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

In the Matter 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

NOTICE OF PROPOSED RULEMAKING AND NOTICE OF INQUIRY

Adopted: March 17, 2021 **Released: March 19, 2021**

Comment Date for Notice of Proposed Rulemaking: (21 days after date of publication in the Federal Register)
Reply Comment Date for Notice of Proposed Rulemaking: (35 days after date of publication in the Federal Register)

Comment Date for Notice of Inquiry: (45 days from the date of publication in the Federal Register)
Reply Comment Date for Notice of Inquiry: (75 days from the date of publication in the Federal Register)

By the Commission: Acting Chairwoman Rosenworcel issuing a statement.

TABLE OF CONTENTS

I. INTRODUCTION

1. As required by Section 9201 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021,[1] we initiate this proceeding to explore opportunities to improve the way the public receives emergency alerts on their mobile phones, televisions, and radios. The nation's Emergency Alert System (EAS) and Wireless Emergency Alert System (WEA) ensure that the public is quickly informed about emergency alerts issued by federal, state, local, Tribal, and territorial governments and delivered over the radio, television, and mobile wireless devices. These announcements keep the public safe and informed and have ever-increasing importance in the wake of the emergencies and disasters Americans have faced in the past few years. However, in 2018, a false emergency alert mistakenly warning of a ballistic missile threat to Hawaii highlighted the need to improve these systems. Consistent with congressional directive, we initiate this rulemaking to consider proposals to ensure that more people receive relevant emergency alerts, to enable EAS and WEA participants to report false alerts when they occur, and to improve the way states plan for emergency alerts.

2. In this Notice of Proposed Rulemaking, we propose to implement Sections 9201(a)-(d) of the NDAA21 by adopting rules to ensure that mobile devices cannot opt-out of receiving WEA alerts from the Administrator of the Federal Emergency Management Agency (FEMA). We also propose rules to encourage chief executives of states to form State Emergency Communications Committees (SECC) if none exist in their states and to adopt additional requirements concerning their SECC's administration of State EAS Plans.[2] For states that already have a SECC, we encourage chief executives to review its composition and governance. We propose to enable the Administrator of FEMA and State, local, Tribal, and territorial governments to report false EAS and WEA alerts when they occur.[3] Finally, we propose rules to permit repeating EAS alerts issued by the President, the Administrator of FEMA, and any other entity determined appropriate under the circumstances by the Commission.[4] The rules we propose today are intended to facilitate the further development of a robust and redundant system for distributing vital alert information to all Americans.

3. In the Notice of Inquiry, we implement Section 9201(e) of the NDAA21 by seeking comment on whether it is technically feasible to deliver EAS alerts through the internet, including through streaming services..[5] We also seek comment on whether and how to leverage the capabilities of the Internet to enhance the alerting capabilities of the radio and television broadcasters, cable systems, satellite radio and television providers, and wireline video providers that currently participate in EAS (EAS Participants).[6] As directed by Congress, after the conclusion of this inquiry, the Commission will submit a report on its findings and conclusions to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Energy and Commerce of the House of Representatives.[7]

---

[1] *See* National Defense Authorization Act of 20221, Pub. L. 116-283, 134 Stat. 3388, § 9201(a) (NDAA21).

[2] *See id*., § 9201(b).

[3] *See id*., § 9201(c).

[4] *See id*., § 9201(d).

[5] *See id*., § 9201(e).

[6] *See id*.; *see also* 47 CFR § 11.2(b) (defining EAS Participants as "[e]ntities required under the Commission's rules to comply with EAS rules, *e.g.*, analog radio and television stations, and wired and wireless cable television systems, DBS, DTV, SDARS, digital cable and DAB, and wireline video systems).

[7] *See* NDAA21, §9201(e).

II. BACKGROUND

4. *IPAWS*. FEMA administers the Integrated Public Alert and Warning System Open Platform for Emergency Networks (IPAWS),[8] an alert aggregator that, as illustrated in *Figure 1*, receives emergency alerts from federal, state, local, Tribal, and territorial alert originators, and then authenticates, validates and delivers those alert for dissemination over EAS, WEA, and other alert distribution pathways.[9]

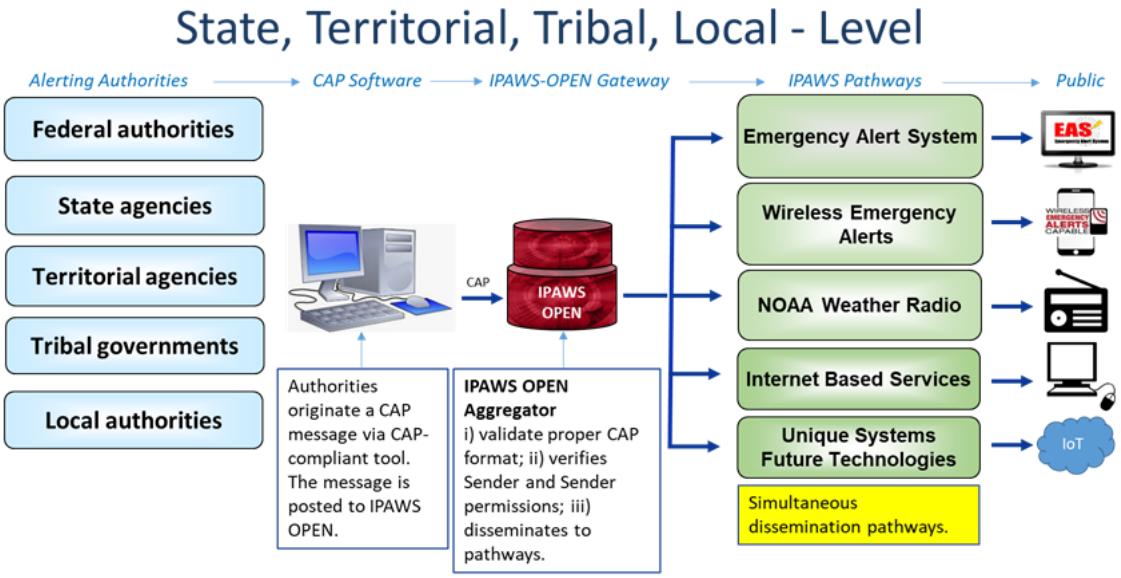

Figure 1: IPAWS Architecture[10]

5. *WEA*. WEA[11] is a tool for authorized federal, state and local government entities to geographically target alerts and warnings to WEA-capable mobile devices of participating Commercial

---

[8] *See* FEMA, Integrated Public Alert and Warning System, https://www.fema.gov/emergency-managers/practitioners/integrated-public-alert-warning-system (last visited Jan 11, 2021). FEMA also administers the Primary Entry Point (PEP) system for legacy EAS and interfaces with the White House on the administration of the Presidential Alert.

[9] *See* FEMA, IPAWS-OPEN, https://www.fema.gov/emergency-managers/practitioners/integrated-public-alert-warning-system/technology-developers/ipaws-open (visited Jan. 29, 2021). The term "alert originator" refers to a federal, state, local, Tribal, or territorial entity authorized by FEMA to use the Integrated Public Alert and Warning System (IPAWS) to issue critical public alerts and warnings in emergency situations. See FEMA, Alerting Authorities, https://www.fema.gov/emergency-managers/practitioners/integrated-public-alert-warning-system/public-safety-officials/alerting-authorities (visited Jan. 29, 2021).

[10] The "Internet Based Services" illustrated in *Figure 1* are services offered by entities that sign a Memorandum of Agreement with the FEMA IPAWS Program Management Office to receive and transmit alerts from the IPAWS All-Hazards Information Feed. FEMA posts every public alert sent to IPAWS to the All-Hazards Information Feed, a mechanism for Internet services to monitor and retrieve IPAWS alerts. *See* FEMA, IPAWS All Hazards Information Feed, https://www.fema.gov/emergency-managers/practitioners/integrated-public-alert-warning-system/technology-developers/all-hazards-information-feed (last visited Jan. 25, 2021). At least 111 organizations use the All-Hazards Information Feed, including Facebook, Layer3 TV Inc, The Weather Channel, and National Public Radio. IPAWS also intermediates alerting to the NOAA Weather Radio system and digital signage.

[11] WEA was established by the WARN Act. From a technical standpoint, the WEA system currently deployed by FEMA and participating CMS providers is based on standards created by the Alliance for Telecommunications

(continued….)

Mobile Service (CMS) providers' subscribers.[12] These alert messages are separated into four categories, with varying requirements governing their use: (i) Presidential Alert; (ii) Imminent Threat Alert; (iii) Child Abduction Emergency/AMBER Alert; and (iv) Public Safety Message.[13] In terms of distribution, an alert originator sends a WEA Alert Message using FEMA-approved alert origination software to the IPAWS. The IPAWS system then authenticates, validates and delivers that alert for dissemination to participating CMS providers' alert gateways.[14] Participating CMS providers' WEA infrastructure then transmits the alert message content to their subscribers' WEA-capable devices. These devices receive alerts from IPAWS in a standard message format called the Common Alerting Protocol, which is an open, interoperable format.[15] When the alert message is received by a WEA-capable mobile device, it is prominently presented to the subscriber as long as the subscriber has not opted out of receiving alert messages of that category.[16] WEA messages must be accessible to individuals with disabilities.[17] Of particular relevance to this proceeding, the Commission's WEA rules currently allow CMS Providers to provide their subscribers with the option (which the subscriber selects on their mobile device) to opt out of receiving any or all of the WEA alert categories, except the Presidential Alert.[18]

6. *EAS*. The EAS is a national public warning system through which broadcasters, cable systems, and other EAS Participants deliver alerts to the public to warn them of impending emergencies and dangers to life and property.[19] The primary purpose of the EAS is to provide the President with "the

---

Industry Solutions (ATIS), the Telecommunications Industry Association (TIA) (jointly, ATIS/TIA), and the 3rd Generation Partnership Project (3GPP). See Communications Security, Reliability, and Interoperability Council (CSRIC) IV, Working Group Two, Wireless Emergency Alerts, Geotargeting, Message Content and Character Limitation Subcommittee, Final Report at 7 (2014), available at https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_CMAS_Geo-Target_Msg_Content_Msg_Len_Rpt_Final.pdf (last visited Feb. 9, 2021) (CSRIC IV WEA Messaging Report).

[12] A "Participating CMS Provider" is a Commercial Mobile Service Provider that has voluntarily elected to transmit Alert Messages under Part 10 of the Commission's rules. 47 CFR § 10.10(f). *See also* 47 CFR § 10.10(d); 47 U.S.C. § 332(d)(1) (defining the term "commercial mobile service").

[13] *See* 47 CFR § 10.400.

[14] *See id.*

[15] The Common Alerting Protocol standard was developed by the Organization for the Advancement of Structured Information Standards (OASIS), and incorporates a language developed and widely used for web documents. *See 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*, ET Docket No. 04-296, Fifth Report and Order, 27 FCC Rcd 642, 648-49, paras. 10-11 (2012) (*Fifth Report and Order*). The Common Alerting Protocol is an open, interoperable, XML-based standard that can include multimedia such as streaming audio or video. *See* OASIS CAP v1.2 (IPAWS Profile for the OASIS Common Alerting Protocol IPAWS USA). Common Alerting Protocol-formatted messages contain standardized fields that facilitate interoperability between and among devices. *See id*.

[16] *See* Joint ATIS/TIA CMAS Mobile Device Behavior Specification (ATIS-TIA-J-STD-100). *See also* 47 CFR § 10.280.

[17] WEA messages must be accompanied by a unique audio attention signal and vibration cadence to ensure accessibility. *See* 47 CFR §§ 10.520, 10.530; *see also The Commercial Mobile Alert System*, First Report and Order, 23 FCC Rcd 6144, 6168-69, paras. 64-67 (2008) (explaining that these requirements were adopted in order to ensure WEA accessibility).

[18] *See* 47 CFR § 10.280.

[19] *See, e.g., Fifth Report and Order*, 27 FCC Rcd at 646, para. 6; *Review of the Emergency Alert System,* EB Docket No. 04-296, *Notice of Proposed Rulemaking*, 19 FCC Rcd 15775, 15776-77, paras. 6-8 (2004). The Commission's rules define EAS Participants as analog radio broadcast stations, including AM, FM, and Low-power FM stations; digital audio broadcasting stations, including digital AM, FM, and Low-power FM stations; Class A television and

(continued….)

capability to provide immediate communications and information to the general public at the National, State and Local Area levels during periods of national emergency."[20] The EAS also is used to distribute alerts issued by state, local, Tribal, and territorial governments, as well as by the National Weather Service (NWS).[21] Although EAS Participants are required to broadcast Presidential alerts, they participate in broadcasting state and local EAS alerts on a voluntary basis.[22] The Commission, FEMA, and the NWS implement the EAS at the federal level.[23]

7. Communications technologies have evolved significantly over the seventy years since the earliest precursors to EAS were created. As Americans adopted new technologies, the Commission amended its EAS rules to ensure that emergency alerts remain available and continue to warn the public to take appropriate action to protect their lives and property.[24] In some instances, advancements in technology have called for the Commission to require new communications service providers to

Low-power TV stations; digital television broadcast stations, including digital Class A and digital Low-power TV stations; analog cable systems; digital cable systems; wireline video systems; wireless cable systems; direct broadcast satellite service providers; and digital audio radio service providers. *See* 47 CFR § 11.11(a).

[20] 47 CFR § 11.1. Under the Part 11 rules, national activation of the EAS for a Presidential alert message, initiated by the transmission of an Emergency Action Notification (EAN) event code, is designed to provide the President the capability to transmit an alert message (in particular, an audio alert message) to the American public within ten minutes from any location at any time and must take priority over any other alert message and preempt other alert messages in progress. *See, e.g., First Report and Order*, 20 FCC Rcd. 18625, 18628, para. 8. *See also, e.g.*, 47 CFR §§ 11.33(a)(11), 11.51(m), (n).

[21] The National Weather Service is the most prolific originator of alerts containing emergency weather information. NWS also administers NOAA Weather Radio. *See* National Weather Service, NOAA Weather Radio, https://www.weather.gov/nwr/ (last visited Jan. 15, 2021).

[22] *See* 47 CFR § 11.55(a); *First Report and Order*, 20 FCC Rcd at 18628, para. 8.

[23] The respective roles of the Commission, FEMA, and NWS are defined in a series of Executive documents. *See* 1981 State and Local Emergency Broadcasting System (EBS) Memorandum of Understanding Among the Federal Emergency Management Agency (FEMA), Federal Communications Commission (FCC), the National Oceanic and Atmospheric Administration (NOAA), and the National Industry Advisory Committee (NIAC) reprinted as Appendix K to Partnership for Public Warning Report 2004-1, The Emergency Alert System (EAS): An Assessment; Assignment of National Security and Emergency Preparedness Telecommunications Functions, Exec. Order No. 12472, 49 Fed. Reg. 13471 (1984); and Memorandum, Presidential Communications with the General Public During Periods of National Emergency, The White House (Sept. 15, 1995) (1995 Presidential Statement).

[24] *See Providing for Emergency Control Over Certain Government and Non-Government Stations Engaged in Radio Communication or Radio Transmission of Energy*, Exec. Order No. 10,312, 51 Fed. Reg. 14,769 (1951) (directing the creation of Control of Electromagnetic Radiation (CONELRAD) to provide a means for the President to address the American people, to provide attack warning, and to supply emergency information over broadcast radio); *Assigning Emergency Preparedness Functions to the Federal Communications Commission*, Exec. Order No. 11,092, 63 Fed. Reg. 2216 (1963) (directing the creation of the Emergency Broadcast System (EBS) to include broadcast television); *1994 Report and Order*, 10 FCC Rcd at 1809 (requiring that cable providers participate in EBS and, accordingly, renaming the system "EAS"); *First Report and Order*, 20 FCC Rcd 18625 (requiring digital television (DTV), digital audio broadcast (DAB), digital cable, direct broadcast satellite (DBS) and satellite digital audio radio service (SDARS) providers to participate in the EAS).

participate in EAS.[25] In other instances, the Commission has allowed the providers of some emerging communications technologies to participate voluntarily.[26]

8. The EAS is a broadcast-based, hierarchical alert message distribution system in which an alert message originator at the local, state, or national level encodes (or arranges to have encoded) a message in the EAS Protocol.[27] The alert is then broadcast from one or more EAS Participants, and subsequently relayed from one station to another until all affected EAS Participants have received the alert and delivered it to the public.[28] This process of EAS alert distribution among EAS Participants is often referred as the "daisy chain" distribution architecture. Because this EAS architecture has been in place since the inception of the EAS, it is often referred to as the "legacy EAS." Since June 30, 2012, however, authorized emergency alert authorities also have been able to distribute EAS alerts over the Internet to EAS Participants (who in turn deliver the alert to the public) by formatting those alerts in the Common Alerting Protocol and delivering those alerts through the FEMA administered IPAWS.[29]

9. Both the legacy and Common Alerting Protocol-based EAS architectures are designed so that EAS Participants pass through to the public the alert content they receive from the EAS sources they monitor. The EAS is not designed to facilitate alert origination by EAS Participants or repetition of alerts.[30] In particular, the EAS header codes, End-of-Message (EOM) code, and audio message (if included) that comprise any given EAS alert are set in place by the entity that originates the alert (typically, the NWS or state and local emergency management authorities).[31] The EAS equipment of EAS Participants that receive the EAS alert validates the header codes to confirm, among other things,

---

[25] Pursuant to the Commission's EAS rules, EAS Participants install EAS equipment at their facilities to monitor and receive EAS alerts and to transmit them to other EAS Participants and the public, among other requirements. *See also* 47 CFR §§ 11.11, 11.56 (requiring EAS Participants to deploy equipment capable of acquiring, encoding, and decoding EAS alert messages, and converting EAS messages from the Common Alerting Protocol to the EAS Protocol (as defined in Section 11.31)).

[26] *See*, *e.g.*, *1994 Report and Order*, 10 FCC Rcd at 1809-11, paras. 66-74 (permitting telephony, satellite, and microwave network, DAR, High Definition Television (HDTV), and digital/interactive systems to voluntarily participate in EAS).

[27] *See* 47 CFR § 11.31. Under this protocol, an EAS alert uses a four-part message: (1) preamble and EAS header codes (which contain information regarding the identity of the sender, the type of emergency, its location, and the valid time period of the alert); (2) audio attention signal; (3) audio message, if included by the alert originator; and (4) preamble and "end of message" (EOM) codes. *See id*. § 11.31(a). Although the EAS Protocol specifies that the message can be audio, video, or text, in practice, only audio is sent.

[28] At the national level, EAS message distribution starts at Primary Entry Point (PEP) stations, which are a group of geographically diverse, high power radio stations designated and tasked by FEMA to transmit "Presidential Level" messages initiated by FEMA. *See Fifth Report and Order*, 27 FCC Rcd at 646-47, para. 7. At the state level, state and local emergency operations managers activate the EAS by utilizing state-designated EAS entry points—specifically, State Primary stations and "State Relay" stations. *See* 47 CFR § 11.18. State Relay stations relay both national and state emergency messages to local areas. *See id*. § 11.18(d).

[29] *See* 47 CFR § 11.56; *see also Fifth Report and Order*, 27 FCC Rcd at 644-45, para. 4. EAS Participants are required to convert Common Alerting Protocol-formatted EAS messages into messages that comply with the EAS Protocol requirements for distribution over the legacy EAS following the procedures set forth in the EAS-CAP Industry Group's (ECIG) Recommendations for a CAP EAS Implementation Guide, Version 1.0 (May 17, 2010) ("ECIG Implementation Guide") (this document is available on ECIG's web site at: http://eas-cap.org/documents.htm) (last visited Jan. 20, 2021). *See* 47 CFR § 11.56.

[30] Nonetheless, EAS Participants may voluntarily serve as manual entry points for alerts originated by state and local authorities.

