the proposed

²⁷ *Id.* ¶¶ 97, 111. The Commission contends that “this annual certification would establish minimum expectations for security, and provide the Commission with the necessary assurances that EAS Participants are adhering to industry best practices and therefore taking appropriate measures to secure the EAS.” *Id.* ¶ 111.

²⁸ *See* Proposed Rule 11.44; *Notice* ¶ 111 n.241 (estimating that 27,468 EAS Participants would be required to file the certification).

²⁹ *See* Proposed Rule 11.44.

³⁰ *See Notice* ¶ 111.

³¹ *See id.* ¶¶ 98-103 (discussing six EAS security incidents that occurred in 2014, 2013, 2010, and 2007).

certification.³² Furthermore, if the goal is to ensure accountability for false alerts and other EAS security breaches that may endanger public safety, the recent enforcement investigation and \$1 million fine resulting from the “Bobby Bones Show” incident show that the Commission can address such occurrences under existing rules.³³

To the extent there are remaining EAS security vulnerabilities, the certification proposed in the *Notice* would mark a departure from the Commission’s prior efforts to promote effective cybersecurity risk management across the communications sector. Through the Communications Security, Reliability, and Interoperability Council (“CSRIC”) and other multi-stakeholder efforts focused on voluntary implementation of the NIST Cybersecurity Framework,³⁴ the Commission has acknowledged that its approach to cybersecurity “must be more dynamic than traditional regulation” and should be based on “a new paradigm of proactive, accountable cyber risk management.”³⁵ Here, however, Comcast is concerned that the *Notice*’s certification proposal could lock in a checklist of mandatory actions that would become obsolete over time and that would divert resources from proactive cyber risk management tailored to the specific circumstances of individual EAS Participants.³⁶ Under the proposal, EAS Participants would be

³² See *id.* ¶¶ 100-103 (describing incidents as “accidental,” “inadvertent” and caused by equipment that was “incorrectly” installed).

³³ See *iHeartCommunications, Inc.*, Order, 30 FCC Rcd. 4442 (EB 2015) (fining a distributor of syndicated radio programming \$1 million for misuse of EAS tones under Section 325(a) of the Communications Act and Section 11.45 of the Commission’s rules).

³⁴ See, e.g., CSRIC IV Working Group 4 Final Report at 4 (Mar. 2015) (noting that CSRIC “was given the task of developing *voluntary mechanisms* that give the [FCC] and the public assurance that communication providers are taking the necessary measures to manage cybersecurity risks across the enterprise”) (emphasis in original).

³⁵ Remarks of Chairman Wheeler to the American Enterprise Institute at 1, 3 (June 12, 2014), https://apps.fcc.gov/edocs_public/attachmatch/DOC-327591A1.pdf (adding that “success will rely on proactive risk management, not reactive compliance with a cybersecurity to-do list”).

³⁶ The *Notice* states (¶ 109) that the certification proposal is merely intended “to codify best practices consistent with” CSRIC recommendations, but CSRIC’s recommendations were intended to produce voluntary

required to certify whether they have installed software updates and patches; whether they require complex passwords; whether they remove or disable unnecessary user accounts; whether they have configured firewalls to isolate EAS equipment from the Internet; whether they log remote access; and so on.³⁷ The *Notice* suggests that the option to certify alternative measures would add flexibility to each of these requirements, but it still would place the burden on EAS Participants to explain and justify commercially reasonable security measures of their choice.³⁸

Comcast also is concerned that the proposals do not fully account for the costs of the proposed certification regime on EAS Participants.³⁹ For example, the *Notice* suggests that certain certification requirements could be implemented industry-wide at “no additional cost” and with “little or no additional effort.”⁴⁰ However, there would be significant costs and burdens entailed in certifying to each of the specified security practices. As a practical matter, the engineering time, due diligence, and legal review required to prepare a corporate officer to submit a formal declaration would greatly exceed the Commission’s estimate.⁴¹ And these costs

guidelines, not regulatory mandates. See CSRIC IV Working Group 3 Final Report at 3, 15 (Mar. 2015), https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG3-EAS_SECURITY_FINAL_011316.pdf (noting CSRIC’s intention to provide “*best practices guidelines* for each of the relevant stakeholders” and recommending that the Commission “undertake an EAS security outreach effort” involving handbooks, newsletters, webcasts, and the like) (emphasis added).

³⁷ See Proposed Rule 11.44.

³⁸ The certification also would prescribe certain “baseline” security practices in an area where technologies and security threats evolve rapidly, and many EAS Participants have already developed more sophisticated security policies and procedures.

³⁹ The *Notice* suggests that each certification should take “an average of fifteen minutes,” and that if EAS Participants are not already in compliance with specified practices “it should take no more than four hours per device to perform the necessary changes.” See *Notice* ¶ 111.

⁴⁰ *Id.* ¶¶ 111, 117.

⁴¹ The *Notice* assumes that all information required to complete a certification is “readily available” and that “the amount of legal and management review is negligible” because CSRIC has already developed and endorsed relevant best practices. *Id.* ¶ 111. It further states that “[i]f additional legal and management review would be required, we assume it would only be required the first year to ensure appropriate internal processes were in place and would amount to no more than an average of one hour per company.” *Id.* This would not be the case for a large

and burdens would not be limited to the first year of the certification, but would recur annually in light of ongoing network investments, software updates, and personnel changes.⁴²

If the Commission nonetheless decides to proceed with a security certification, it must afford strong confidentiality protection to all information collected through each certification.

Otherwise, the certification regime could create public safety risks by divulging critical infrastructure information and details about EAS Participants' network security to those who would cause the very kinds of confusion and harm that the Commission seeks to prevent.

Comcast believes that such confidential treatment should be afforded to all information provided with the certification, including not only the data reported on the certification, but also the responses on the face of certification forms.⁴³ Moreover, the Commission should refrain from sharing certification information broadly with other entities, including "non-governmental entities," given the risk that such information sharing could result in the disclosure of EAS Participants' proprietary information to hostile parties or competitors.⁴⁴

company like Comcast, which would require many times the estimated time and cost each year to compile, verify, and review certification information for legal compliance.

⁴² The *Notice* states that the proposed rules "represent an incremental improvement to the nation's alerting capability that could readily save multiple lives per year in the foreseeable future." *Id.* ¶ 14. But the *Notice* provides no evidence that the specific practices identified in the proposed certification would reduce mortality risk.

⁴³ The proposed rule states that "the responses on the face of . . . certification forms shall not be treated as confidential." *See* Proposed Rule 11.45. However, certain certification responses could be highly sensitive even in a "yes/no" or check-box format, e.g., whether an EAS Participant has changed default passwords, whether its EAS devices are directly accessible from the Internet, and whether its devices are configured to validate digital signatures on CAP messages. The Commission should ensure that *all* information provided with a certification is unambiguously protected from disclosure.

⁴⁴ The *Notice* states that "EAS Participants do not risk competitive disadvantage due to disclosure of the kind of information we now seek." *Notice* ¶ 147. Comcast is concerned that the proposed certification and accompanying explanations of alternative measures would include detailed information about network operations and security practices that would be of great interest to competitors and provide economically valuable insight into each company's broader cybersecurity posture.

In other cybersecurity contexts, CSRIC has recommended that information shared with the Commission through voluntary meetings to discuss security threats and risk-management activities be treated as Protected Critical Infrastructure Information (“PCII”) under a program administered by the Department of Homeland Security.⁴⁵ Here, information provided in an EAS security certification would be at least as sensitive from a critical infrastructure standpoint, and participation would be mandatory, extending to more than 27,000 EAS Participants.

Accordingly, to the extent the Commission proceeds with its certification proposal, it should explore PCII treatment or a legally sustainable equivalent in lieu of the limited confidentiality proposed in the *Notice*.

V. IP-FIRST DELIVERY IS THE LONG-TERM FUTURE OF EAS.

The *Notice* asks about the long-term future of EAS, specifically if the Commission “need[s] a wholesale re-thinking of the alerting system.”⁴⁶ In examining the future of EAS, Comcast would welcome the opportunity to work with the Commission and other interested stakeholders to modernize the government’s delivery of EAS alerts to EAS Participants by migrating toward IP-first delivery of such alerts via IPAWS. Consistent with the Commission’s legal authority and current consumer expectations, however, Comcast suggests that such an effort be focused on improvements to core EAS infrastructure, rather than on efforts to extend EAS obligations to new devices and new services.⁴⁷

⁴⁵ See CSRIC IV, Working Group 4 Final Report at 7 (Mar. 2015), https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf (“Companies that choose to participate in this program would be afforded the protections that are given by the federal government to critical infrastructure owners and operators under the PCII program or a legally sustainable equivalent.”).

⁴⁶ *Notice* ¶ 176.