[31] *See* 47 CFR § 11.31.

that the alert is within the valid time period and not a duplicate of a prior alert.[32] If valid, the EAS equipment will then convert the header codes into visual crawls and broadcast the audio.[33] If the EAS Participant's broadcasts are monitored by downstream stations, the EAS equipment will re-encode the alert so as to trigger EAS equipment in such monitoring stations, thus perpetuating the daisy chain alert distribution cycle. All of these functions are typically done automatically. In terms of timing, state and local EAS alerts are required to be broadcast within 15 minutes of receipt, and the alert messages themselves are typically limited to a duration of two minutes.[34] EAS alerts must be accessible to individuals with disabilities.[35]

10. *Hawaii False Alert*. In January 2018, the Hawaii Emergency Management Agency mistakenly issued an emergency alert through IPAWS that falsely warned the public of a non-existent inbound ballistic missile attack.[36] Following this event, the Public Safety and Homeland Security Bureau (Bureau) conducted an investigation and issued a report of factual findings about the causes of the incident with recommendations in April of 2018.[37] The Bureau recommended several improvements towards the goal of preventing such false alert in the future, including changes to states' internal emergency alert readiness testing processes, additional steps for states to publicize corrections to false alerts, and regular consulting between state governments and SECCs for review of EAS procedures and review of State EAS Plans.[38] The Hawaii false alert event and the Bureau's review were a major impetus to the eventual adoption of Section 9201 of the NDAA21.[39]

11. On January 1, 2021, Congress adopted Section 9201 the NDAA21 to clarify the class of emergency alerts that must be received by all wireless subscribers, improve the preparedness of SECCs, strengthen the FCC's oversight of EAS and WEAs systems, and examine the feasibility of expanding the reach of emergency alerts using new technologies.[40] Specifically, the NDAA directs the Commission to complete a rulemaking to amend the WEA and EAS rules to (i) ensure that mobile devices cannot opt-out of receiving WEA alerts from the Administrator of FEMA; (ii) amend the annual reporting requirements for SECCs; (iii) enable reporting of false EAS and WEA alerts by the FEMA Administrator and State, Tribal, or local governments; and (iv) provide for repeating EAS alerts issued by the President, the Administrator of FEMA, and any other entity determined appropriate by the Commission.[41] The

---

[32] EAS equipment determines whether timing of an alert is valid by confirming whether the time when the alert is received falls between the alert's origination time minus 15 minutes and the alert's expiration time. *See* 47 CFR § 11.33(a)(10). EAS devices are required to reject duplicate alerts. *See id*.

[33] *See* 47 CFR § 11.51(d), (g)(3), (h)(3), (j)(2). For state and local alerts, EAS Participants broadcast any accompanying audio message on a permissive basis but are required to broadcast the audio message associated with the Emergency Action Notification alert. *See* 47 CFR § 11.51(a), (b).

[34] *See* 47 CFR §§ 11.51(n), 11.33(a)(9).

[35] Further, EAS Participants that transmit EAS alerts to end-user devices capable of displaying a visual and audio message, such as set-top boxes and televisions, must comply with specific visual and audio display requirements to ensure accessibility. *See, e.g.,* 47 CFR §§ 11.51(d), (g)(3), (h)(3), (j)(2); *Review of the Emergency Alert System*, EB Docket No. 04-296, Sixth Report and Order, 30 FCC Rcd 6520, 6536-42, paras. 34-46 (2015) (*Sixth Report and Order*).

[36] S. Rep. No. 116-240, at 3 (2020).

[37] Report and Recommendations; Hawaii Emergency Management Agency January 13, 2018 False Alert, (PSHSB 2018), https://www.fcc.gov/document/fcc-releases-report-hawaii-false-emergency-alert.

[38] *Id*., at 24-25.

[39] S. Rep. No. 116-240, at 3-4 (2020).

[40] S. Rep. No. 116-240, at 3 (2020); H. Rep. No. 116-582, at 2 (2020).

[41] NDAA21, § 9201(a)-(d).

NDAA21 also directs the Commission to examine the feasibility of updating EAS to enable or improve alerts to consumers provided through the Internet, including over streaming services.[42]

III. NOTICE OF PROPOSED RULEMAKING

A. Wireless Emergency Alert System Offerings

12. The NDAA21 amends Section 602(b)(2)(E) of the WARN Act to prevent CMS providers from allowing subscribers to opt out of receiving alerts issued by "the Administrator of [FEMA]."[43] The NDAA21 further directs the Commission to "adopt regulations to implement the amendment."[44] To implement this statutory directive, we propose to rename WEA's "Presidential Alert" class of alert messages to "National Alert."[45] We propose in turn to define this newly created class of "National Alert" as alerts issued by the President (or the President's authorized designee)[46] or by the Administrator of FEMA.[47] We also propose to require participating CMS providers that use WEA header displays that read "Presidential Alert" to change those alert headers to read "National Alert."[48] As detailed below, under our proposed approach, all participating CMS providers' wireless systems currently receiving mandatory Presidential Alerts will receive National Alerts the same way—distributed automatically as a non-optional alert to the same wireless customers that can currently receive Presidential Alerts.

13. *National Alert Class*. Rather than mandating the creation of a new alert category, we believe that merging alerts originated by the FEMA Administrator and the President (or the President's designee) under the existing class for non-optional WEA alerts would provide the most efficient way to implement the statute's requirement for non-optional FEMA Administrator alerts because it would obviate the need for major technical changes to WEA infrastructure. When a Presidential Alert is issued through WEA today, FEMA transmits the WEA message via IPAWS to the participating CMS provider gateway using a unique WEA handling code to distinguish the alert from all other classes of WEAs.[49] All WEA-enabled mobile devices of participating CMS providers are programmed to automatically display a Presidential Alert based on that unique handling code identifier, with no subscriber choice to opt out of the alert.[50] The effect of our proposal would be for alerts originating from the President (or the President's authorized designee) and the FEMA Administrator to use the same, existing WEA handling code for Presidential Alerts. Because the WEA handling code could remain the same, our proposal would

---

[42] *See* i*d*., § 9201(e).

[43] NDAA21, § 9201(a); *see also* 47 U.S.C. § 1201(b)(2)(E) (CMS providers that elect to transmit WEA alerts can offer subscribers the capability to opt out of such alerts, except for alerts issued by the President).

[44] NDAA21, § 9201(a).

[45] *See* Appendix A, proposed revisions to 47 CFR §§ 10.11, 10.320, 10.400, 10.410, 10.420, and 10.500.

[46] The President may designate additional officials, *e.g*., by Executive Order under 3 U.S.C. § 301.

[47] *See* Appendix A, proposed revision to 47 CFR §10.400(a).

[48] *See* Appendix A, proposed addition of subsection (b) to 47 CFR §10.11.

[49] *See* ATIS Standard on Wireless Emergency Alert (WEA) 3.0 Federal Alert Gateway to CMSP Gateway Interface Specification, ATIS-0700037.v002, Alliance for Telecommunications Industry Solutions (May 2, 2019) at 48, 64. The WEA handling code is the element in Common Alerting Protocol messages that IPAWS transforms into messages that are sent to the participating CMS provider gateways. This element is exchanged between IPAWS and the participating CMS provider gateways as the Commercial Mobile Alert for C Interface (CMAC) "CMAC_special_handling" element, and the CMS provider systems use this element to identify an alert as "Presidential" or otherwise.

[50] 47 CFR § 10.280(a). Some mobile devices show the Presidential Alert in the opt-out menu without providing the user the ability to opt-out, while some mobile devices do not list the Presidential Alert at all, since the user cannot opt-out of Presidential Alerts.

require few, if any, technical changes be made to participating CMS provider networks or the mobile devices of their subscribers before alerts originating from the FEMA Administrator could be received.

14. We seek comment on the efficiency and effectiveness of our proposed approach. Are there any technical alert transmission or presentation issues that could arise under our "National Alert" proposal that we have not identified and should consider? For situations in which FEMA deemed it appropriate to send WEA messages to only a specific region or state, could the proposed National Alert class support the transmission and delivery of geographically targeted WEA messages? Would any additional standards development or rules be required to ensure that FEMA can initiate, and participating CMS providers' subscribers can receive and display, such a targeted alert? Are there costs or other burdens arising from our proposal that we have not considered? What public safety benefits would arise from our proposal that would not arise from alternative approaches? For example, would renaming the "Presidential Alert" class make such alerts more likely to be trusted and heeded by recipients?[51]

15. If we do not adopt our proposed approach, implementing this NDAA21 requirement would require the creation of a new, separate handling code and class of non-optional alerts named "FEMA Administrator Alert." We tentatively conclude that this approach would be inefficient and costly. We believe this approach would require participating CMS providers and mobile device manufacturers to develop new standards and would require changes to CMS provider gateways, Radio Access Networks, and mobile devices to enable a new handling code that is specific to FEMA Administrator Alert. We estimate that the maximum reasonable one-time cost of creating a new alert message classification for FEMA Administrator alerts would be $43.5 million, with an estimated implementation timeframe of approximately 30 months. We arrive at this cost estimate in part based on the costs we assessed as attendant to adding the Public Safety Message alert message classification to WEA.[52] Nevertheless, we seek comment on any merits to creating a new alert message classification for FEMA Administrator alerts, including any costs and other burdens that would be necessary for its implementation as well as any public safety benefits that it might generate. We seek comment on any other alternative approaches that may exist for implementing non-optional FEMA Administrator alerts. Are there more effective and/or less burdensome ways to meet NDAA21's requirements on this matter?

16. *National Alert Header*. We anticipate that when certain subscribers with WEA-capable mobile devices receive a National Alert, their devices will continue to display a heading for that alert that reads "Presidential Alert" rather than "National Alert," until their devices receive a software upgrade to reflect the changes we propose today. We believe that if subscribers received an alert with the header "Presidential Alert" when the alert was not actually originated by the President, the alert would cause confusion and undermine the authoritativeness and effectiveness of WEA. To mitigate these harms, we propose to require participating CMS providers to make any necessary upgrades to their network infrastructure to ensure that WEA headers displayed on new or existing devices that read "Presidential Alert," including those listed in a mobile device's setting menus, are updated so that they instead read

[51] *See* Farnoush Amiri, *FEMA's 'Presidential Alert' test postponed as some Americans want to disconnect*, NBC News (Oct. 3, 2018), https://www.nbcnews.com/tech/mobile/fema-s-presidential-alert-test-postponed-some-americans-want-disconnect-n910406 (discussing some individuals' concerns that a President may use WEA for political purposes).

[52] *See Wireless Emergency Alerts*, PS Docket No. 15-91, Report and Order and Further Notice of Proposed Rulemaking, 31 FCC Rcd 11112, 11166, para. 87 (2016) ("In this section, we show that we can reasonably expect the minimum benefit resulting from the improvements to WEA we adopt today to exceed their maximum cost. The maximum reasonable cost burden our rules could present to Participating CMS Providers is $40 million as a one-time cost, and $2.3 million as an annual cost. These costs result from modifications to standards and software, as well as recordkeeping and reporting."). There would be no relevant technical difference between creating a new alert message classification for Public Safety Messages and creating a new alert message classification for FEMA Administrator alerts.

"National Alert."[53] We note that our WEA rules currently do not require participating CMS providers to display a header of "Presidential Alert" at all when a Presidential Alert is displayed on a mobile device, although many providers have chosen to do so.[54] Accordingly, our proposed requirement could be satisfied by ensuring that "Presidential Alert" is not displayed on a user's mobile device, whether by changing the displayed header or not displaying the header at all. We further propose that in instances in which network infrastructure is technically incapable of meeting this requirement, such as situations in which legacy devices or networks cannot be updated to support this functionality, participating CMS providers would be excepted from satisfying it. We seek comment on this proposal. How prevalent are mobile devices that are designed to display the "Presidential Alert" header to subscribers? Would the erroneous display "Presidential Alert" header introduce confusion and undermine the effectiveness of WEA? How can the benefit of ensuring the authoritativeness and effectiveness of WEA in this instance be quantified? What kinds of technical changes would participating CMS providers experience in meeting this requirement? What percentage of mobile devices currently in use by consumers would be technically capable of receiving an upgrade to effectuate this proposed requirement?

17. We specifically seek comment on the cost that may be incurred by participating CMS providers to make changes to existing "Presidential Alert" headers. We believe display changes to deployed mobile devices can be implemented via over-the-air software updates or changes to newly manufactured devices.[55] Because our proposal would only require a change to a header displayed to subscribers, we anticipate that the one-time implementation costs associated with our proposed requirement would be low, and would be exceeded by the benefits of ensuring the authoritativeness and effectiveness of the EAS during a national emergency. We specifically seek comments that quantify the costs of developing and implementing the necessary display changes via software update, as well as any additional costs that participating CMS providers may incur. We also seek comment on the potential burdens to states or state-level alert originators of all of our proposed WEA rule changes discussed above and any alternatives thereto.

18. We seek comment on the amount of time that will be necessary for participating CMS providers to implement our proposed header display requirement. We note that when the Commission adopted rules in 2017 to enable the delivery of Blue Alerts over WEA, the Commission allowed a period of 18 months for participating CMS providers to make the necessary changes to their network infrastructure.[56] We believe that it will take significantly less time for participating CMS providers to

[53] *See* Appendix A, proposed addition of paragraph (b) to section 10.11.

[54] Section 10.333 of our rules specifies that wireless provider WEA infrastructure remains under the control of participating CMS providers, and section 10.420 of our rules exempts Presidential Alerts from message element requirements. *See* 47 CFR §§ 10.333(c), 10.420. Our proposed rule changes would expand the message element exemption to all National Alerts covering both alerts originating from the President (or the President's designee) and the FEMA Administrator. Participating CMS providers do have minimal requirements to inform customers about the kinds of alerts they will not receive if they opt out under section 10.280, but that rule does not mandate specific customer notice about Presidential Alerts, which customers cannot opt out of. *See* 47 CFR § 10.280.

[55] We estimate that the cost of the standards and software updates that would likely be required remove the "Presidential Alert" display text from phones and replace it with "National Alert" will be minimal. We arrive at this cost estimate in part based on the costs we assessed as attendant to adding Blue Alerts to WEA. *See Amendment of Part 11 of the Commission's Rules Regarding Emergency Alert System*, PS Docket No. 15-94, Report and Order, 32 FCC Rcd 10812, 10824, para. 25 (2017) (*Blue Alert Order*) ("Although we recognize that EAS equipment manufacturers will incur some costs... we believe that 12 months will provide sufficient time to dovetail the BLU upgrade with other scheduled upgrades, posing minimal expense to equipment manufacturers. We believe that the costs for implementation of WEA will be similarly low, because Blue Alerts will be delivered over the existing Imminent Threat WEA classification, using WEA in its current configuration."). Like the addition of Blue Alerts to WEA delivered under the existing Imminent Threat Alert classification, pursuant to the approach we propose today, National Alerts will be delivered under the existing Presidential Alert classification.

[56] *See* id., 32 FCC Rcd 10822, para. 21.

implement the header display requirements we propose today, as developing, testing, and distributing the necessary software upgrades would be a far less difficult undertaking than ensuring that network infrastructure can properly transmit, receive, and display a Blue Alert, which required modification of the secure interface between IPAWS and CMS provider gateways.[57] Accordingly, we propose to allow an implementation period of approximately 12 months from the effective date of the requirement, with a date certain of July 31, 2022.[58] We further propose to delegate authority to the Public Safety and Homeland Security Bureau (Bureau), which would seek OMB review of any new information collections that the Commission might adopt in implementing the NDAA21, to extend this effective date briefly by Public Notice published in the Federal Register (*e.g.*, if a required OMB review of information collections is delayed). We seek comment on our estimated implementation timeline. Commenters proposing alternatives should explain each of the steps that participating CMS providers must take to implement the header display requirement and how much time each of those steps is estimated to complete.

19. Given the overwhelming importance to public safety, we propose to require that participating CMS providers support FEMA Administrator-issued National Alerts upon the effective date of the rules, even though some mobile devices will not yet support the National Alert header. This approach will allow subscribers of participating CMS providers to receive all Presidential and FEMA Administrator-initiated alerts in the soonest possible timeframe, which we believe achieves the NDAA21's purpose and intent.[59] In the event that a National Alert is issued in the window between the time our rules are adopted and necessary mobile device upgrades are made, we note that the FEMA Administrator can distinguish their alert from a national Presidential Alert in the alert message text itself. We seek comment on this proposal. In particular, are there any risks or concerns associated with alerts initiated by FEMA continuing to be displayed on handsets as "Presidential Alerts" during the transition period? If so, does this merit a faster implementation timeline for the header display requirement or a slower implementation timeline for supporting alerts initiated by FEMA? We also seek comment on whether inclusion of identifying information about which federal official issues a National Alert is necessary to inform the public and encourage them to take appropriate action in response to an emergency.

B. State EAS Plans and SECCs

20. The Commission's EAS rules require the filing of a State EAS Plan with the Commission documenting the distribution architecture within the state.[60] More specifically, State EAS Plans describe state and local EAS operations, alert distribution origination and pathways, and "contain guidelines which must be followed by EAS Participants' personnel, emergency officials, and [NWS] personnel to activate the EAS."[61] State EAS Plans are prepared and administered by SECCs, along with associated Local Emergency Communications Committees (LECCs). The SECCs and LECCs are volunteer organizations composed of state broadcaster associations, EAS Participants, emergency management personnel, and other stakeholders. State EAS Plans must be reviewed and approved by the Chief of the Bureau prior to their implementation "to ensure that they are consistent with national plans, FCC regulations, and EAS operation."[62]

---

[57] *Id.* at 10822-23, para. 22.

[58] The NDAA21 requires the Commission to complete this rulemaking proceeding by June 30, 2021. *See* NDAA21, § 9201(a)(2).

[59] *See id.*, § 9201(a).

[60] *See* 47 CFR § 11.21.

[61] *Id.*, § 11.21(a).

[62] *Id.*

21. NDAA21 directs the Commission to conduct a rulemaking to implement provisions concerning SECCs and State EAS Plans. With respect to SECCs, the legislation requires that the Commission adopt regulations that "encourage the chief executive of each State [] (i) to establish an SECC if the State does not have an SECC; or (ii) if the State has an SECC, to review the composition and governance of the SECC,"[63] and provide that "(i) each SECC, not less frequently than annually, shall [] (I) meet to review and update its State EAS Plan; (II) certify to the Commission that the SECC has met [as required under this meeting obligation]; and (III) submit to the Commission an updated State EAS Plan."[64]

22. With respect to State EAS Plans, the statute also requires that the Commission adopt rules that provide that "not later than 60 days after the date on which the Commission receives an updated State EAS Plan [as required under the statute's SECC-related regulation above], the Commission shall [] (I) approve or disapprove the updated State EAS Plan; and (II) notify the chief executive of the State of the Commission's approval or disapproval of such plan, and reason therefor."[65] The statute further requires that the Commission, in consultation with FEMA, adopt regulations that "establish a State EAS Plan content checklist for SECCs to use when reviewing and updating a State EAS Plan for submission to the Commission."[66]

1. SECC Provisions

23. We propose to amend the introductory paragraph of section 11.21 of our rules covering State EAS Plans to include language encouraging the chief executive of each state to establish an SECC if the state does not have an SECC, and if the state has an SECC, to review the composition and governance of the SECC.[67] To ensure that this encouragement language reaches state chief executives, however, we further propose to direct the Bureau to directly contact the chief executive of any state lacking a functioning SECC to encourage that state chief executive to form an SECC. In such cases, the Bureau also will work with the relevant state agencies, FEMA and our other federal partners, and EAS Participant representative organizations to help facilitate SECC formation or restoration. To the Commission's knowledge, all states and all but two territories have active SECCs.[68] In addition, we seek comment (below) on additional measures the Commission could take to facilitate the formation of SECCs.

24. With respect to reviewing the composition of SECCs, we observe that the composition and governance information for each SECC is required to be included in the State EAS Plan.[69] While State EAS Plans currently are accessible on the Commission's website, all State EAS Plans will be required to be electronically filed using the Alert Reporting System (ARS) within one year from the date

[63] NDAA21, § 9201(b)(1)(A).

[64] *Id*., § 9201(b)(1)(B)(i).

[65] *Id*., § 9201(b)(1)(B)(ii).

[66] *Id*., § 9201(b)(1)(C).

[67] Given that there are no current rules specifically covering SECCs, we propose to add this provision to the existing rule about State EAS Plans created by such SECCs. *See* proposed amendments to section 11.21, Appendix A (inserting the following language into the introductory paragraph, "The plans are administered by State Emergency Communications Committees. The Commission encourages the chief executive of each State to establish an SECC if their State does not have an SECC, and if the State has an SECC, to review the composition and governance of the SECC.").

[68] Two territories, U.S. Virgin Islands and Northern Mariana Islands, currently lack fully active SECCs. The Bureau already has been working to facilitate SECC formation in those territories, and will work with the relevant territorial agencies, FEMA and local EAS Participants to hasten that result.