⁴⁷ For example, stakeholders could focus on enhancing and streamlining how the government delivers emergency alerts via IPAWS as part of a migration toward a more robust national EAS infrastructure that provides all the functionality of the legacy daisy chain with IP as the primary mode of transmission to EAS Participants. However, as discussed *supra* Section II, the fact that individual EAS Participants may use IP-based networks to pass

The broadcast daisy chain is a vital and needed EAS transmission line of defense, particularly in the event that a natural or man-made catastrophic event diminishes IP capability, but it should be considered a second line of defense with the primary focus on alert transmission via IP. As a primary method of delivery, IP is superior to the legacy daisy chain and can provide life-saving alerts faster and more efficiently by disseminating EAS alerts at once to all EAS Participants. IP alerts can also contain more helpful alert information, such as pictures and maps, and enable more precise geo-targeting than the daisy chain. IP alerts can also provide more sophisticated security protection to prevent unauthorized alerts and, when paired with secondary delivery via the daisy chain, enable the sort of redundancy and resiliency in the EAS delivery network that the Commission seeks.⁴⁸ Security, reliability, and timeliness are all areas of potential IPAWS improvement, however, and Comcast encourages the Commission to work with its federal partners toward those goals. For example, in contrast to the daisy chain, an EAN cannot be supported via IPAWS-OPEN CAP today, but certainly should be in the future.

As part of its effort to modernize EAS, the Commission should consider convening a multi-stakeholder initiative to examine how to migrate EAS to an IPAWS-based, IP-first delivery system.⁴⁹ Many interested stakeholders, including the Commission, FEMA, MVPDs, broadcasters, state and local governments, alert originators, and equipment vendors, among

through messages they have received from alert originators provides no basis for requiring alerts to be available to end users through Internet-related services or devices.

⁴⁸ See Notice ¶¶ 177-178; see also *Review of the Emergency Alert System; Independent Spanish Broadcasters Association, the Office of Communication of the United Church of Christ, Inc., and the Minority Media and Telecommunications Council, Petition for Immediate Relief*, Order, 31 FCC Rcd. 2414 ¶ 8 (2016) (observing the legacy system's ability to provide alerts to the public even after damage to the electrical power grid).

⁴⁹ Adopting a multi-stakeholder initiative is consistent with recent Congressional action directing FEMA to create an IPAWS Subcommittee tasked with developing recommendations on modernizing and improving IPAWS. See *Integrated Public Alert and Warning System Modernization Act of 2015*, Pub. L. No. 114-143 (2016).

others, should have a seat at the table in this initiative. The Commission has a track record of relying on multi-stakeholder advisory committees to aid its consideration of long-term EAS reforms,⁵⁰ and could utilize a similar approach here to help identify possible solutions to the challenges of migrating EAS to an IP-first network while promoting security, resiliency, and other goals identified in the *Notice*.

VI. CONCLUSION

Comcast appreciates the opportunity to comment on strengthening EAS and looks forward to working with the Commission to achieve this important goal. Consistent with these comments, Comcast urges the Commission to retain the existing requirements relating to delivery of EAS messages over programmed channels, refrain from imposing EAS obligations on OTT services (and certainly not in an arbitrary and capricious manner solely on EAS

⁵⁰ See, e.g., Charter of the Communications Security, Reliability, and Interoperability Council (Mar. 19, 2015), https://transition.fcc.gov/bureaus/pshs/advisory/csric5/CSRIC_Charter_Renewal_2014.pdf (directing CSRIC V to “[d]evelop recommendations for actions the FCC should take to enhance the ability of the public to receive timely and accurate emergency alerts and warnings, including ways to leverage advanced communications technologies and the Internet, including broadband technologies and social media platforms”); *Amendment of Part 73, Subpart G, of the Commission’s Rules Regarding the Emergency Broadcast System*, Report and Order and Further Notice of Proposed Rulemaking, 10 FCC Rcd. 1786 ¶¶ 136-137 (1994) (noting reliance on the Emergency Broadcast System Advisory Committee and amending its name and membership to charter the National Advisory Committee to coordinate and help direct implementation of the new EAS regulations).

Participants) or adopting new security certification mandates, and establish a multi-stakeholder process for examining long-term EAS issues.

WILLKIE FARR & GALLAGHER LLP
1875 K Street, NW
Washington, DC 20006

Counsel for Comcast Corporation

Respectfully submitted,

/s/ Kathryn A. Zachem

Kathryn A. Zachem
Jordan B. Goldstein
James R. Coltharp
*Regulatory Affairs,
Comcast Corporation*

Francis M. Buono
Brian A. Rankin
Catherine Fox
*Legal Regulatory Affairs,
Comcast Corporation*

COMCAST CORPORATION
300 New Jersey Avenue, NW,
Suite 700
Washington, DC 20001

June 8, 2016