[69] *See* 47 CFR § 11.21(a)(7).

notice of such operational status is published in the Federal Register.[70] From that date forward, no State EAS Plan information will be publicly available from the Commission's website except for names and some contact information of the SECC Chairpersons. Instead, the Commission will share State EAS Plan information maintained within the ARS (or otherwise in the Commission's possession) only on a confidential basis with other federal entities and state governmental agencies that have confidentiality protection at least equal to that provided by the Freedom of Information Act (FOIA); the Commission premised this confidential treatment on the notion that disclosure of the plans, at least in form where each plan is one place and in a uniform and easily searchable format, could highlight potential vulnerabilities that malefactors could exploit, thereby potentially hindering emergency planning efforts.[71] Requests from state chief executives to the Commission for the composition and governance information pertaining to the SECC of their states are requests from state governmental entities and, as such, would be covered by this policy's confidentiality requirements for obtaining access to such information. We thus propose that state governments follow the Commission's requirements for access to the State EAS Plans in order to obtain this information or else may request the information directly from the SECCs.

25. In response to the legislation's requirement for regulations requiring SECCs to meet annually to review and update their State EAS Plan, and to certify that such meeting was completed, we propose to amend section 11.21 to include as a required element in the State EAS Plan, a certification by the SECC Chairperson or Vice-Chairperson that the SECC met (in person, via teleconference, or via other methods of conducting virtual meetings) at least once in the twelve months prior to submitting the annual updated plan to review and update their State EAS Plan.[72] We further propose that such certification, if adopted, would be incorporated into the ARS.[73] Section 11.21 already includes a requirement that State EAS Plans be updated annually,[74] and that requirement is incorporated into the ARS as well,[75] however, we propose to add some clarifying language to section 11.21 to more closely reflect the legislation's requirements on this point.[76] We tentatively conclude that the costs associated with these proposals will be far less than the benefits gained. The requirement to certify that the SECC has met in person, via teleconference, or via other methods of conducting virtual meetings at least once annually, for example, would implicate some costs to SECC members. Maintaining communications between SECC members about the status of their State EAS Plan, however, promotes more efficient and accurate administration of

[70] *See Amendment of Part 11 of the Commission's Rules Regarding the Emergency Alert System*, PS Docket No. 15-94, Report and Order, 33 FCC Rcd 3627, 3645-46, para. 54 (2016) (*State Plan Order*).

[71] *See State Plan Order*, 33 FCC Rcd 3634, para. 17.

[72] *See* Appendix A, section 11.21 (proposing to add subparagraph (a)(8), stating "Certification by the SECC Chairperson or Vice-Chairperson that the SECC met (in person, via teleconference, or via other methods of conducting virtual meetings) at least once in the twelve months prior to submitting the annual updated plan to review and update the plan.").

[73] The certification would be included on one of the data entry menus in the ARS, such as the Review and Submit menu which contains the "submit" button that formally submits the plan to the Bureau for review and approval, as the following statement: "CERTIFICATION OF MEETING – By submitting this State EAS Plan to the Commission for review and approval, the SECC Chairperson and Vice-Chairperson certify that the SECC has met (in person, via teleconference, or via other methods of conducting virtual meetings) at least once in the prior twelve months to review and update the plan."

[74] *See* 47 CFR § 11.21(a).

[75] Once a State EAS Plan is approved in ARS, the ARS system sends an email to the SECC Chairperson and Vice-Chairperson 30 days prior to the one-year anniversary of that approval date to notify them that their State EAS Plan must be resubmitted by that one-year anniversary date, and that they have 30 days before that deadline arrives.

[76] *See* Appendix A, section 11.21 (proposing to amend subparagraph (a) to clarify that: "The plans, including each annual updated plan, must be reviewed and approved by the Chief, Public Safety and Homeland Security Bureau, prior to implementation to ensure that they are consistent with national plans, FCC regulations, and EAS operation.").

the plan, which benefits state and local alerting and public safety generally. Many, if not most, SECCs likely already are meeting in some form on a regular basis, and therefore the proposed annual meeting certification likely will certify an activity already being undertaken.

26. We seek comment on the foregoing proposals. Is our proposed approach on encouraging SECC formation sufficient? In addition to working with all interested parties, would it be helpful if the Bureau prepared recommendations for SECC membership and/or developed a model governance structure for SECCs that could be provided to a state executive to help it more easily create a new SECC? Are there other affirmative steps the Commission could take to aid state executives form SECCs where none exist in their state? Are there recurring factors that have prevented the creation and/or maintenance of active SECCs, and are there measures the Commission could take to help address those? Is the Part 11 rule section covering State EAS Plans the appropriate rule section to incorporate the proposed SECC-related amendment or would a different rule section be more appropriate? Should any restrictions be placed upon state-formed SECCs, such as requiring that the positions of SECC Chairperson or Vice-Chairpersons be held only by persons who are not employed by the state government that formed the SECCs, to prevent any appearance that the Commission was improperly regulating State activities? Would incorporating inclusion of the certification discussed above on the ARS as an electronic function (click box) be appropriate, or would a stand-alone certification, uploaded as an attachment render SECC Chairpersons and Vice-Chairpersons more accountable?

27. We also seek comments on the costs and benefits of these proposals. Would our proposal on sharing SECC governance information with state chief executives impose costs on SECCs or others in responding to requests from their states' chief executives for State EAS Plans? Would the benefits of these proposed rule changes offset whatever costs might be imposed on those required to follow them? Are there more efficient and/or less burdensome alternative ways to meet NDAA21's requirements on these matters? Are there other steps (including but not limited to regulatory options) that the Commission could take to encourage jurisdictions that do not have SECCs to form them, and if so, what are such methods and their costs and benefits? Would the SECC meeting requirement impose new costs upon SECCs or other entities? What benefits would be derived from these proposals, and would their value exceed whatever costs might be imposed by them? Are there more efficient and/or less burdensome alternative ways to meet NDAA21's requirements on these matters?

2. State EAS Plan Provisions

28. As described above, the Commission's EAS rules require the filing of a State EAS Plan with the Commission documenting the distribution architecture within the state.[77] The plans are required to include certain information, such as the monitoring assignments for distributing EAS alerts within the state, SECC governance structure, and multilingual alerting activities.[78] Bureau staff reviews the plans to ensure that all required informational elements are included, that there are no apparent internal inconsistencies in the information provided, and that the state and local EAS activities described are consistent with national plans, FCC regulations, and EAS operational parameters. Currently, plans are submitted in paper or soft file format. The Bureau reviews the plans and if defects are found, the Bureau contacts the SECC to identify the defects, propose corrections, and request that the SECC revise their plan accordingly and resubmit the corrected version. This process can vary in duration depending upon how long the SECC takes to correct and resubmit a revised plan.

29. With respect to the legislation's requirement for regulations that require the Commission to approve or reject an updated State EAS Plan within 60 days of receipt, and to notify the State's chief executive of such decision and reasons therefor, we propose to add language to section 11.21 of our rules requiring that the Bureau approve or reject State EAS Plans submitted for approval within 60 days of

[77] *See* 47 CFR § 11.21.

[78] *See id*.

receipt, and that the approval dates of State EAS Plans will be listed on the Commission's website (which chief executives of states and the public generally can view, if desired).[79]

30. We observe that State EAS Plans filed in ARS will be reviewed by the Bureau. If deficiencies are found, the plan will be rejected, and the ARS will generate and send an email to the SECC Chairperson and Vice-chairperson, notifying them of the rejection along with the reviewer's comments identifying the errors and required corrections, and the need to resubmit a corrected version. In such cases, the overall back-and-forth process of submission and resubmission may exceed 60 days, depending on how long the SECC takes to complete the necessary work to correct and resubmit their rejected plan. As we believe the intent of the statute is to ensure that the Commission completes its review in a timely fashion, not to pressure SECC's into making snap decisions about state and local EAS procedures, we propose that for those instances in which the Bureau finds defects in a submitted plan and the SECC considers and implements the Bureau's feedback, we would consider the State EAS Plan to be temporarily withdrawn, restarting the 60-day review and approval period anew upon resubmission in ARS. We anticipate that, under this approach, State EAS Plans would only be formally rejected by the Bureau in those rare instances in which an SECC declines to correct defects that the Bureau identified in a State EAS Plan or fails to respond at all.

31. We seek comment on this proposal. Would this approach impose additional costs to SECCs or other entities? Are there more efficient and/or less burdensome alternative ways to meet NDAA21's requirements on this matter? For example, would it be more efficient, rather than restarting the 60-day decision clock to day one upon plan resubmission, to merely pause the clock when feedback was provided to an SECC and resume the clock upon resubmission of the plan in ARS?

32. In terms of notifying State chief executives of decisions and accompanying rationales to reject or approve plan submissions, we tentatively propose to list on our website the dates of State EAS Plan approvals issued by the Bureau so that state chief executives can track their status, if they desire. That listing would indicate that the plan has been found to be compliant with the Commission's rules. In our experience with prior review of these State EAS Plans, it is unlikely that a plan will be rejected by the Bureau, however, we propose that, if such a rejection should occur, the Bureau would directly notify the chief executive of that determination and state the reason for such rejection. Consistent with the above-proposed approach to the timing of determinations on plans, we anticipate that State chief executives would only need or desire to be notified about the Bureau's final determinations on plans and not the Bureau's requests for corrections, which may address simple issues such as clerical errors or misreading of the required information.

33. We seek comment on this proposal. Is there any reason why state chief executives should be notified about Bureau requests for plan revisions? Is listing the dates of approval of State EAS Plans submitted for approval a sufficient mechanism to notify State chief executives of such status? Would this approach impose additional costs to anyone? Are there more efficient and/or less burdensome alternative ways to meet NDAA21's requirements on this matter?

34. With respect to the legislation's requirement for regulations that "establish a State EAS Plan content checklist for SECCs to use when reviewing and updating a State EAS Plan for submission to the Commission," we observe that section 11.21 already includes a listing of information required in the State EAS Plan, and the ARS data entry menus mirror these informational requirements (and will not

[79] *See* Appendix A, section 11.21 (proposing to add the following sentences to subparagraph (a): "Plans, including annual updated plans, submitted for approval will be reviewed and approved within 60 days of receipt, provided that no defects are found requiring the plan to be returned to the SECC for correction and resubmission. If a plan submitted for approval is found defective, the SECC will be notified of the required corrections, and the corrected plan may be resubmitted for approval, thus starting the 60-day review and approval period anew. The approval dates of State EAS Plans will be listed on the Commission's website.").

allow a State EAS Plan to be submitted unless all required fields are completed).[80] We propose, however, to create a checklist, to be posted on our website, and incorporated into the ARS user manual[81] that identifies the information required in each ARS section that will provide the corresponding explanation of what that information requirement entails, as expressed in the *State Plan Order* wherein the ARS filing mechanism was adopted.[82] We seek comment on this approach. Are there any practical reasons why the checklist explaining the required content of State EAS Plans set forth in section 11.21 and the ARS should be made available in some form other than a separate document? Should the checklist also be referenced in Section 11.21 or reproduced there? Would this approach impose additional costs to anyone? Do commenters believe that the statute envisioned something more or different than what the Commission proposes here? For example, should the checklist be codified in the section 11.21 (governing State EAS Plans) in addition to the measures we propose here? Are there more efficient and/or less burdensome alternative ways to meet NDAA21's requirements on this matter? Is there other information that should be included as part of the checklist?

C. Reporting of False Alerts

35. The NDAA21 requires the Commission to "establish a system to receive from the Administrator or State, Tribal, or local governments reports of false alerts under the Emergency Alert System or the Wireless Emergency Alerts System for the purpose of recording such false alerts and examining the causes of such false alerts."[83] An impetus for this requirement was an incident that occurred in January 2018, in which the Hawaii Emergency Management Agency mistakenly issued an emergency alert through IPAWS that warned the public of a non-existent inbound ballistic missile attack.[84]

36. In response to the Hawaii false missile alert, the Commission adopted a requirement that EAS Participants report false EAS alerts to the FCC Operations Center at FCCOPS@fcc.gov.[85] The Commission sought further comment on whether it should establish a system for other stakeholders, such as emergency managers or members of the public, to report EAS and WEA false alerts; however, to date, no such system has been established. Accordingly, there currently is no formal system or procedure for FEMA or State, Tribal, local, or territorial governments to report false EAS or WEA transmissions to the Commission. Of course, such entities are free to report these events to the Commission, including through the informal complaint process, if such alerts are transmitted by third parties.[86]

---

[80] *See* 47 CFR § 11.21. The ARS data entry menus standardize monitoring and other common elements of State EAS Plans, while offering sufficient flexibility to accommodate non-standardized EAS deployment and operational elements.

[81] We observe that each ARS menu has a help button that brings up the ARS user manual section for that menu. The checklist information can be included in the user manual on a section-by-section basis, making the relevant portions for each ARS menu accessible as needed. In addition, the checklist can be included in the ARS user manual as an appendix.

[82] *See State Plan Order*, 33 FCC Rcd 3637-42, paras. 32-46.

[83] NDAA21, § 9201(c).

[84] *See Amendment of Part 11 of the Commission's Rules Regarding the Emergency Alert System; Wireless Emergency Alerts*, PS Docket 15-94, Report and Order and Further Notice of Proposed Rulemaking, 33 FCC Rcd 7086, 7089, para. 4 and n. 15 (2018) (*Alerting Reliability Order and FNPRM*). *See also* H.R. Rep. No 116-582, at 2-3 (2020); S. Rep. No. 116-240, at 3-4 (2020) (noting that "[f]alse emergency alerts like [Hawaii] threaten the credibility of emergency alert messaging and Americans' response to such alerts, which could be catastrophic in the event of a real emergency").

[85] *See Alerting Reliability Order and FNPRM*, 33 FCC Rcd at 7094-95, paras. 17-18. This reporting requirement is codified in section 11.45(b) of our rules, 47 CFR § 11.45(b).

[86] *See Alerting Reliability Order and FNPRM*, 33 FCC Rcd 7103, para. 41.

37. We propose to revise both Parts 10 and 11 of our rules to formalize and enlarge the process by which government entities may submit reports of false alerts to the Commission. Specifically, we propose to add rule sections to state that, if the Administrator of FEMA or a State, Tribal, local, or territorial government entity becomes aware of transmission of an EAS or WEA false alert to the public, they are encouraged to send an email to the Commission at the FCC Ops Center at FCCOPS@fcc.gov, informing the Commission of the false alert event and of any details that they may have concerning the event.[87] Under this rule, government entities may report any false alerts they become aware of (regardless of whether those entities originated the false alerts). Furthermore, currently, EAS industry participants must report EAS false alerts when they have "transmitted or otherwise sent" a false alert.[88] We propose to revise section 11.45(b), which describes this false alert reporting requirement for EAS Participants, to add the word "shall" to further distinguish between the required reporting by EAS Participants of false alerts and the voluntary reporting mechanism for the Administrator of FEMA or a State, Tribal, local, or territorial government that we propose today.[89] We seek comment on these proposals.

38. We believe our proposed approach conforms to both the text and underlying intent of the statute, while also giving appropriate deference to the discretion of the FEMA Administrator or State, Tribal, local, or territorial governments. We also believe our proposed approach will best facilitate the receipt of reports of false alerts from FEMA or State, Tribal, local, or territorial governments, creating minimal burden on these entities to submit these voluntary reports. In particular, we note that establishing a reporting system for receipt of these reports via email directed to the Commission's Operations Center is the most efficient, and least onerous method to implement this system since it can be implemented immediately with minimum complexity. We seek comment on this determination and any alternative approaches. Specifically, would a formal web-based interface or electronic filing system provide greater benefits than using a direct email method? If so, what are those benefits and what form should such a system take? Would the costs and time to develop and construct such a system outweigh those benefits? Would a more complex web-based or electronic filing system interface deter reporting of false alerts or unnecessarily delay the availability of the reporting system to government entities? We seek comment on these questions and whether there are more efficient and/or less burdensome alternative ways to meet NDAA21's requirements on this matter.

39. We believe that requesting "any details . . .concerning the event" rather than a specified list of requested information will best encourage prompt reporting of false alert events. We seek comment on this assessment. Should we instead request specific minimum details regarding the false alert for the purpose of "examining the causes of such false alerts?"[90] If so, what details should be requested to enable the Commission to best track and examine the cause of a false alert? Should we instead provide a template of specific optional questions government entities are requested to answer, either as a list of questions on the Commission's web site or using a web form system?

40. Finally, we note that our existing rules do not provide a definition of "false alerts"[91] nor is the term defined in the NDAA21. Currently, section 11.45(a) of our rules states "No person may transmit or cause to transmit the EAS codes or Attention Signal, or a recording or simulation thereof, in any

[87] *See* Appendix A, proposed rules 47 CFR § 10.520(d)(1) and 11.45(c). These two proposed rules are identical except for reference to either EAS or WEA, and read as follows: "If the Administrator of FEMA or a State, Tribal, local or territorial government entity becomes aware of transmission of a [WEA or EAS] false alert to the public, they are encouraged to send an email to the Commission at the FCC Ops Center at FCCOPS@fcc.gov, informing the Commission of the event and of any details that they may have concerning the event."

[88] 47 CFR 11.45(b).

[89] *See* Appendix A, proposed rule 47 CFR § 11.45(b).

[90] NDAA21, § 9201(c).

[91] *See* 47 CFR § 11.45.

circumstance other than in an actual National, State or Local Area emergency or authorized test of the EAS."[92] Importantly, our proposal for government entity reporting of false alerts is not intended to alter the purpose of section 11.45(a). For purposes of our proposal, a "false alert" would include alerts that are transmitted in circumstances that are not an actual emergency or test. As discussed above, we observe that the legislation's impetus for establishing a system for reporting false alerts are those incidents like the false missile alert that threaten the credibility of emergency alert messaging and Americans' response to such alerts.[93] Nevertheless, we do not propose to define "false alerts" here since doing so may deter government entities from reporting a false alert when they may believe in good faith that a false alert was transmitted. We seek comment on this determination and ask whether our rules should include a definition of "false alerts." In this regard, should any definition of a false alert be necessarily limited to events like the Hawaii false missile alert (*i.e.*, an event that is not actually happening anywhere in the U.S. at the time of the alert). If not, why not and what alternative definition do commenters propose and why?

D. Repeating EAS Messages for National Security

41. Section 9201 of NDAA21 requires the Commission, in consultation with FEMA, to "complete a rulemaking proceeding to modify the [EAS] to provide for repeating [EAS] messages while an alert remains pending that is issued by [] (A) the President; (B) the Administrator; or (C) any other entity determined appropriate under the circumstances by the Commission, in consultation with [FEMA]."[94] Section 9201 further specifies that the "[s]cope of [this] rulemaking . . . shall [] (A) apply to warnings of national security events, meaning emergencies of national significance, such as a missile threat, terror attack, or other act of war or threat to public safety; and (B) not apply to more typical warnings, such as a weather alert, AMBER Alert, or disaster alert."[95] Finally, Section 9201 specifies with respect to this rulemaking obligation that "[n]othing in this subsection shall be construed to impair, limit, or otherwise change [] (A) the authority of the President granted by law to alert and warn the public; or (B) the role of the President as commander-in-chief with respect to the identification, dissemination, notification, or alerting of information of missile threats against the United States, or threats to public safety."[96]

42. We observe that the EAS is designed to provide for repeating alerts by any entity authorized to originate alerts (not just those identified in the three categories set out in the statute). Specifically, any EAS alert originators can reissue an alert without it being rejected as a duplicate alert by downstream monitoring EAS Participants,[97] provided that it is transmitted at least one minute subsequent to the initial alert's initiation, as reflected in the alert's time stamp.[98] If the alert originator wanted the valid time period (i.e., the time period during which the alert warning is in effect) in the original alert to be reflected in the repeated version of that alert, it also would need to revise the valid time period of the repeat alert to account for the elapsed time between when the original alert was sent and when the repeat

[92] *Id*., § 11.45(a).

[93] H.R. Rep. No 116-582, at 2-3 (2020); S. Rep. No. 116-240, at 3-4 (2020). *See also Alerting Reliability Order and FNPRM*, 33 FCC Rcd at 7094-95, paras. 17-18.

[94] NDAA21, § 9201(d)(1).

[95] *Id*., § 9201(d)(2).

[96] *Id*., § 9201(d)(3).

[97] *See* 47 CFR § 11.33(a)(10).

[98] An EAS alert's header codes include a data field called "JJJHHMM," which indicates the day in Julian Calendar days (JJJ) of the year and the time in hours and minutes (HHMM) when the message was initially released by the alert originator using 24-hour Universal Coordinated Time. *See* 47 CFR § 11.31(c). Thus, for example, an alert released at 5:00 PM on July 4, 2021, could be reissued by the alert originator at 5:15, 5:30 and 5:45, provided that the JJJHHMM header code for each was set at 1851715, 1851730 and 1851745, respectively. *See id*.

of that alert was sent[99]—otherwise, the repeat alert would continually extend the valid time period associated with the original alert being repeated.[100] We further observe, however, that this capability to repeat alerts may not be fully understood within the alert originator community.

43. Accordingly, we propose to keep the current EAS rules governing alert (re)transmission intact, but modify section 11.33(a)(10) (governing alert validation) by adding language to specify how alert originators can repeat their alert transmissions.[101] This approach appears to meet the legislation's requirements. While we acknowledge the legislation's language that the scope of this rulemaking excludes "typical warnings, such as a weather alert, AMBER Alert, or disaster alert,"[102] we observe again that the EAS already provides for repeating any and all EAS alerts, if the alert originator deems the particular circumstances warrant such action, and we do not read the legislation's language as requiring *removal* of that capability. Under our approach, members of the public who miss an alert because, for example, they stepped away from their television for a moment, may yet experience the alert when repeated by the alert originator. Further, this applies not just to alerts expressly captured under the legislation, such as missile alerts, but also tsunami alerts, and all other state and local alerts that may or may not have national significance, but which are nonetheless significant to people in the affected areas. We believe this approach maximizes the functional utility of the EAS to deliver public warnings, and thus maximizes public safety.

44. We do not read the legislation as directing the adoption of rules requiring or enabling automated repetition of alerts related to national security events.[103] We nevertheless suspect that

[99] The valid time period of the alert is the time period during which the alert warning is in effect. When the valid time period has expired, the warning is no longer in effect because the underlying threat is anticipated by the alert originator to have passed by that time. This time period is included in the EAS alert's header codes as a data field called "+TTTT," which establishes the valid time period of the alert in 15-minute segments for the first hour and then in 30-minute segments thereafter. *See* 47 CFR § 11.31(c). If the alert originator wanted to repeat an alert but retain the valid time period in the original alert, it would need to revise the valid time period "+TTTT" header code data to account for the elapsed time from when the original version was sent and when the repeat alert is sent. *See id*. For example, if the original alert was released at 5:00 PM on July 4, 2021, with a one-hour valid time period (i.e., with the +TTTT code set at +0100, so that the valid time period was 5:00 PM until 6:00 PM) and the first repeat alert was issued at 5:15, the repeat alert would require a valid time period set at 45 minutes (i.e., a +TTTT code set at +0045, to keep the end of the valid time period at 6:00 PM) because 15 minutes have expired since the original alert was sent. *See id*. Repeat intervals that do not match the time settings available in the +TTTT code options, however, would not always be capable of accurately reflecting the change in the original valid time period in the case of alerts issued using the legacy EAS. The Common Alerting Protocol offers more flexibility for short time intervals due to the way it converts the valid time period to the legacy EAS format, but can still result in an inaccurate reflection of the valid time period of the original alert being repeated. *See* ECIG Implementation Guide, § 3.4.1.4.)

[100] For example, using the example above, if the if the original alert was released at 5:00 PM on July 4, 2021, with a one-hour valid time period (i.e., with the +TTTT code set at +0100) and the first repeat alert was issued at 5:15, but the valid time period was not changed (i.e., the +TTTT code remained set at +0100), the valid time period of the repeat alert would be one hour, or 5:15 PM to 6:15 PM.

[101] *See* Appendix A, section 11.33 (proposing to amend subparagraph (a)(10) to add the following sentence: "An alert repeated by the alert originator that was released at least one minute subsequent to the original alert's initiation, as reflected in the repeat alert's JJJHHMM header code, shall not be treated as a duplicate.").

[102] NDAA21, § 9201(d)(2)(B).

[103] In this regard, NDAA21 directs the Commission to "modify the Emergency Alert System to provide for repeating Emergency Alert System messages while an alert remains pending …" NDAA21, § 9201(d)(1). As indicated, the EAS currently provides for alert repetition, though this function may not be well understood by alert originators or EAS Participants. Such repetition can be effected "while an alert remains pending," or put in EAS terms, while the valid time period of that alert is in effect (though, as explained above, some technical limitations exist with respect to repeating alerts and maintaining the exact termination time of the valid time period expressed in the initial version (continued….)

automating repetition of Common Alerting Protocol-formatted alerts—including the setting of repetition intervals to occur within the valid time period established for the initial alert, to the extent feasible—via the various commercial alerting origination and management software programs in use today, should be achievable with minimal changes to such software packages.[104] In addition, we believe FEMA could integrate an automated alert repeating function (all set to occur within the valid time period established for the initial alert, to the extent feasible) within IPAWS in the event it elected to originate EAS alerts, and/or could simply issue and reissue Common Alerting Protocol-formatted EAS alerts via IPAWS manually.

45. We seek comment on this proposed approach. Does this approach sufficiently capture the legislation's provisions on alert repetition? Is this approach beneficial to alert originators? Would any additional rule changes be helpful to enable alert originators to repeat their alerts? Would widespread repetition of state and local alerts cause alert fatigue and/or EAS Participants to stop processing some or all state and local alerts? Has the specter of such result caused alert originators to refrain from repeating alerts they otherwise would? Should alert repetition be limited in some fashion? Does section 11.51(n) of the EAS rules, which provides EAS Participants with a 15-minute window to transmit state and local alerts, present any obstacles to repeating alerts at intervals less than 15 minutes?[105] Would our proposed approach impose additional costs to anyone? Are there more efficient and/or less burdensome alternative ways to meet NDAA21's provisions on this matter? While we do not read the legislation as requiring automated repetition of the national security alert, we seek comments on what costs would be involved with modifying existing EAS device models to enable alert originators to select automatic repetition of the alerts they originate via both the Common Alerting Protocol and legacy methods. Would the EAS devices also need to be modified to allow the alert originator to select a repeat interval, and at what costs for which entities?

46. We observe that, from a functional standpoint, our proposed approach would not require adoption of a new originator code to identify that a given alert is being issued by FEMA or other alert originator authorized by the Commission and FEMA to issue alerts, nor would it be necessary to adopt a new event code covering national security events.[106] However, to more closely track and codify the language of the legislation, one or both codes could be added to the EAS Protocol.[107] Accordingly, in the alternative to relying solely upon the addition of clarifying language to section 11.33(a)(10) proposed above, we seek comment on whether to also add a new originator code and a new event code to more accurately reflect the scope of the legislation. Specifically, the Commission could adopt a new alert originator code called the National Command Authority (NCA) code that would encompass FEMA, and other entities determined appropriate under the circumstances by the Commission, in consultation with

---

of the alert being repeated). The plain language of section 9201(d)(1) does not call for automated repetition by the alert originator or by EAS Participants. While we anticipate that automated repetition could be implemented in alert origination software, incorporating such automated functionality into EAS devices operated by EAS Participants likely would entail significant modifications to those devices and possibly other systems that interface with the EAS. We seek comment on the modifications such automated repetition would entail below.

[104] It is unclear whether any or all EAS encoder/decoder device models currently deployed could be programmed to enable alert originators to repeat EAS alerts they originate, as such alerts are typically initiated through manual entry of the alert data and audio. We suspect that many encoder/decoder models would require modifications to achieve this capability.

[105] 47 CFR § 11.51(n).

[106] For Common Alerting Protocol-formatted alerts issued through IPAWS, FEMA could use the PEP originator code and Civil Danger Warning (or Civil Emergency Message (CEM)) event code. The same codes could be used if FEMA were to issue the national security alert using the legacy EAS.

[107] *See* 47 CFR § 11.31(d) (listing the originator codes authorized for use with the EAS), (e) (listing the event codes authorized for use with the EAS).

FEMA.[108] Entities so designated by the Commission in consultation with FEMA would be limited to entities authorized to issue alerts related to national security events. In addition, we could add a new event code for national security event-related alerts issued by FEMA (or other entities designated by the Commission in consultation with FEMA) called the National Security Event (NSE) event code that would encompass "warnings of national security events, meaning emergencies of national significance, such as a missile threat, terror attack, or other act of war or threat to public safety."[109]

47. Adoption of an alert event dedicated to national security events could more accurately categorize such warnings within the EAS ecosystem.[110] The missile alert mistakenly issued in Hawaii, for example, was issued under the state and local Civil Danger Warning (CDW) event code.[111] Absent adoption of an event code dedicated to national security events, a missile alert issued by FEMA also would have to use an existing state and local catch-all event code, such as the Civil Danger Warning or Civil Emergency Message event codes, which could pertain to any number of emergencies.[112] Because visual scrolls are derived from the EAS alert header codes, the visual scroll would show a civil defense warning issued by whatever originator code was used (if the NCA originator code were adopted, this would be "national command authorities"; if not, the "CIV" originator code for "national authorities" likely would be used).[113] While adoption of the catch-all NSE event code would not be more specific as to the underlying threat, it would be national or regional in scope, and the visual scroll would identify that it was a national security event issued by national command authorities (assuming the NCA originator code also was adopted).[114] That additional information might make the public more attentive to such an alert, and thus enhance its effectiveness.

48. We seek comment on this alternative proposal. Is it desirable from an operational standpoint to adopt a new originator code for FEMA or other alert originator authorized by the Commission in consultation with FEMA to issue alerts, and/or a new event code covering national security events? Would such approach better reflect the legislation's provisions on repeating alerts than relying solely upon clarifying the existing EAS rules on duplicate alerts? If we were to adopt such codes, are the titles proposed sufficient? Would such actions require any changes to NWS/National Weather Radio (NWR) systems or consumer devices they serve? Would such change require amending the ECIG Implementation Guide? Could such codes be implemented in the deployed base of EAS devices via software updates? Would the adoption of the NSA code create confusion when used for events that currently would fall under other event codes? If the existing NIC event code could be repurposed for use

[108] *See* NDAA21, § 9201(d)(1).

[109] *Id*., § 9201(d)(2)(A).

[110] Currently, the only non-test event code with a national scope in use in the EAS is the Emergency Action Notification alert. (There is a national event code called National Information Center (NIC), however, this code was intended for use in connection with an Emergency Action Notification alert.) It is possible that the NIC code could be repurposed for use as a national security alert event code in lieu of adopting a new national security event code. The remaining event codes fall under the "State and local" event category. *See* 47 CFR § 11.31(e) (listing the national and state and local event codes authorized for use in the EAS).

[111] *See* Report and Recommendations; Hawaii Emergency Management Agency January 13, 2018 False Alert, at n.55 (PSHSB 2018), https://www.fcc.gov/document/fcc-releases-report-hawaii-false-emergency-alert.

[112] *See* 47 CFR § 11.31(e).

[113] *See*, *e.g*., 47 CFR § 11.51(d), (g)(3), (h)(3), (j)(2).

[114] The audio message issued by the alert originator likely would indicate, among other things, the name of that originating entity (although if the NCA originator code was adopted, that generic name might be used instead) along with the specific threat (e.g., missile alert). We observe, however, that if no audio message is provided, audio typically can be derived by EAS devices from the header codes using Text-to-Speech. In such cases, using the NCA and NSE codes in tandem may be more effective in conveying to the public the nature, scope and urgency of the warning, even if the specific threat in issue is not articulated.

as an event code for national security alerts, would that be a less burdensome approach than adopting a new event code to cover such alerts? How much time would be required to facilitate addition of one or both of these codes? Would adoption of a new originator code and/or event code impose costs upon EAS Participants or other entities?[115] Would adoption of a new originator code and/or event code require modifications to equipment downstream from the EAS device at the EAS Participant's facilities and/or revision of equipment standards that govern their design, and if so, at what cost? If a new originator code and/or event code were adopted, should EAS Participants be required to install one or both of the codes into their EAS devices, and if so, on what legal grounds?

49. We tentatively propose that, under our proposed rules, Presidential alerts—i.e., Emergency Action Notification alerts—may only be repeated by the President or the President's authorized designee. If the President desires to repeat his or her alert message, in whole or in part, that functionality already exists within the EAS—and in the President's case, can be effected multiple ways. For example, once the President issues an Emergency Action Notification alert, he or she maintains control of EAS Participants' audio transmissions for as long as the President deems necessary (i.e., until the President issues an EOM code), thus allowing for multiple audio addresses to be made during a single Emergency Action Notification event. Alternatively, the President could issue and repeat Emergency Action Notification alerts using prerecorded audio (or issue a single Emergency Action Notification alert with prerecorded audio message that repeats itself). In light of these existing mechanisms, we seek comment on our proposal to limit the issuance of repeated Presidential alerts to the President or the President's authorized designee.

50. We tentatively find that requiring EAS Participants' EAS equipment to automatically repeat the Presidential alert would present technical impediments that would impair the President's ability to issue Emergency Action Notification alerts, which is inconsistent with NDAA21's provisions.[116] As an initial matter, Emergency Action Notification alerts are not time-limited.[117] While most encoder/decoder EAS device models can originate alerts manually, it is likely that significant programming changes would be required to many such models to facilitate automatic repeat (or re-origination) functionality, which is not a systemic function designed into the EAS architecture. Downstream equipment at the EAS Participant's facilities devices (that process the output of the EAS device to generate the visual crawl, insert the audio into a station's main transmit audio channel, etc.) could be implicated as well. Beyond that, the EAS is designed for Emergency Action Notification alerts to be terminated by their associated EOM code. It is unclear what would happen within the EAS systemically if a new Emergency Action Notification alert was received while a repeat Emergency Action Notification alert was in progress; the EAS is not designed to function that way and there are no provisions in the EAS rules that cover such

[115] We observe that the cost to EAS Participants of adding the extreme wind and storm surge event codes, and revising the territorial boundaries of two geographic location codes for two offshore marine areas, in 2016 was estimated by the Commission, based on the record before it, to be one hour of labor (to download software patches into their devices and associated clerical work). *See Amendment of Part 11 of the Commission's Rules Regarding the Emergency Alert System*, PS Docket No. 15-94, Report and Order, 31 FCC Rcd 7915, 7924, para. 23 (2016). The Commission further found that even using a worst-case cost figure of $125.00 per device, the aggregate cost of all EAS Participants adopting the codes would be approximately $3.5 million, which it concluded was far outweighed by the benefit of saving a single life, using the VSL then estimated at $9.1 million. *See id*., 31 FCC Rcd 7925, para. 24. *See also Blue Alert Order*, 32 FCC Rcd 10812, 10824-25, para. 25 (wherein the Commission concluded that the cost of implementing the BLU (blue alert) event code was the cost of downloading a software update into the EAS device and conducting associated testing, for a total, worst-case, aggregate cost, if all EAS Participants installed the BLU event code, of $3.5 million).

[116] *See* NDAA21, § 9201(d)(3) (stating "[n]othing in this subsection shall be construed to impair, limit, or otherwise change … the authority of the President granted by law to alert and warn the public …").

[117] *See*, *e.g*., 47 CFR § 11.33(a)(9) (requiring disabling the EAS device reset function when receiving Emergency Action Notification alerts so that lengthy audio can be received).

scenario.[118] Ensuring consistent handling across all EAS device models likely would involve modifications to some or all.

51. There also is a lack of synchronization between alerts issued via the legacy EAS and Common Alerting Protocol-formatted EAS alerts issued through IPAWS.[119] These timing disparities create opportunities for errors in repeating Emergency Action Notification alerts (or any other EAS alert), which could hamper the President's ability to use the EAS to deliver Presidential alerts.[120]

---

[118] On the contrary, the EAS rules require Emergency Action Notification alerts to be transmitted "immediately" (*see*, *e.g.*, 47 CFR §§ 11.2(a), 11.51(n)) and require the EOM for an Emergency Action Notification alert to terminate an Emergency Action Notification alert in progress (*see* 47 CFR § 11.33(a)(9)), which could cause a chaotic system-wide reaction where some encoder/decoder models might interrupt the automated repeat of an Emergency Action Notification alert originated in the encoder/decoder and others to buffer the incoming Emergency Action Notification alert until the Emergency Action Notification alert in progress is terminated by its EOM code.

[119] Each monitored station in the daisy chain of legacy EAS alert distribution regenerates the EAS header codes and attention signal, which takes approximately 14 seconds. Because the audio message begins after the codes and attention signal, the audio message from the first station to air the alert begins around 14 seconds; the audio message from the second station to air the alert also begins around 14 seconds into the alert, but 28 seconds after the alert was initiated by the first station; and the audio message aired by the third station to air the alert also begins around 14 seconds into the alert, but 42 seconds after the alert was initiated by the first station If the audio is "live" streaming audio, as would be likely in a legacy Emergency Action Notification alert, if the president were to begin talking directly after the initial 14-seconds of header codes and attention signal was complete, by the time the third station got to airing that audio, it would capture that audio from the 28-second mark—having missed the initial 28 seconds due to the time it took for the second station and third station to air the header codes and attention signal. *See* CSRIC IV, Working Group 3, National Testing and Operational Issues Task Group, Final Report, Annex C (2014), https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG-3_Final-Report_061814.pdf; *see also* FCC White Paper, The Capacity of the Integrated Public Alert and Warning System to Deliver Sensor-Based Earthquake Early Warnings: An Engineering Analysis, at 41 (2016: PSHSB), https://transition.fcc.gov/bureaus/pshs/eas/Earthquake_Alert_WhitePaper-120216.pdf (*EEW White Paper*). Receipt of Common Alerting Protocol-formatted alerts are dependent upon the polling cycle set by the EAS Participant in their EAS device for checking IPAWS for new Common Alerting Protocol-formatted EAS alerts. Typical EAS device configurations set the polling rate between 30 and 60 seconds. *See EEW White Paper* at 42.

[120] For example, if a Common Alerting Protocol cancellation message or new Common Alerting Protocol-formatted Emergency Action Notification alert was placed on the IPAWS EAS server, and the Internet went down throughout portions of the country 25 seconds later, some EAS Participants would retrieve that message or alert and others would not (because there is no fixed polling cycle among EAS Participants' EAS devices for querying the IPAWS EAS servers), leaving some EAS Participants to cancel the repeating alert (if a Common Alerting Protocol cancellation message was issued) but others to continue repeating the alert. If a new Common Alerting Protocol-formatted Emergency Action Notification alert were issued (instead of a Common Alerting Protocol cancellation message), the same result would obtain, because while that Common Alerting Protocol-formatted alert will have been converted into and transmitted as a legacy alert by the EAS Participants that received the Common Alerting Protocol-formatted alert, those legacy transmissions will activate throughout only portions of the country. If the Common Alerting Protocol-formatted Emergency Action Notification alert was simultaneously issued via the legacy EAS, with both versions having identical header code information, the legacy Emergency Action Notification alert may be received by those EAS Participants that did not receive the Common Alerting Protocol-formatted version from IPAWS (or the legacy version from those EAS Participants that did receive the Common Alerting Protocol-formatted version), but if the EAS Participant's EAS device started the repeat of the original Emergency Action Notification alert before that legacy Emergency Action Notification alert was received, that legacy version would be rejected because the internally repeated EAN would have a more recent time stamp (any EAS alert generated as a repeat inside an EAS device would have to set the time stamp for that repeated alert at the repeat interval time to prevent duplicate alerts from airing throughout the EAS system). This scenario is not unlikely, given how long it takes for legacy EAS alerts to activate throughout the EAS system. The timing disparities are not just due to the differing nature of the Common Alerting Protocol-based EAS (which is delivered over IP connections) versus legacy EAS (which is delivered over the air), but also to EAS device output processing delays from downstream

(continued….)

52. Further, requiring some predetermined interval of automatic repetition of an Emergency Action Notification alert by the EAS device would impair the President from reacting to fast-moving emergency events where circumstances may be changing rapidly. For legacy EAS alerts, there is no mechanism in the EAS Protocol for identifying repeating intervals, and adding one would require modifying the EAS Protocol, which potentially could negatively impact NWS/NWR systems used to transmit critical weather warnings to the public as well as weather radios of consumers, schools, local and state emergency management authorities and first responders. While repeat intervals could be communicated in Common Alerting Protocol-formatted alerts with an extension to the Common Alerting Protocol format, an Emergency Action Notification alert most likely would be issued using the legacy EAS.[121] Adopting a single repeat interval for Emergency Action Notification alerts is not practical. Emergency Action Notification alerts may be very long in duration and there is a range of emergencies that might cause the President to issue an Emergency Action Notification alert, thus, it is unclear what single preset repeat interval would be appropriate for all occasions.

53. Based on the foregoing, we seek comment on our analysis and proposal that only the President or the President's authorized designee may repeat his or her Emergency Action Notification alerts, and those repeat Emergency Action Notification alerts must be initiated by the President. We believe that the Commission's authority permits it to require EAS Participants to repeat Emergency Action Notification alerts (if it is technically feasible to do so) and seek comment on our view. Is it technically feasible for any entity other than the President to repeat an Emergency Action Notification alert within the EAS system? What changes to the EAS rules would be required to facilitate such repetition? Would such rule changes require changes to EAS devices, downstream processing equipment, and NWS/NWR systems and the various consumer and enterprise radios that receive NWR transmissions? Could such equipment changes be effected via software updates or would firmware and/or hardware changes also be required? How long would such changes take to implement and at what costs to EAS Participants and/or other entities? Would equipment standards for downstream equipment need to be revised to accommodate Emergency Action Notification alert repetition in EAS devices? If so, how long would that take? What benefits would be derived from requiring EAS devices to repeat Emergency Action Notification alerts? Would those benefits outweigh the costs in enabling such repetition? Could the EAS Protocol be revised to enable sending repeat interval information and Emergency Action Notification alert cancellation data via the legacy EAS? What impact would such action have on EAS devices, downstream processing equipment, NWS/NWR systems and the various consumer and enterprise radios that receive NWR transmissions? To the extent any such equipment would need to be modified, what would the costs of such modification be and who would bear them? Would the benefits of such action outweigh the costs involved? Is there a single repeat interval for Emergency Action Notification alerts that would function well for any emergency condition that might cause the President to issue an Emergency Action Notification alert?

54. We also seek comment on whether automatic (or manual) repetition of national security alerts by EAS Participants' EAS devices is technically feasible within the EAS architecture. As an initial matter, requiring special treatment of national security alerts in the form of automatic repetition would require adoption of an event code for national security alerts so that EAS devices know which alert would

equipment. *See EEW White Paper* at 15-16 (observing that EAS Participant services—including TV broadcast, coax, fiber and wireless cable service, radio, satellite, etc.—utilize different transmission systems, equipment and standards, resulting in downstream equipment processing delays from 5 seconds to two minutes before the EAS device output is transmitted to the EAS Participant's audience).

[121] Currently, although the Common Alerting Protocol can be used to deliver Emergency Action Notification alerts with prerecorded audio files, there are no procedures in place for processing Common Alerting Protocol-formatted Emergency Action Notification alerts with streaming "live" audio. By contrast, the legacy EAS, which is more resilient than Common Alerting Protocol-based alerting, is designed precisely to enable the President to address the public live without time limitation.

have to be repeated. Many of the technical roadblocks to requiring automatic repeats of Emergency Action Notification alerts would appear to apply to repeating the national security alert if regular alert processing procedures applied. For example, because the legacy EAS is incapable of relaying a repeat interval period or cancelling a repeat requirement for a national security alert, relaying such information would be limited to the Common Alerting Protocol or require adoption of a fixed repetition interval that would apply to national security alerts regardless of whether that interval made sense for the alert's underlying circumstances. If Internet problems prevented some or all EAS Participants from accessing the IPAWS EAS server, there would be no mechanism to communicate an alert cancellation to those EAS Participants (assuming they received the initial alert to begin with). Further, because Common Alerting Protocol alerts are required to be converted and transmitted as legacy EAS alerts, the repeat version of the national security alert transmitted by EAS Participants that could not receive the cancellation message from IPAWS would restart the alert within the EAS system (because the time stamp and valid time period code of the repeated version would be different than the original version of the alert). Incorporating the capability to relay alert cancellation and repeat interval information into the legacy EAS would require modifying the EAS Protocol and modifying 27,000+ EAS devices deployed in EAS Participant facilities across the country, not including any changes that might be required to NWS systems or processing equipment at the EAS Participant facilities downstream from the EAS device. Adopting a single repeat interval for national security alerts would eliminate the need to relay the repeat interval but a single interval would not be appropriate to all emergencies and would take control of the repetition (and the ability to manage emergency responses) away from the alert originator.

55. Timing issues likely also would arise, particularly with respect to the legacy version of the repeated alert (i.e., the repeat alert that is encoded by designated EAS Participants for the benefit of downstream monitoring stations). Assuming the national security alert was processed like NWS and other alerts categorized as state and local alerts, it would have no priority in terms of processing – the transmission of any alert in-progress (or in the transmit queue) when the national security alert was received would have to complete transmission before the national security alert could be transmitted. Any new alerts received while the alert is repeated would also be delayed (for example, a radiologic hazard warning or civil danger warning alert with evacuation information due to a terrorist attack could be delayed due to a repeat of the initial national security alert warning of the imminent attack). In addition, disparities among EAS device repeat times would cause systemic problems. EAS Participants that only decode alerts would repeat the original alert but EAS Participants that encode alerts would change the time stamp and valid time period data for the repeated version of the alert – that new version of the alert would be received by the EAS Participants that only decode and would be treated as a new alert (that itself would have to be repeated) directly after they completed repeating the original version of that alert. Requiring EAS devices to simply repeat the original alert, including the original header codes, with or without encoding, or just the attention signal and audio message, with no encoding, would require significant changes to EAS device programming and possibly modifications to enable storing (as opposed to buffering) the original alert for subsequent repetition. Downstream equipment at the EAS Participant's facilities devices could be implicated as well.

56. We seek comment on the feasibility of repeating national security alerts automatically (or manually) by EAS Participants' EAS devices. Would re-origination of the national security alert require that every EAS Participant be authorized by the Commission in consultation with FEMA, and if so, what would be the point of adopting a new origination code for FEMA and entities authorized by the Commission in consultation with FEMA? Is it technically feasible for any entity other than the alert originator to repeat a national security alert within the EAS system? What changes to the EAS rules would be required to facilitate such repetition? Would such rule changes require changes to EAS devices, downstream processing equipment, and/or NWS/NWR systems and the various consumer and enterprise radios that receive NWR transmissions? Could such equipment changes be affected via software updates or would firmware and/or hardware changes also be required? How long would such changes take to implement and at what costs to EAS Participants and/or other entities? Would equipment standards for downstream equipment need to be revised to accommodate such repetition in EAS devices? If so, how

long would that take? What benefits would be derived from requiring EAS devices to repeat national security alerts? Would those benefits outweigh the costs in enabling such repetition? Could the EAS Protocol be revised to enable sending repeat interval information and national security alert cancellation data via the legacy EAS? What impact would such action have on EAS devices, downstream processing equipment, NWS/NWR systems and the various consumer and enterprise radios that receive NWR transmissions? To the extent any such equipment would need to be modified, what would the costs of such modification be and who would bear them? Would the benefits of such action outweigh the costs involved? Is there a single repeat interval for national security alerts that would function well for any emergency condition that might cause the alert to be issued in the first place?

IV. NOTICE OF INQUIRY

A. Feasibility of EAS Participation for Internet-related services

57. Section 9201(e) of the NDAA21 requires that we, "[n]ot later than 180 days after the date of enactment of [the] Act, and after providing public notice and opportunity for comment…complete an inquiry to examine the feasibility of updating the Emergency Alert System to enable or improve alerts to consumers provided through the internet, including through streaming services." Accordingly, in this Notice of Inquiry, we seek comment on the definition of "streaming services" and whether it would be technically feasible for streaming services to complete each step that EAS Participants complete under the Commission's rules in ensuring the end-to-end transmission of EAS alerts, including monitoring for relevant EAS alerts, receiving and processing EAS alerts, retransmitting EAS alerts, presenting EAS alerts in an accessible manner to relevant consumers, and testing.

58. *Definition of "streaming."* Neither the Commission nor the NDAA21 has defined "streaming" services. Accordingly, we seek comment on how to define this term. The 3rd Generation Partnership Project (3GPP) defines the term as "the ability of an application to play synchronised media streams like audio and video streams in a continuous way while those streams are being transmitted to the client over a data network."[122] Is there a more authoritative definition that we should consider? Would it be consistent with the best available definitions of "streaming" to consider streaming video, audio, and applications within the scope of this inquiry? We seek comment on whether any streaming services already support emergency alerts, including EAS alerts.

59. *Monitoring for EAS Alerts*. Streaming services' large geographic service areas may present a monitoring challenge. How can streaming services monitor for EAS alerts that pertain to any location where they offer service, but only present EAS alerts to the consumers for whom the alert is relevant? Would it be technically feasible and appropriate for streaming services to differentiate between market areas they serve when determining what kinds of EAS alerts to support? Would a similar issue present with respect to the types of events about which streaming services alert consumers? We observe that SECCs and LECCs, as well as state, local, Tribal, or territorial government officials are well-positioned to advise EAS Participants on the types of EAS alerts they should monitor for and present to consumers.[123] Are these officials equally well-positioned to advise streaming services on the types of EAS alerts they should monitor for and present to consumers in different geographic areas?

60. We seek comment on whether it is technically feasible for streaming services to monitor for EAS alerts formatted in the Common Alerting Protocol or the EAS Protocol. Do streaming services operate equipment that can poll Internet feeds? Do streaming services operate equipment that can tune to broadcast channels? Can streaming services monitor for EAS alerts initiated in the EAS Protocol at the federal, state, local, Tribal, or territorial level?

---

[122] 3GPP, Transparent end-to-end Packet-switched Streaming Service (PSS); Protocols and codecs, TS 26.234 (2020), https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=1436.

[123] *See* 47 CFR § 11.21.

61. *Receiving and Processing EAS Alerts.* Streaming services would not be able to present EAS alerts to the public unless they are able to receive EAS alerts and process them into a format suitable for transmission to end-user devices. We seek comment on whether it would be technically feasible for streaming services to use traditional EAS equipment for this purpose. What, if any, changes to EAS equipment or applicable standards would be necessary to enable streaming services to use EAS equipment to receive and process EAS alerts? In the alternative, we seek comment on whether virtualized (*i.e.*, software-only) versions of EAS equipment would fit better within streaming services' service architectures.

62. Streaming services would also need to be able to authenticate and validate EAS alerts to ensure that their participation in EAS does not compromise the EAS system, such as by accepting spoofed alerts.[124] We seek comment on the technical tools available to streaming services to protect the confidentiality, integrity, and availability of data at rest and in transit. Is it technically feasible for streaming services to apply those tools to EAS alerts? Do streaming services operate equipment capable of validating XML or Audio Frequency Shift Keyed content? Could streaming services use the Common Alerting Protocol digital signature to authenticate and protect the integrity of EAS alerts?

63. *Retransmitting EAS Alerts.* EAS Participants that retransmit EAS alerts in the EAS Protocol do so using over-the-air broadcast. Some streaming services, however, might not own or operate over-the-air broadcast technology as part of their core businesses. We seek comment on whether streaming services operate equipment that is capable of retransmitting EAS alerts in the EAS Protocol. We seek comment on how, if at all, allowing streaming services to participate in EAS without retransmitting EAS alerts in the EAS Protocol might affect the reliability, resiliency, and redundancy of EAS. If streaming services cannot rebroadcast EAS Protocol-formatted EAS alerts, would it be technically feasible for streaming services to retransmit EAS alerts formatted in the Common Alerting Protocol?

64. Sometimes, like existing EAS Participants, streaming services deliver content to consumer premises equipment that does not contain a graphical user interface, such as set-top boxes. How do wireline video, cable, and broadcast television EAS Participants ensure that the set-top boxes to which they deliver service retransmit EAS alerts to televisions in an accessible manner? Could streaming services adopt a similar approach?

65. *Presenting EAS Alerts on End-User Devices.* EAS Participants that transmit EAS alerts to end-user devices capable of displaying a visual message, such as set-top boxes and televisions, must display that message accessibly.[125] We seek comment on whether it is technically feasible for streaming audio services to present the EAS attention signal and the audio portion of the EAS message in full at least once during any EAS message. We seek comment on whether streaming audio providers would be able to display the visual EAS message in the accessible manner described above notwithstanding the fact that they provide an audio service, as we note that many audio services also provide graphical user interfaces that could support pop-ups and the display of text. We seek comment on whether streaming video services would be able to present the EAS attention signal along with the EAS audio message and

[124] *See* 47 CFR § 11.56(c) (requiring EAS Participants to reject all alerts that do not have a valid Common Alerting Protocol digital signature); 47 CFR § 11.33(a)(10) ("An EAS Decoder must provide error detection and validation of the header codes of each message to ascertain if the message is valid.").

[125] 47 CFR § 11.51 (requiring that these EAS Participants present alerts "(i) At the top of the television screen or where it will not interfere with other visual messages; (ii) In a manner (*i.e.,* font size, color, contrast, location, and speed) that is readily readable and understandable; (iii) That does not contain overlapping lines of EAS text or extend beyond the viewable display (except for video crawls that intentionally scroll on and off of the screen), and (iv) In full at least once during any EAS message" and that "[t]he audio portion of an EAS message must play in full at least once during any EAS message" and the EAS attention signal must precede any audio message"). The audio, but not the visual EAS alert message presentation requirements apply to EAS Participants that transmit EAS alerts to end-user devices that are not capable of displaying a visual message, such as analog radio stations.

visual message in the accessible manner described above. We seek comment on the end-user devices on which streaming services present content and services that currently or could be upgraded to support the presentation of EAS alerts formatted in the Common Alerting Protocol or a format derived therefrom.

66. We seek comment on whether consumer choice at the end-user device could help to address the enterprise-level challenges of determining which EAS alerts are relevant, as raised above. Could part of the user setup of an end-user device include opting in or out of receiving emergency alerts intended for specific geographic regions relevant to the user? Could Internet-connected end-user devices empower individuals to choose the kinds of events about which they want to receive alerts (*e.g.*, child abductions or imminent threats) and, in so doing, help to prevent alert fatigue? Alternatively, would it be technically feasible for streaming services to use the Internet Protocol addresses of end-user equipment as the basis for geographically targeting EAS alerts, while respecting consumer privacy?

67. Consistent with the language in Section 9201(e), we seek comment on which additional Internet-based services, if any, we should examine as part of our inquiry. Commenters offering suggestions should discuss relevant definitions and whether it is technically feasible for the service to complete each step that EAS Participants complete under the Commission's rules.

B. Feasibility of Internet-Related Updates for EAS Participants

68. In addition to directing the Commission to examine the feasibility of updating the EAS to enable alerts to consumers provided through the Internet, Section 9201(e) of the NDAA21 also requires the Commission to examine the feasibility of improving alerts to consumers that are already delivered over the Internet. Existing EAS Participants already receive Common Alerting Protocol-based alerts over the Internet by polling IPAWS.[126] While the Common Alerting Protocol is capable of supporting text, audio, video, data, multiple languages, links to Internet-based audio or video files, and a digital signature, EAS Participants' current approach to EAS distribution does not transfer those benefits to consumers.[127] Accordingly, we seek to establish whether it is feasible for EAS Participants to leverage the Internet to offer the full feature suite of the Common Alerting Protocol to the public.[128]

69. We seek comment on whether advancements in Internet-related technologies now make it feasible for EAS Participants to retransmit EAS alerts to the public in the Common Alerting Protocol. We seek comment on what mechanisms EAS equipment uses today to monitor for, receive, and process Common Alerting Protocol-based EAS alerts, including Ethernet, Wi-Fi, and intermediary devices.[129] Is it feasible for EAS equipment to use these same mechanisms to retransmit such alerts to end-user devices? What, if any updates to EAS equipment software, firmware, or hardware would be required to render them capable of retransmitting Common Alerting Protocol-formatted EAS alerts? What, if any, Internet-related functionalities have EAS equipment manufacturers already upgraded their equipment to include?

---

[126] *See* FEMA, Integrated Public Alert and Warning System, https://www.fema.gov/emergency-managers/practitioners/integrated-public-alert-warning-system (last visited Jan 11, 2021).

[127] *Compare* OASIS, Common Alerting Protocol Version 1.2 (2010), http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2-os.html (last visited Jan. 4, 2021) *with* 47 CFR § 11 *et seq.*

[128] Pub. L. 116-283, 134 Stat. 3388, § 9201(e).

[129] Intermediary devices are stand-alone devices that carry out the functions of monitoring for, receiving, and decoding Common Alerting Protocol-formatted messages and converting such messages into a format that can be inputted into a separate, stand-alone legacy EAS device to produce an output that complies with the Part 11 rules. There are two types of intermediary devices, "universal" intermediary devices, which interoperate with all EAS equipment but can only generate EAS alerts in the EAS Protocol, and "component" intermediary devices, which enhance the functionality of certain legacy EAS devices by processing additional Common Alerting Protocol alert content.

70. To what extent are the end-user devices to which current EAS Participants deliver EAS alerts (*e.g.*, radios and televisions) capable of receiving and presenting EAS alerts formatted in the Common Alerting Protocol or a format derived therefrom? What software, firmware, or hardware updates would be necessary to enable radios, televisions, and Internet-connected end-user devices to receive and present EAS alerts formatted in the Common Alerting Protocol or a format derived therefrom? What are the estimated costs of those updates? To the extent that legacy end-user devices would need to be replaced for EAS Participants to offer the benefits of the Common Alerting Protocol to the public, how quickly should we expect consumers to replace incompatible equipment with new, compatible equipment through normal market churn?

71. We seek comment on the public safety benefits that would accrue from EAS Participants' transmitting EAS alerts to the public in the Common Alerting Protocol. To what extent would it help Americans to protect their lives and property to receive EAS alerts that contain the embedded hyperlinks, multilingual alert translations, multimedia content, and alert authentication that the Common Alerting Protocol supports? We also seek comment on the public safety benefits of a greater variety of end-user devices receiving EAS alerts, such as laptop or desktop computers. How might these new devices improve upon how EAS Participants present EAS alerts to consumers, and thereby better motivate protective actions?

V. PROCEDURAL MATTERS

72. *Ex Parte Rules*.—This proceeding shall be treated as "permit-but-disclose" proceedings in accordance with the Commission's *ex parte* rules.[130] Persons making *ex parte* presentations must file a copy of any written presentation or a memorandum summarizing any oral presentation within two business days after the presentation (unless a different deadline applicable to the Sunshine period applies). Persons making oral ex parte presentations are reminded that memoranda summarizing the presentation must: (1) list all persons attending or otherwise participating in the meeting at which the *ex parte* presentation was made; and (2) summarize all data presented and arguments made during the presentation. If the presentation consisted in whole or in part of the presentation of data or arguments already reflected in the presenter's written comments, memoranda, or other filings in the proceeding, the presenter may provide citations to such data or arguments in his or her prior comments, memoranda, or other filings (specifying the relevant page and/or paragraph numbers where such data or arguments can be found) in lieu of summarizing them in the memorandum. Documents shown or given to Commission staff during *ex parte* meetings are deemed to be written *ex parte* presentations and must be filed consistent with rule 1.1206(b). In proceedings governed by rule 1.49(f) or for which the Commission has made available a method of electronic filing, written *ex parte* presentations and memoranda summarizing oral *ex parte* presentations, and all attachments thereto, must be filed through the electronic comment filing system available for that proceeding, and must be filed in their native format (e.g., .doc, .xml, .ppt, searchable .pdf). Participants in this proceeding should familiarize themselves with the Commission's *ex parte* rules.

73. *Comment Filing Procedures*. —Pursuant to sections 1.415 and 1.419 of the Commission's rules, 47 CFR §§ 1.415, 1.419, interested parties may file comments and reply comments on or before the dates indicated on the first page of this document. Comments may be filed using the Commission's Electronic Comment Filing System (ECFS). *See* Electronic Filing of Documents in Rulemaking Proceedings, 63 FR 24121 (1998).

[130] *See id*., §§ 1.1200—1.1216. Notices of Inquiry are exempt from *ex parte* rules. *See* 47 CFR § 1.1204(b)(1). The Commission and its staff have the authority, however, to modify the applicable *ex parte* rules by order, letter, or public notice. *See* 47 CFR § 1.1200. We modify the *ex parte* rules to make this Notice of Inquiry a permit-but-disclose proceeding to allow for greater transparency and better documentation of the conclusions made in the required report,

- Electronic Filers: Comments may be filed electronically using the Internet by accessing the ECFS: http://fjallfoss.fcc.gov/ecfs2/.
- Paper Filers: Parties that choose to file by paper must file an original and one copy of each filing. If more than one docket or rulemaking number appears in the caption of this proceeding, filers must submit two additional copies for each additional docket or rulemaking number.
- Filings can be sent by hand or messenger delivery, by commercial overnight courier, or by first-class or overnight U.S. Postal Service mail. All filings must be addressed to the Commission's Secretary, Office of the Secretary, Federal Communications Commission.
    - Commercial overnight mail (other than U.S. Postal Service Express Mail and Priority Mail) must be sent to 9050 Junction Drive, Annapolis Junction, MD 20701
    - Postal Service first-class, Express, and Priority mail must be addressed to 45 L Street, NE, Washington DC 20554
- Effective March 19, 2020, and until further notice, the Commission no longer accepts any hand or messenger delivered filings. This is a temporary measure taken to help protect the health and safety of individuals, and to mitigate the transmission of COVID-19.
- During the time the Commission's building is closed to the general public and until further notice, if more than one docket or rulemaking number appears in the caption of a proceeding, paper filers need not submit two additional copies for each additional docket or rulemaking number; an original and one copy are sufficient.

74. *People with Disabilities*: To request materials in accessible formats for people with disabilities (braille, large print, electronic files, audio format), send an e-mail to fcc504@fcc.gov or call the Consumer & Governmental Affairs Bureau at 202-418-0530.

75. *Regulatory Flexibility Act*. The Regulatory Flexibility Act of 1980, as amended (RFA),[131] requires that a regulatory flexibility analysis be prepared for notice and comment rulemaking proceedings, unless the agency certifies that "the rule will not, if promulgated, have a significant economic impact on a substantial number of small entities."[132] Accordingly, the Commission has prepared an Initial Regulatory Flexibility Analysis (IRFA) concerning potential rule and policy changes contained in this Notice of Proposed Rulemaking. The IRFA is set forth in Appendix B.

76. *Initial Paperwork Reduction Act Analysis*. This Notice of Proposed Rulemaking may contain potential new or revised information collection requirements. Therefore, we seek comment on potential new or revised information collections subject to the Paperwork Reduction Act of 1995.[133] If the Commission adopts any new or revised information collection requirements, the Commission will publish a notice in the Federal Register inviting the general public and the Office of Management and Budget to comment on the information collection requirements, as required by the Paperwork Reduction Act of 1995, Public Law 104-13. In addition, pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107-198, see 44 U.S.C. 3506(c)(4), we seek specific comment on how we might further reduce the information collection burden for small business concerns with fewer than 25 employees.

77. *Further Information*. For further information regarding the Notice of Proposed Rulemaking, contact Christopher Fedeli, Attorney Advisor, Public Safety and Homeland Security Bureau

[131] 5 U.S.C. § 603. The RFA, 5 U.S.C. §§ 601–612, was amended by the Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA), Pub. L. No. 104-121, Title II, 110 Stat. 857 (1996).

[132] *Id*. § 605(b).

[133] Public Law 104-13.

at 202-418-1514 or Christopher.Fedeli@fcc.gov. For further information regarding the Notice of Inquiry, contact James Wiley, Attorney-Advisor, Public Safety and Homeland Security Bureau, Cybersecurity and Communications Reliability Division at (202) 418-1678 or James.Wiley@fcc.gov.

VI. ORDERING CLAUSES

78. Accordingly, IT IS ORDERED, pursuant to the NDAA21, Pub. L. 116-283, 134 Stat. 3388, § 9201, that this Notice of Proposed Rulemaking and Notice of Inquiry in PS Docket Nos. 15-94 and 15-91 IS HEREBY ADOPTED.

79. IT IS FURTHER ORDERED that the Commission's Consumer and Governmental Affairs Bureau, Reference Information Center, SHALL SEND a copy of this Notice of Proposed Rulemaking, including the Initial Regulatory Flexibility Analysis, to the Chief Counsel for Advocacy of the Small Business Administration.

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

Appendix A

Proposed Rules

Part 10 – WIRELESS EMERGENCY ALERTS

Authority: [TO BE INSERTED PRIOR TO PUBLICATION OF FEDERAL REGISTER SUMMARY]

Section 10.11 is revised by adding paragraph (b) to read as follows:

§ 10.11 WEA implementation timeline.

(a) * * *

(b) If a Participating CMS Provider's network infrastructure would generate and display WEA headers with the text "Presidential Alert" to subscribers upon receipt of a National Alert, or include the text "Presidential Alert" in a mobile device's settings menus, then by July 31, 2022, that Participating CMS Provider's network infrastructure shall either generate and display WEA headers and menus with the text "National Alert," or no longer display those headers and menu text to the subscriber. Network infrastructure that is technically incapable of meeting this requirement, such as situations in which legacy devices or networks cannot be updated to support header display changes, are exempt from this requirement.

Section 10.320 is revised by amending paragraph (e)(3) to read as follows:

§ 10.320 Provider Alert Gateway Requirements.

* * * * *

(e) * * *

(3) Prioritization. The CMS provider gateway must process an Alert Message on a first in-first out basis except for National Alerts, which must be processed before all non-National Alerts.

* * * * *

Section 10.400 is revised by amending paragraph (a) as follows:

§ 10.400 Classification.

* * * * *

(a) National Alert. A National Alert is an alert issued by the President of the United States or the President's authorized designee, or by the Administrator of FEMA.

* * * * *

Section 10.410 is revised as follows:

§ 10.410 Prioritization.

A Participating CMS Provider is required to transmit National Alerts upon receipt. National Alerts preempt all other Alert Messages. A Participating CMS Provider is required to transmit Imminent Threat Alerts, AMBER Alerts and Public Safety Messages on a first in-first out (FIFO) basis.

Section 10.420 is revised as follows:

§ 10.420 Message Elements.

A WEA Alert Message processed by a Participating CMS Provider shall include five mandatory CAP elements — Event Type; Area Affected; Recommended Action; Expiration Time (with time zone); and Sending Agency. This requirement does not apply to National Alerts.

Section 10.500 is revised by amending paragraph (f) as follows:

§ 10.500 General Requirements.

* * * * *

(f) Presentation of alert content to the device, consistent with subscriber opt-out selections. National Alerts must always be presented.

* * * * *

Section 10.520 is revised by adding subsection (d)(2) to read as follows:

§ 10.520 Common Audio Attention Signal.

* * * * *

(d)(1) * * *

(d)(2) If the Administrator of the Federal Emergency Management Agency (FEMA) or a State, local, Tribal, or territorial government entity becomes aware of transmission of a WEA false alert to the public, they are encouraged to send an email to the Commission at the FCC Ops Center at FCCOPS@fcc.gov, informing the Commission of the event and of any details that they may have concerning the event.

* * * * *

Part 11 – EMERGENCY ALERT SYSTEM (EAS)

Authority: [TO BE INSERTED PRIOR TO PUBLICATION OF FEDERAL REGISTER SUMMARY]

Section 11.21 is revised by amending the introductory paragraph, and paragraph (a), and adding paragraph (a)(8) as follows:

§ 11.21 State and Local Area plans and FCC Mapbook.

EAS plans contain guidelines which must be followed by EAS Participants' personnel, emergency officials, and National Weather Service (NWS) personnel to activate the EAS. The plans include the EAS header codes and messages that will be transmitted by key EAS sources (NP, LP, SP and SR). State and local plans contain unique methods of EAS message distribution such as the use of the Radio Broadcast Data System (RBDS). The plans also include information on actions taken by EAS Participants, in coordination with state and local governments, to ensure timely access to EAS alert content by non-English speaking populations. The plans must be reviewed and approved by the Chief, Public Safety and Homeland Security Bureau (Bureau), prior to implementation to ensure that they are consistent with

national plans, FCC regulations, and EAS operation. The plans are administered by State Emergency Communications Committees (SECC). The Commission encourages the chief executive of each State to establish an SECC if their State does not have an SECC, and if the State has an SECC, to review the composition and governance of the SECC. The Bureau will review and approve plans, including annual updated plans, within 60 days of receipt, provided that no defects are found requiring the plan to be returned to the SECC for correction and resubmission. If a plan submitted for approval is found defective, the SECC will be notified of the required corrections, and the corrected plan may be resubmitted for approval, thus starting the 60-day review and approval period anew. The approval dates of State EAS Plans will be listed on the Commission's website.

(a) State EAS Plans contain guidelines that must be followed by EAS Participants' personnel, emergency officials, and National Weather Service (NWS) personnel to activate the EAS. The Plans include information on actions taken by EAS Participants, in coordination with state and local governments, to ensure timely access to EAS alert content by non-English speaking populations. State EAS Plans must be updated on an annual basis. State EAS Plans must include the following elements:

* * *

(8) Certification by the SECC Chairperson or Vice-Chairperson that the SECC met (in person, via teleconference, or via other methods of conducting virtual meetings) at least once in the twelve months prior to submitting the annual updated plan to review and update the plan.

* * * * *

Section 11.33 is revised by amending paragraph (a)(10) as follows:

§ 11.33 EAS Decoder.

(a) * * *

(10) *Message Validity*. An EAS Decoder must provide error detection and validation of the header codes of each message to ascertain if the message is valid. Header code comparisons may be accomplished through the use of a bit-by-bit compare or any other error detection and validation protocol. A header code must only be considered valid when two of the three headers match exactly; the Origination Date/Time field (JJJHHMM) is not more than 15 minutes in the future and the expiration time (Origination Date/Time plus Valid Time TTTT) is in the future (i.e., current time at the EAS equipment when the alert is received is between origination time minus 15 minutes and expiration time). Duplicate messages must not be relayed automatically. An alert repeated by the alert originator that was released at least one minute subsequent to the time the message was initially released by the originator, as reflected in the repeat alert's JJJHHMM header code, shall not be treated as a duplicate.

Section 11.45 is revised by amending paragraph (b) and adding paragraph (c) to read as follows:

§ 11.45 Prohibition of false or deceptive EAS transmissions.

* * * * *

(b) No later than twenty-four (24) hours of an EAS Participant's discovery (i.e., actual knowledge) that it has transmitted or otherwise sent a false alert to the public, the EAS Participant shall send an email to the Commission at the FCC Ops Center at FCCOPS@fcc.gov, informing the Commission of the event and of any details that the EAS Participant may have concerning the event.

(c) If the Administrator of the Federal Emergency Management Agency or a State, local, Tribal, or territorial government entity becomes aware of transmission of an EAS false alert to the public, they

are encouraged to send an email to the Commission at the FCC Ops Center at FCCOPS@fcc.gov, informing the Commission of the event and of any details that they may have concerning the event.

APPENDIX B

Initial Regulatory Flexibility Analysis

1. As required by the Regulatory Flexibility Act of 1980, as amended (RFA),[1] the Commission has prepared this Initial Regulatory Flexibility Analysis (IRFA) of the possible significant economic impact on a substantial number of small entities by the policies and rules proposed in the Notice of Proposed Rulemaking (*Notice*). Written public comments are requested on this IRFA. Comments must be identified as responses to the IRFA and must be filed by the deadlines for comments on the *Notice*. The Commission will send a copy of the *Notice*, including this IRFA, to the Chief Counsel for Advocacy of the Small Business Administration (SBA).[2] In addition, the *Notice* and IRFA (or summaries thereof) will be published in the Federal Register.[3]

A. Need for, and Objectives of, the Proposed Rules

2. In the *Notice*, the Commission proposes amending the rules governing Wireless Emergency Alerts (WEA) and the Emergency Alert System (EAS) in response to the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021.[4] Specifically, the Commission seeks comment on proposed rules that would (i) replace WEA's existing Presidential Alert class with a National Alert class that would ensure that WEA-enabled mobile devices could not opt-out of receiving WEA alerts issued by the President (or the President's authorized designee) or by the Administrator of the Federal Emergency Management Agency (FEMA); (ii) require participating CMS providers that use WEA header displays that read "Presidential Alert" to change those alert headers to read "National Alert;" (iii) encourage chief executives of states to form State Emergency Communications Committees (SECC) if none exist in their states, or if they do, to review their composition and governance; (iv) incorporate certain processing actions concerning SECCs' and the FCC's administration of State EAS Plans; (v) enable false EAS and WEA alert reporting by the Administrator of FEMA as well as State, local, Tribal, and territorial governments; and (vi) provide for repeating EAS alerts issued by the President, the Administrator of FEMA and any other entity determined appropriate under the circumstances by the Commission, in consultation with the Administrator of FEMA. To the extent these proposed and contemplated actions may result in greater participation by state, local, Tribal, and territorial governments in the administration of State EAS Plans, enhanced administration of EAS alerting, hasten corrective action of any false alerts issued, and better enable alert originators to repeat alerts, they would benefit the public by strengthening national, state, local, Tribal, and territorial alerting activities, minimizing confusion and disruption caused by false alerts, and increase the chances for the public to receive critical alert messages.

B. Legal Basis

3. The proposed action is authorized pursuant to the National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283, 134 Stat. 3388 (2021), Pub. L. 116-283, 134 Stat. 3388, § 9201.

[1] *See* 5 U.S.C. § 603. The RFA, *see* 5 U.S.C. §§ 601-612, has been amended by the Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA), Pub. L. No. 104-121, Title II, 110 Stat. 857 (1996).

[2] *See* 5 U.S.C. § 603(a).

[3] *See id.*

[4] National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283, 134 Stat. 3388 (2021) (NDAA21).

C. Description and Estimate of the Number of Small Entities to Which the Proposed Rules Will Apply

4. The RFA directs agencies to provide a description of and, where feasible, an estimate of, the number of small entities that may be affected by the proposed rules, if adopted.[5] The RFA generally defines the term "small entity" as having the same meaning as the terms "small business," "small organization," and "small governmental jurisdiction."[6] In addition, the term "small business" has the same meaning as the term "small business concern" under the Small Business Act.[7] A "small business concern" is one which: (1) is independently owned and operated; (2) is not dominant in its field of operation; and (3) satisfies any additional criteria established by the SBA.[8]

5. *Small Businesses, Small Organizations, and Small Governmental Jurisdictions*. Our action may, over time, affect small entities that are not easily categorized at present. We therefore describe here, at the outset, three broad groups of small entities that could be directly affected herein.[9] First, while there are industry specific size standards for small businesses that are used in the regulatory flexibility analysis, according to data from the SBA's Office of Advocacy, in general a small business is an independent business having fewer than 500 employees.[10] These types of small businesses represent 99.9% of all businesses in the United States which translates to 30.7 million businesses.[11]

6. Next, the type of small entity described as a "small organization" is generally "any not-for-profit enterprise which is independently owned and operated and is not dominant in its field."[12] Internal Revenue Service (IRS) uses a revenue benchmark of $50,000 or less to delineate its annual electronic filing requirements for small exempt organizations.[13] Nationwide, for tax year 2018, there were approximately 571,709 small exempt organizations in the U.S. reporting revenues of $50,000 or less according to the registration and tax data for exempt organizations available from the IRS.[14]

---

[5] 5 U.S.C. § 603(b)(3).

[6] 5 U.S.C. § 601(6).

[7] 5 U.S.C. § 601(3) (incorporating by reference the definition of "small-business concern" in the Small Business Act, 15 U.S.C. § 632). Pursuant to 5 U.S.C. § 601(3), the statutory definition of a small business applies "unless an agency, after consultation with the Office of Advocacy of the Small Business Administration and after opportunity for public comment, establishes one or more definitions of such term which are appropriate to the activities of the agency and publishes such definition(s) in the Federal Register."

[8] 15 U.S.C. § 632.

[9] *See* 5 U.S.C. § 601(3)-(6).

[10] *See* SBA, Office of Advocacy, "What's New With Small Business," https://cdn.advocacy.sba.gov/wp-content/uploads/2019/09/23172859/Whats-New-With-Small-Business-2019.pdf (Sept. 2019).

[11] *Id*.

[12] 5 U.S.C. § 601(4).

[13] The IRS benchmark is similar to the population of less than 50,000 benchmark in 5 U.S.C § 601(5) that is used to define a small governmental jurisdiction. Therefore, the IRS benchmark has been used to estimate the number small organizations in this small entity description. See Annual Electronic Filing Requirement for Small Exempt Organizations — Form 990-N (e-Postcard), "Who must file," https://www.irs.gov/charities-non-profits/annual-electronic-filing-requirement-for-small-exempt-organizations-form-990-n-e-postcard. We note that the IRS data does not provide information on whether a small exempt organization is independently owned and operated or dominant in its field.

[14] See Exempt Organizations Business Master File Extract (EO BMF), "CSV Files by Region," https://www.irs.gov/charities-non-profits/exempt-organizations-business-master-file-extract-eo-bmf. The IRS Exempt Organization Business Master File (EO BMF) Extract provides information on all registered tax-exempt/non-profit organizations. The data utilized for purposes of this description was extracted from the IRS EO

(continued….)

7. Finally, the small entity described as a "small governmental jurisdiction" is defined generally as "governments of cities, counties, towns, townships, villages, school districts, or special districts, with a population of less than fifty thousand."[15] U.S. Census Bureau data from the 2017 Census of Governments indicate that there were 90,056 local governmental jurisdictions consisting of general purpose governments and special purpose governments in the United States.[16] Of this number there were 36,931 General purpose governments (county[17], municipal and town or township[18]) with populations of less than 50,000 and 12,040 special purpose governments – independent school districts[19] with enrollment of less than 50,000.[20] Accordingly, based on the 2017 U.S. Census of Governments data, we estimate that at least 48,971 entities fall into the category of "small governmental jurisdictions."[21]

8. *Radio Stations*. This Economic Census category comprises establishments primarily engaged in broadcasting aural programs by radio to the public. Programming may originate in their own studio, from an affiliated network, or from external sources."[22] The SBA has established a small business size standard for this category as firms having $41.5 million or less in annual receipts.[23] Economic Census data for 2012 show that 2,849 radio station firms operated during that year.[24] Of that number,

---

BMF data for Region 1-Northeast Area (76,886), Region 2-Mid-Atlantic and Great Lakes Areas (221,121), and Region 3-Gulf Coast and Pacific Coast Areas (273,702) which includes the continental U.S., Alaska, and Hawaii. This data does not include information for Puerto Rico.

[15] 5 U.S.C. § 601(5).

[16] *See* U.S. Census Bureau, 2017 Census of Governments—Organization, Table 2. Local Governments by Type and State: 2017 [CG1700ORG02], https://www.census.gov/data/tables/2017/econ/gus/2017-governments.html. Local governmental jurisdictions are made up of general purpose governments (county, municipal and town or township) and special purpose governments (special districts and independent school districts). See also Table 2. CG1700ORG02 Table Notes_Local Governments by Type and State_2017.

[17] *See id* at Table 5, County Governments by Population-Size Group and State: 2017 [CG1700ORG05], https://www.census.gov/data/tables/2017/econ/gus/2017-governments.html. There were 2,105 county governments with populations less than 50,000. This category does not include subcounty (municipal and township)

[18] *See id* at Table 6, Subcounty General-Purpose Governments by Population-Size Group and State: 2017 [CG1700ORG06], https://www.census.gov/data/tables/2017/econ/gus/2017-governments.html. There were 18,729 municipal and 16,097 town and township governments with populations less than 50,000.

[19] *See id* at Table 10, Elementary and Secondary School Systems by Enrollment-Size Group and State: 2017 [CG1700ORG10], https://www.census.gov/data/tables/2017/econ/gus/2017-governments.html. There were 12,040 independent school districts with enrollment populations less than 50,000. See also Table 4. Special-Purpose Local Governments by State Census Years 1942 to 2017 [CG1700ORG04], CG1700ORG04 Table Notes Special Purpose Local Governments by State_Census Years 1942 to 2017.

[20] While the special purpose governments category also includes local special district governments, the 2017 Census of Governments data does not provide data aggregated based on population size for the special purpose governments category. Therefore, only data from independent school districts is included in the special purpose governments category.

[21] This total is derived from the sum of the number of general purpose governments (county, municipal and town or township) with populations of less than 50,000 (36,931) and the number of special purpose governments - independent school districts with enrollment populations of less than 50,000 (12,040), from the 2017 Census of Governments - Organizations Tables 5, 6, and 10.

[22] *See* U.S. Census Bureau, *2017 NAICS Definition, "515112 Radio Stations,"* https://www.census.gov/cgi-bin/sssd/naics/naicsrch?input=515112&search=2017+NAICS+Search&search=2017.

[23] *See* 13 CFR § 121.201, NAICS code 515112.

[24] *See* U.S. Census Bureau, *2012 Economic Census of the United States*, Table ID: EC1251SSSZ4, *Information: Subject Series—Estab and Firm Size: Receipts Size of Firms for the U.S.: 2012,* NAICS Code 515112,

(continued….)

2,806 firms operated with annual receipts of less than $25 million per year, 17 with annual receipts between $25 million and $49,999,999 million and 26 with annual receipts of $50 million or more.[25] Therefore, based on the SBA's size standard the majority of such entities are small entities.

9. In addition to the U.S. Census Bureau's data, based on Commission data we estimate that there are 4,560 licensed AM radio stations, 6,704 commercial FM radio stations and 8,339 FM translator and booster stations.[26] The Commission has also determined that there are 4,196 noncommercial educational (NCE) FM radio stations.[27] The Commission however does not compile and does not otherwise have access to information on the revenue of NCE stations that would permit it to determine how many such stations would qualify as small entities under the SBA size standard.

10. We also note, that in assessing whether a business entity qualifies as small under the above definition, business control affiliations must be included.[28] The Commission's estimate therefore likely overstates the number of small entities that might be affected by its action, because the revenue figure on which it is based does not include or aggregate revenues from affiliated companies. In addition, to be determined a "small business," an entity may not be dominant in its field of operation.[29] We further note, that it is difficult at times to assess these criteria in the context of media entities, and the estimate of small businesses to which these rules may apply does not exclude any radio station from the definition of a small business on these bases, thus our estimate of small businesses may therefore be over-inclusive. Also, as noted above, an additional element of the definition of "small business" is that the entity must be independently owned and operated. The Commission notes that it is difficult at times to assess these criteria in the context of media entities and the estimates of small businesses to which they apply may be over-inclusive to this extent.

11. *FM Translator Stations and Low-Power FM Stations.* FM translators and Low Power FM Stations are classified in the category of Radio Stations and are assigned the same NAICS Code as licensees of radio stations.[30] This U.S. industry, Radio Stations, comprises establishments primarily engaged in broadcasting aural programs by radio to the public.[31] Programming may originate in their own studio, from an affiliated network, or from external sources.[32] The SBA has established a small business size standard which consists of all radio stations whose annual receipts are $38.5 million dollars or less.[33] U.S. Census Bureau data for 2012 indicate that 2,849 radio station firms operated during that year.[34] Of

https://data.census.gov/cedsci/table?text=EC1251SSSZ4&n=515112&tid=ECNSIZE2012.EC1251SSSZ4&hidePreview=false.

[25] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[26] *See* Broadcast Station Totals as of September 30, 2020, FCC News Release (rel. Oct. 2, 2020) (Sept. 30, 2020 Broadcast Station Totals), https://docs.fcc.gov/public/attachments/DOC-367270A1.pdf.

[27] *See id*.

[28] "[Business concerns] are affiliates of each other when one concern controls or has the power to control the other, or a third party or parties controls or has power to control both." 13 CFR § 121.103(a)(1).

[29] 13 CFR § 121.102(b).

[30] *See* U.S. Census Bureau, *2017 NAICS Definition, "515112 Radio Stations,"* https://www.census.gov/cgi-bin/sssd/naics/naicsrch?input=515112&search=2017+NAICS+Search&search=2017.

[31] *Id.*

[32] *Id.*

[33] *See* 13 CFR § 121.201, NAICS Code 515112.

[34] *See* U.S. Census Bureau, *2012 Economic Census of the United States*, Table ID: EC1251SSSZ4, *Information: Subject Series—Estab and Firm Size: Receipts Size of Firms for the U.S.:2012,* NAICS Code 515112,

(continued….)

that number, 2,806 operated with annual receipts of less than $25 million per year, 17 with annual receipts between $25 million and $49,999,999 million and 26 with annual receipts of $50 million or more.[35] Therefore, based on the SBA's size standard we conclude that the majority of FM Translator Stations and Low Power FM Stations are small.

12. We note again, however, that in assessing whether a business concern qualifies as "small" under the above definition, business (control) affiliations must be included.[36] Because we do not include or aggregate revenues from affiliated companies in determining whether an entity meets the applicable revenue threshold, our estimate of the number of small radio broadcast stations affected is likely overstated. In addition, as noted above, one element of the definition of "small business" is that an entity would not be dominant in its field of operation. We are unable at this time to define or quantify the criteria that would establish whether a specific radio broadcast station is dominant in its field of operation. Accordingly, our estimate of small radio stations potentially affected by the rule revisions discussed in the NPRM includes those that could be dominant in their field of operation. For this reason, such estimate likely is over-inclusive.

13. *Television Broadcasting*. This Economic Census category "comprises establishments primarily engaged in broadcasting images together with sound."[37] These establishments operate television broadcast studios and facilities for the programming and transmission of programs to the public.[38] These establishments also produce or transmit visual programming to affiliated broadcast television stations, which in turn broadcast the programs to the public on a predetermined schedule. Programming may originate in their own studio, from an affiliated network, or from external sources. The SBA has created the following small business size standard for such businesses: those having $41.5 million or less in annual receipts.[39] The 2012 Economic Census reports that 751 firms in this category operated in that year.[40] Of that number, 656 had annual receipts of $25,000,000 or less, and 25 had annual receipts between $25,000,000 and $49,999,999.[41] Based on this data we therefore estimate that the majority of commercial television broadcasters are small entities under the applicable SBA size standard.

14. The Commission has estimated the number of licensed commercial television stations to be 1,368.[42] According to Commission staff review of the BIA Kelsey Inc. Media Access Pro Television Database (BIA) on November 16, 2017, 1,258 stations (or about 91 percent) had revenues of $38.5

---

https://data.census.gov/cedsci/table?text=EC1251SSSZ4&n=515112&tid=ECNSIZE2012.EC1251SSSZ4&hidePreview=false.

[35] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[36] "[Business concerns] are affiliates of each other when one concern controls or has the power to control the other, or a third party or parties controls or has power to control both." 13 CFR § 121.103(a)(1).

[37] *See* U.S. Census Bureau, 2017 NAICS Definitions, "*515120 Television Broadcasting,"* https://www.census.gov/cgi-bin/sssd/naics/naicsrch?input=515120&search=2017+NAICS+Search&search=2017.

[38] *Id.*

[39] *See* 13 CFR § 121.201, 2012 NAICS Code 515120.

[40] *See* U.S. Census Bureau, *2012 Economic Census of the United States*, Table ID: EC1251SSSZ4, *Information: Subject Series—Estab and Firm Size: Receipts Size of Firms for the U.S.: 2012,* NAICS Code 515120, https://data.census.gov/cedsci/table?text=EC1251SSSZ4&n=515120&tid=ECNSIZE2012.EC1251SSSZ4&hidePreview=false.

[41] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[42] *See Broadcast Station Totals* as of September 30, 2020, FCC News Release (rel. Oct. 2, 2020) (Sept. 30, 2020 Broadcast Station Totals), https://docs.fcc.gov/public/attachments/DOC-367270A1.pdf.

million or less, and therefore these licensees qualified as small entities under the SBA definition. In addition, the Commission has estimated the number of licensed noncommercial educational television stations to be 390.[43] Notwithstanding, the Commission does not compile and otherwise does not have access to information on the revenue of NCE stations that would permit it to determine how many such stations would qualify as small entities. There are also 2,246 low power television stations, including Class A stations (LPTV), and 3,543 TV translator stations.[44] Given the nature of these services, we will presume that all of these entities qualify as small entities under the above SBA small business size standard.

15. We note, however, that in assessing whether a business concern qualifies as "small" under the above definition, business (control) affiliations[45] must be included. Our estimate, therefore, likely overstates the number of small entities that might be affected by our action, because the revenue figure on which it is based does not include or aggregate revenues from affiliated companies. In addition, another element of the definition of "small business" requires that an entity not be dominant in its field of operation. We are unable at this time to define or quantify the criteria that would establish whether a specific television broadcast station is dominant in its field of operation. Accordingly, the estimate of small businesses to which rules may apply does not exclude any television station from the definition of a small business on this basis and is therefore possibly over-inclusive. Also, as noted above, an additional element of the definition of "small business" is that the entity must be independently owned and operated. The Commission notes that it is difficult at times to assess these criteria in the context of media entities and its estimates of small businesses to which they apply may be over-inclusive to this extent.

16. *Cable and Other Subscription Programming.* The U.S. Census Bureau defines this industry as establishments primarily engaged in operating studios and facilities for the broadcasting of programs on a subscription or fee basis. The broadcast programming is typically narrowcast in nature (e.g., limited format, such as news, sports, education, or youth-oriented). These establishments produce programming in their own facilities or acquire programming from external sources. The programming material is usually delivered to a third party, such as cable systems or direct-to-home satellite systems, for transmission to viewers.[46] The SBA size standard for this industry establishes as small, any company in this category which receives annual receipts of $41.5 million or less.[47] According to 2012 U.S. Census Bureau data, 367 firms operated for the entire year.[48] Of that number, 319 operated with annual receipts of less than $25 million a year and 48 firms operated with annual receipts of $25 million or more.[49] Based on this data, the Commission estimates that the majority of firms operating in this industry are small.

17. *Cable System Operators (Rate Regulation Standard).* The Commission has developed its own small business size standards for the purpose of cable rate regulation. Under the Commission's

---

[43] *Id.*

[44] *Id.*

[45] "[Business concerns] are affiliates of each other when one concern controls or has the power to control the other or a third party or parties controls or has the power to control both." 13 CFR § 21.103(a)(1).

[46] S*ee* U.S. Census Bureau, *2017 NAICS Definition, "515210 Cable and other Subscription Programming,"* https://www.census.gov/cgi-bin/sssd/naics/naicsrch?code=515210&search=2017%20NAICS%20Search.

[47] *See* 13 CFR 121.201, NAICS Code 515210.

[48] *See* U.S. Census Bureau, *2012 Economic Census of the United States*, Table ID: EC1251SSSZ4*, Information: Subject Series - Estab & Firm Size: Receipts Size of Firms for the U.S.: 2012*, NAICS Code 515210, https://data.census.gov/cedsci/table?text=EC1251SSSZ4&n=515210&tid=ECNSIZE2012.EC1251SSSZ4&hidePreview=false.

[49] *Id*. The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

rules, a "small cable company" is one serving 400,000 or fewer subscribers nationwide.[50] Industry data indicate that there are 4,600 active cable systems in the United States.[51] Of this total, all but five cable operators nationwide are small under the 400,000-subscriber size standard.[52] In addition, under the Commission's rate regulation rules, a "small system" is a cable system serving 15,000 or fewer subscribers.[53] Commission records show 4,600 cable systems nationwide.[54] Of this total, 3,900 cable systems have fewer than 15,000 subscribers, and 700 systems have 15,000 or more subscribers, based on the same records.[55] Thus, under this standard as well, we estimate that most cable systems are small entities.

18. *Cable System Operators (Telecom Act Standard)*. The Communications Act of 1934, as amended, also contains a size standard for small cable system operators, which is "a cable operator that, directly or through an affiliate, serves in the aggregate fewer than one percent of all subscribers in the United States and is not affiliated with any entity or entities whose gross annual revenues in the aggregate exceed $250,000,000."[56] As of 2019, there were approximately 48,646,056 basic cable video subscribers in the United States.[57] Accordingly, an operator serving fewer than 524,037 subscribers shall be deemed a small operator if its annual revenues, when combined with the total annual revenues of all its affiliates, do not exceed $250 million in the aggregate.[58] Based on available data, we find that all but nine incumbent cable operators are small entities under this size standard.[59] We note that the Commission neither requests nor collects information on whether cable system operators are affiliated with entities whose gross annual revenues exceed $250 million.[60] Although it seems certain that some of these cable system operators are affiliated with entities whose gross annual revenues exceed $250 million, we are unable at this time to estimate with greater precision the number of cable system operators that would qualify as small cable operators under the definition in the Communications Act.

---

[50] 47 CFR § 76.901(e). The Commission determined that this size standard equates approximately to a size standard of $100 million or less in annual revenues. *Implementation of Sections of the Cable Television Consumer Protection and Competition Act of 1992: Rate Regulation*, MM Docket No. 92-266, MM Docket No. 93-215, Sixth Report and Order and Eleventh Order on Reconsideration, 10 FCC Rcd 7393, 7408 (1995).

[51] The number of active, registered cable systems comes from the Commission's Cable Operations and Licensing System (COALS) database on August 15, 2015. *See* FCC, *Cable Operations and Licensing System (COALS)*, www.fcc.gov/coals (last visited Oct. 25, 2016).

[52] S&P Global Market Intelligence, *Top Cable MSOs as of 12/2019, https://platform.marketintelligence.spglobal.com/ (Dec 2019)*. The five cable operators all had more than 400,000 basic cable subscribers.

[53] 47 CFR § 76.901(c).

[54] *See supra* note 52.

[55] *Id*.

[56] 47 U.S.C. § 543(m)(2); *see also* 47 CFR § 76.901(e).

[57] S&P Global Market Intelligence, *U.S. Cable Subscriber Highlights, Basic Subscribers(actual) 2019*, *U.S. Cable MSO Industry Total, see also U.S. Multichannel Industry Benchmarks, U.S. Cable Industry Benchmarks, Basic Subscribers 2019Y, https://platform.marketintelligence.spglobal.com*.

[58] 47 CFR § 76.901(e).

[59] S&P Global Market Intelligence, *Top Cable MSOs as of 12/2019, https://platform.marketintelligence.spglobal.com*. The five cable operators all had more than 486,460 basic cable subscribers.

[60] The Commission does receive such information on a case-by-case basis if a cable operator appeals a local franchise authority's finding that the operator does not qualify as a small cable operator pursuant to § 76.901(e) of the Commission's rules. *See* 47 CFR § 76.910(b).

19. *Satellite Telecommunications.* This category comprises firms "primarily engaged in providing telecommunications services to other establishments in the telecommunications and broadcasting industries by forwarding and receiving communications signals via a system of satellites or reselling satellite telecommunications."[61] Satellite telecommunications service providers include satellite and earth station operators. The category has a small business size standard of $35 million or less in average annual receipts, under SBA rules.[62] For this category, U.S. Census Bureau data for 2012 show that there was a total of 333 firms that operated for the entire year.[63] Of this total, 299 firms had annual receipts of less than $25 million.[64] Consequently, we estimate that the majority of satellite telecommunications providers are small entities.

20. *All Other Telecommunications.* The **"**All Other Telecommunications" category is comprised of establishments that are primarily engaged in providing specialized telecommunications services, such as satellite tracking, communications telemetry, and radar station operation.[65] This industry also includes establishments primarily engaged in providing satellite terminal stations and associated facilities connected with one or more terrestrial systems and capable of transmitting telecommunications to, and receiving telecommunications from, satellite systems.[66] Establishments providing Internet services or voice over Internet protocol (VoIP) services via client-supplied telecommunications connections are also included in this industry.[67] The SBA has developed a small business size standard for "All Other Telecommunications," which consists of all such firms with gross annual receipts of $32.5 million or less.[68] For this category, U.S. Census data for 2012 show that there were 1,442 firms that operated for the entire year.[69] Of these firms, a total of 1,400 had gross annual receipts of less than $25 million.[70] Thus, the Commission estimates that the majority of "All Other Telecommunications" firms potentially affected by our action can be considered small.

21. *Broadband Radio Service and Educational Broadband Service.* Broadband Radio Service systems, previously referred to as Multipoint Distribution Service (MDS) and Multichannel Multipoint Distribution Service (MMDS) systems, and "wireless cable," transmit video programming to subscribers and provide two-way high speed data operations using the microwave frequencies of the

---

[61] *See* U.S. Census Bureau, *2017 NAICS Definition, "517410 Satellite Telecommunications,"* https://www.census.gov/cgi-bin/sssd/naics/naicsrch?input=517410&search=2017+NAICS+Search&search=2017.

[62] *See* 13 CFR § 121.201, NAICS Code 517410.

[63] *See* U.S. Census Bureau, *2012 Economic Census of the United States*, Table ID: EC1251SSSZ4, *Information: Subject Series - Estab and Firm Size: Receipts Size of Firms for the U.S.: 2012*, NAICS Code 517410, https://data.census.gov/cedsci/table?text=EC1251SSSZ4&n=517410&tid=ECNSIZE2012.EC1251SSSZ4&hidePreview=false&vintage=2012.

[64] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[65] *See* U.S. Census Bureau, *2017 NAICS Definition, "517919 All Other Telecommunications,"* https://www.census.gov/cgi-bin/sssd/naics/naicsrch?input=517919&search=2017+NAICS+Search&search=2017.

[66] *Id.*

[67] *Id.*

[68] *See* 13 CFR § 121.201, NAICS Code 517919.

[69] *See* U.S. Census Bureau, *2012 Economic Census of the United States*, Table ID: EC1251SSSZ4, *Information: Subject Series - Estab and Firm Size: Receipts Size of Firms for the U.S.: 2012*, NAICS Code 517919, https://data.census.gov/cedsci/table?text=EC1251SSSZ4&n=517919&tid=ECNSIZE2012.EC1251SSSZ4&hidePreview=false.

[70] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

Broadband Radio Service (BRS) and Educational Broadband Service (EBS) (previously referred to as the Instructional Television Fixed Service (ITFS)).[71]

22. *BRS* - In connection with the 1996 BRS auction, the Commission established a small business size standard as an entity that had annual average gross revenues of no more than $40 million in the previous three calendar years.[72] The BRS auctions resulted in 67 successful bidders obtaining licensing opportunities for 493 Basic Trading Areas (BTAs). Of the 67 auction winners, 61 met the definition of a small business. BRS also includes licensees of stations authorized prior to the auction. At this time, we estimate that of the 61 small business BRS auction winners, 48 remain small business licensees. In addition to the 48 small businesses that hold BTA authorizations, there are approximately 86 incumbent BRS licensees that are considered small entities (18 incumbent BRS licensees do not meet the small business size standard).[73] After adding the number of small business auction licensees to the number of incumbent licensees not already counted, there are currently approximately 133 BRS licensees that are defined as small businesses under either the SBA or the Commission's rules.

23. In 2009, the Commission conducted Auction 86, the sale of 78 licenses in the BRS areas.[74] The Commission offered three levels of bidding credits: (i) a bidder with attributed average annual gross revenues that exceed $15 million and do not exceed $40 million for the preceding three years (small business) received a 15 percent discount on its winning bid; (ii) a bidder with attributed average annual gross revenues that exceed $3 million and do not exceed $15 million for the preceding three years (very small business) received a 25 percent discount on its winning bid; and (iii) a bidder with attributed average annual gross revenues that do not exceed $3 million for the preceding three years (entrepreneur) received a 35 percent discount on its winning bid.[75] Auction 86 concluded in 2009 with the sale of 61 licenses.[76] Of the ten winning bidders, two bidders that claimed small business status won 4 licenses; one bidder that claimed very small business status won three licenses; and two bidders that claimed entrepreneur status won six licenses.

24. *EBS* - Educational Broadband Service has been included within the broad economic census category and SBA size standard for Wired Telecommunications Carriers since 2007. Wired Telecommunications Carriers are comprised of establishments primarily engaged in operating and/or providing access to transmission facilities and infrastructure that they own and/or lease for the transmission of voice, data, text, sound, and video using wired telecommunications networks. Transmission facilities may be based on a single technology or a combination of technologies."[77] The

---

[71] *Amendment of Parts 21 and 74 of the Commission's Rules with Regard to Filing Procedures in the Multipoint Distribution Service and in the Instructional Television Fixed Service and Implementation of Section 309(j) of the Communications Act—Competitive Bidding*, Report and Order, 10 FCC Rcd 9589, 9593, para. 7 (1995).

[72] 47 CFR § 21.961(b)(1).

[73] 47 U.S.C. § 309(j). Hundreds of stations were licensed to incumbent MDS licensees prior to implementation of Section 309(j) of the Communications Act of 1934, 47 U.S.C. § 309(j). For these pre-auction licenses, the applicable standard is SBA's small business size standard of 1500 or fewer employees.

[74] *Auction of Broadband Radio Service (BRS) Licenses*, *Scheduled for October 27*, *2009*, *Notice and Filing Requirements*, *Minimum Opening Bids*, *Upfront Payments*, *and Other Procedures for Auction 86*, Public Notice, 24 FCC Rcd 8277 (2009).

[75] *Id*. at 8296, para. 73.

[76] *Auction of Broadband Radio Service Licenses Closes*, *Winning Bidders Announced for Auction 86*, *Down Payments Due November 23*, *2009*, *Final Payments Due December 8*, *2009*, *Ten-Day Petition to Deny Period*, Public Notice, 24 FCC Rcd 13572 (2009).

[77] *See* U.S. Census Bureau, *2017 NAICS Definition*, "517311 Wired Telecommunications Carriers," http://www.census.gov/cgi-bin/sssd/naics/naicsrch?code=517311&search=2017.

SBA's small business size standard for this category is all such firms having 1,500 or fewer employees.[78] U.S. Census Bureau data for 2012 show that there were 3,117 firms that operated that year.[79] Of this total, 3,083 operated with fewer than 1,000 employees.[80] Thus, under this size standard, the majority of firms in this industry can be considered small. In addition to Census data, the Commission's Universal Licensing System indicates that as of October 2014, there are 2,206 active EBS licenses. The Commission estimates that of these 2,206 licenses, the majority are held by non-profit educational institutions and school districts, which are by statute defined as small businesses.[81]

25. *Direct Broadcast Satellite ("DBS") Service*. DBS service is a nationally distributed subscription service that delivers video and audio programming via satellite to a small parabolic "dish" antenna at the subscriber's location. DBS is included in the category of "Wired Telecommunications Carriers."[82] The Wired Telecommunications Carriers industry comprises establishments primarily engaged in operating and/or providing access to transmission facilities and infrastructure that they own and/or lease for the transmission of voice, data, text, sound, and video using wired telecommunications networks.[83] Transmission facilities may be based on a single technology or combination of technologies. Establishments in this industry use the wired telecommunications network facilities that they operate to provide a variety of services, such as wired telephony services, including VoIP services, wired (cable) audio and video programming distribution; and wired broadband Internet services.[84] By exception, establishments providing satellite television distribution services using facilities and infrastructure that they operate are included in this industry.[85] The SBA size standard considers a wireline business is small if it has fewer than 1,500 employees.[86] U.S. Census Bureau data for 2012 indicates that 3,117 wireline companies were operational during that year.[87] Of that number, 3,083 operated with fewer than 1,000 employees.[88] Based on that data, we conclude that the majority of wireline firms are small under the

[78] *See* 13 CFR § 121.201, NAICS Code 517311 (previously 517110).

[79] *See* U.S. Census Bureau, *2012 Economic Census of the United States,* Table ID: EC1251SSSZ5, *Information: Subject Series - Estab & Firm Size: Employment Size of Firms for the U.S.: 2012* NAICS Code 517110, https://data.census.gov/cedsci/table?text=EC1251SSSZ5&n=517110&tid=ECNSIZE2012.EC1251SSSZ5&hidePreview=false.

[80] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[81] The term "small entity" within SBREFA applies to small organizations (non-profits) and to small governmental jurisdictions (cities, counties, towns, townships, villages, school districts, and special districts with populations of less than 50,000). 5 U.S.C. §§ 601(4)-(6).

[82] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers"*, https://www.census.gov/cgi-bin/sssd/naics/naicsrch?code=517311&search=2017.

[83] *Id.*

[84] *See id*. Examples of this category are: broadband Internet service providers (*e.g.*, cable, DSL); local telephone carriers (wired); cable television distribution services; long-distance telephone carriers (wired); CCTV services; VoIP service providers, using own operated wired telecommunications infrastructure; DTH services; telecommunications carriers (wired); satellite television distribution systems; and MMDS.

[85] *Id*.

[86] *See* 13 CFR § 121.201, NAICS Code 517311 (previously 517110).

[87] *See* U.S. Census Bureau, *2012 Economic Census of the United States,* Table ID: EC1251SSSZ5, *Information: Subject Series - Estab & Firm Size: Employment Size of Firms: 2012,* NAICS Code 517110, https://data.census.gov/cedsci/table?text=EC1251SSSZ5&n=517110&tid=ECNSIZE2012.EC1251SSSZ5&hidePreview=false.

[88] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

applicable SBA standard. Currently, however, only two entities provide DBS service, which requires a great deal of capital for operation: DIRECTV (owned by AT&T) and DISH Network.[89] DIRECTV and DISH Network each report annual revenues that are in excess of the threshold for a small business. Accordingly, we must conclude that internally developed FCC data are persuasive that, in general, DBS service is provided only by large firms.

26. *Wireless Telecommunications Carriers (except Satellite)*. This industry comprises establishments engaged in operating and maintaining switching and transmission facilities to provide communications via the airwaves. Establishments in this industry have spectrum licenses and provide services using that spectrum, such as cellular services, paging services, wireless Internet access, and wireless video services.[90] The appropriate size standard under SBA rules is that such a business is small if it has 1,500 or fewer employees.[91] For this industry, U.S. Census Bureau data for 2012 show that there were 967 firms that operated for the entire year.[92] Of this total, 955 firms had employment of 999 or fewer employees, and 12 firms had employment of 1,000 employees or more.[93] Thus under this category and the associated size standard, the Commission estimates that the majority of wireless telecommunications carriers (except satellite) are small entities.

27. *AWS Services (1710–1755 MHz and 2110–2155 MHz bands (AWS-1); 1915–1920 MHz, 1995–2000 MHz, 2020–2025 MHz and 2175–2180 MHz bands (AWS-2); 2155–2175 MHz band (AWS-3))*. For the AWS-1 bands,[94] the Commission has defined a "small business" as an entity with average annual gross revenues for the preceding three years not exceeding $40 million, and a "very small business" as an entity with average annual gross revenues for the preceding three years not exceeding $15 million. For AWS-2 and AWS-3, although we do not know for certain which entities are likely to apply for these frequencies, we note that the AWS-1 bands are comparable to those used for cellular service and personal communications service. The Commission has not yet adopted size standards for the AWS-2 or AWS-3 bands but proposes to treat both AWS-2 and AWS-3 similarly to broadband PCS service and AWS-1 service due to the comparable capital requirements and other factors, such as issues involved in relocating incumbents and developing markets, technologies, and services.[95]

28. *Narrowband Personal Communications Services*. Two auctions of narrowband personal communications services (PCS) licenses have been conducted. To ensure meaningful participation of

---

[89] *See Annual Assessment of the Status of Competition in the Market for the Delivery of Video Programming, Eighteenth Report,* Table III.A.5*,* 32 FCC Rcd 568, 595 (Jan. 17, 2017).

[90] *See* U.S. Census Bureau, *2017 NAICS Definition*, "*517312 Wireless Telecommunications Carriers (except Satellite)*," https://www.census.gov/cgi-bin/sssd/naics/naicsrch?input=517312&search=2017+NAICS+Search&search=2017.

[91] *See* 13 CFR § 121.201, NAICS Code 517312 (previously 517210).

[92] *See* U.S. Census Bureau, *2012 Economic Census of the United States,* Table ID: EC1251SSSZ5*, Information: Subject Series: Estab and Firm Size: Employment Size of Firms for the U.S.: 2012*, NAICS Code 517210, https://data.census.gov/cedsci/table?text=EC1251SSSZ5&n=517210&tid=ECNSIZE2012.EC1251SSSZ5&hidePreview=false&vintage=2012.

[93] *Id*. The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[94] The service is defined in section 90.1301 *et seq*. of the Commission's Rules, 47 CFR § 90.1301 *et seq*.

[95] *See Service Rules for Advanced Wireless Services in the 1.7 GHz and 2.1 GHz Bands*, Report and Order, 18 FCC Rcd 25162, Appx. B (2003), modified by *Service Rules for Advanced Wireless Services in the 1.7 GHz and 2.1 GHz Bands*, Order on Reconsideration, 20 FCC Rcd 14058, Appx. C (2005); *Service Rules for Advanced Wireless Services in the 1915–1920 MHz, 1995–2000 MHz, 2020–2025 MHz and 2175–2180 MHz Bands; Service Rules for Advanced Wireless Services in the 1.7 GHz and 2.1 GHz Bands*, Notice of Proposed Rulemaking, 19 FCC Rcd 19263, Appx. B (2005); *Service Rules for Advanced Wireless Services in the 2155–2175 MHz Band*, Notice of Proposed Rulemaking, 22 FCC Rcd 17035, Appx. (2007).

small business entities in future auctions, the Commission has adopted a two-tiered small business size standard in the *Narrowband PCS Second Report and Order*.[96] Through these auctions, the Commission has awarded a total of 41 licenses, out of which 11 were obtained by small businesses.[97] A "small business" is an entity that, together with affiliates and controlling interests, has average gross revenues for the three preceding years of not more than $40 million. A "very small business" is an entity that, together with affiliates and controlling interests, has average gross revenues for the three preceding years of not more than $15 million. The SBA has approved these small business size standards.[98]

29. *Broadband Personal Communications Service*. The broadband personal communications service (PCS) spectrum is divided into six frequency blocks designated A through F, and the Commission has held auctions for each block. The Commission initially defined a "small business" for C- and F-Block licenses as an entity that has average gross revenues of $40 million or less in the three previous calendar years.[99] For F-Block licenses, an additional small business size standard for "very small business" was added and is defined as an entity that, together with its affiliates, has average gross revenues of not more than $15 million for the preceding three calendar years.[100] These standards defining "small entity", in the context of broadband PCS auctions, have been approved by the SBA.[101] No small businesses within the SBA-approved small business size standards bid successfully for licenses in Blocks A and B. There were 90 winning bidders that claimed small business status in the first two C-Block auctions. A total of 93 bidders that claimed small business status won approximately 40 percent of the 1,479 licenses in the first auction for the D-, E-, and F-Blocks.[102] On April 15, 1999, the Commission completed the reauction of 347 C-, D-, E-, and F-Block licenses in Auction No. 22.[103] Of the 57 winning bidders in that auction, 48 claimed small business status and won 277 licenses.

30. On January 26, 2001, the Commission completed the auction of 422 C- and F-Block Broadband PCS licenses in Auction No. 35. Of the 35 winning bidders in that auction, 29 claimed small business status.[104] Subsequent events concerning Auction No. 35, including judicial and agency determinations, resulted in a total of 163 C- and F-Block licenses being available for grant. On February 15, 2005, the Commission completed an auction of 242 C-, D-, E-, and F-Block licenses in Auction No.

---

[96] *Amendment of the Commission's Rules to Establish New Personal Communications Services, Narrowband PCS*, GEN Docket No. 90-314, ET Docket No. 92-100, PP Docket No. 93-253*, Second Report and Order and Second Further Notice of Proposed Rulemaking*, 15 FCC Rcd 10456 (2000).

[97] *Id*.

[98] *See* Letter from Aida Alvarez, Administrator, SBA, to Amy Zoslov, Chief, Auctions and Industry Analysis Division, Wireless Telecommunications Bureau, FCC (filed Dec. 2, 1998) (*Alvarez Letter 1998*).

[99] *See Amendment of Parts 20 and 24 of the Commission's Rules—Broadband PCS Competitive Bidding and the Commercial Mobile Radio Service Spectrum Cap; Amendment of the Commission's Cellular/PCS Cross-Ownership Rule*, WT Docket No. 96-59, GN Docket No. 90-314, Report and Order, 11 FCC Rcd 7824, 7850-52, paras. 57-60 (1996) (*PCS Report and Order*); *see also* 47 CFR § 24.720(b).

[100] *See PCS Report and Order*, 11 FCC Rcd at 7852, para. 60.

[101] *See* Letter from Aida Alvarez, Administrator, SBA, to Amy Zoslov, Chief, Auctions & Industry Analysis Division, Wireless Telecommunications Bureau, FCC, (Dec. 2, 1998) (*Alvarez Letter 1998*).

[102] *See D, E and F Block Auction Closes*, Public Notice, DA 97-81, 1 (Jan. 15, 1997) 1997 WL 20711.

[103] *See C, D, E, and F Block Broadband PCS Auction Closes*, Public Notice, 14 FCC Rcd 6688 (WTB 1999). Before Auction No. 22, the Commission established a very small standard for the C Block to match the standard used for F Block. *Amendment of the Commission's Rules Regarding Installment Payment Financing for Personal Communications Services (PCS) Licensees*, WT Docket No. 97-82, Fourth Report and Order, 13 FCC Rcd 15743, 15768, para. 46 (1998).

[104] *See C and F Block Broadband PCS Auction Closes; Winning Bidders Announced*, Public Notice, 16 FCC Rcd 2339 (2001).

58. Of the 24 winning bidders in that auction, 16 claimed small business status and won 156 licenses.[105] On May 21, 2007, the Commission completed an auction of 33 licenses in the A-, C-, and F-Blocks in Auction No. 71.[106] Of the 12 winning bidders in that auction, five claimed small business status and won 18 licenses.[107] On August 20, 2008, the Commission completed the auction of 20 C-, D-, E-, and F-Block Broadband PCS licenses in Auction No. 78.[108] Of the eight winning bidders for Broadband PCS licenses in that auction, six claimed small business status and won 14 licenses.[109]

31. *Wireless Communications Services*. This service can be used for fixed, mobile, radiolocation, and digital audio broadcasting satellite uses. The Commission defined "small business" for the wireless communications services (WCS) auction as an entity with average gross revenues of $40 million for each of the three preceding years, and a "very small business" as an entity with average gross revenues of $15 million for each of the three preceding years.[110] The SBA has approved these small business size standards.[111] In the Commission's auction for geographic area licenses in the WCS there were seven winning bidders that qualified as "very small business" entities, and one that qualified as a "small business" entity.[112]

32. *Radio and Television Broadcasting and Wireless Communications Equipment Manufacturing*. This industry comprises establishments primarily engaged in manufacturing radio and television broadcast and wireless communications equipment.[113] Examples of products made by these establishments are: transmitting and receiving antennas, cable television equipment, GPS equipment, pagers, cellular phones, mobile communications equipment, and radio and television studio and broadcasting equipment.[114] The SBA has established a small business size standard for this industry of 1,250 employees or less.[115] U.S. Census Bureau data for 2012 shows that 841 establishments operated in this industry in that year.[116] Of that number, 828 establishments operated with fewer than 1,000

---

[105] *See Broadband PCS Spectrum Auction Closes; Winning Bidders Announced for Auction No. 58*, Public Notice, 20 FCC Rcd 3703 (2005).

[106] *See Auction of Broadband PCS Spectrum Licenses Closes; Winning Bidders Announced for Auction No. 71*, Public Notice, 22 FCC Rcd 9247 (2007).

[107] *Id*.

[108] *See Auction of AWS-1 and Broadband PCS Licenses Closes; Winning Bidders Announced for Auction 78*, Public Notice, 23 FCC Rcd 12749 (WTB 2008).

[109] *Id*.

[110] *Amendment of the Commission's Rules to Establish Part 27, the Wireless Communications Service (WCS)*, Report and Order, 12 FCC Rcd 10785, 10879, para. 194 (1997).

[111] *See* Letter from Aida Alvarez, Administrator, SBA, to Amy Zoslov, Chief, Auctions and Industry Analysis Division, Wireless Telecommunications Bureau, FCC (filed Dec. 2, 1998) (*Alvarez Letter 1998*).

[112] *See WCS Auction Closes; Winning Bidders in the Auction of 128 Wireless Communications Licenses; FCC Form 600s Due May 12, 1997,* 12 FCC Rcd 21653, DA-97-886, Report No. AUC-997-14-E (Auction No.14) (April 28, 1997).

[113] *See* U.S. Census Bureau, *2017 NAICS Definition, "334220 Radio and Television Broadcasting and Wireless Communications Equipment Manufacturing",* https://www.census.gov/cgi-bin/sssd/naics/naicsrch?code=334220&search=2017.

[114] *Id*.

[115] *See* 13 CFR § 121.201, NAICS Code 334220.

[116] *See* U.S. Census Bureau, *2012 Economic Census of the United States*, Table ID: EC1231SG2, *Manufacturing: Summary Series: General Summary: Industry Statistics for Subsectors and Industries by Employment Size: 2012*, NAICS Code 334220,

(continued….)

employees, 7 establishments operated with between 1,000 and 2,499 employees, and 6 establishments operated with 2,500 or more employees.[117] Based on this data, we conclude that a majority of manufacturers in this industry are small.

D. Description of Projected Reporting, Recordkeeping, and Other Compliance Requirements for Small Entities

33. The actions proposed in the *Notice*, if adopted, will impose additional reporting, recordkeeping and/or other compliance obligations on certain small, as well as other, entities that process WEA alerts and manufacture mobile devices that receive such alerts, and could impose additional reporting, recordkeeping and/or other compliance obligations on small, as well as other, entities that , administer State EAS Plans, process and transmit EAS alerts, and manufacture equipment designed to process EAS alerts.

34. More specifically, the *Notice* seeks comment on adding a national alert category of FEMA Administrator national alerts to WEA that WEA-enabled mobile devices could not opt-out of receiving, which, as proposed will require modifications to Commercial Mobile Service (CMS) providers' network and/or mobile device equipment. Our proposal would accomplish this required change by combining the existing Presidential Alert class of WEA alerts with the new FEMA Administrator class of alerts into a single new category of "National Alerts." As proposed, our actions would require certain CMS providers to update device WEA alert header displays and settings menus related to their network infrastructure, including mobile devices. We propose an implementation timeline of approximately one year for CMS providers to make these changes to device displays.

35. The *Notice* also seeks comment on requiring that each SECC, not less frequently than annually, shall meet to review and update its State EAS Plan, and certify as much in the updated plan it submits annually to the Commission. In response to NDAA21's requirement for the Commission to adopt regulations requiring SECCs to meet annually to review and update their State EAS Plan, and to certify that such meeting was completed, we propose to amend section 11.21 of our rules to include as a required element in the State EAS Plan, a certification by the SECC Chairperson or Vice-Chairperson that the SECC meet (in person, via teleconference, or via other methods of conducting virtual meetings) at least once in the twelve months prior to submitting the annual updated plan to review and update their State EAS Plan. We further propose that such certification, if adopted, would be incorporated into the ARS. Section 11.21 already includes a requirement that State EAS Plans be updated annually, and the ARS requires annual updating as well, however, we propose to add some clarifying language to section 11.21 to more closely reflect the legislation's requirements on this point. To the extent any SECC is not meeting annually, such meeting requirement may require greater coordination efforts on the part of such SECC. The *Notice* also seeks comment on the creation of a proposed State EAS Plan content checklist for SECCs to use when reviewing and updating a State EAS Plan for submission to the Commission that identifies the information requested to ensure more complete State EAS Plan reporting. Section 11.21 already includes a listing of information required in the State EAS Plan, and the Alert Reporting System (ARS) data entry menus mirror these informational requirements (and will not allow a State EAS Plan to be submitted unless all required fields are completed). In the *Notice,* we inquire whether there is other information that should be included as part of the checklist for reporting.

36. In addition, the *Notice* seeks comment on modifying the EAS rules to provide for repeating EAS alerts issued by the President, the Administrator of FEMA and any other entity determined appropriate under the circumstances by the Commission. To the extent the modifications adopted involve adding a new alert originator and/or event code, or other changes to the EAS Protocol or alert processing

https://data.census.gov/cedsci/table?text=EC1231SG2&n=334220&tid=ECNSIZE2012.EC1231SG2&hidePreview=false.

[117] *Id*. The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

by the EAS device, such change(s) likely would entail modifying the existing deployed base of EAS devices via software updates, which would entail some installation-related costs.

37. The NDAA21 also requires the Commission to establish a voluntary reporting system to receive from the FEMA Administrator or State, local, Tribal, or territorial governments reports of false alerts under the Emergency Alert System or the Wireless Emergency Alerts System for the purpose of recording such false alerts and examining the causes of such false alerts. To address this requirement, we propose to revise our rules to specify that, if the Administrator of FEMA or a State, local, Tribal, or territorial government entity becomes aware of transmission of an EAS or WEA false alert to the public, they may send an email to the Commission to inform the Commission of the false alert event and of any details that they may have concerning the event. In addition, we propose a minor revision to the existing rule requiring false alert reports from EAS industry participants to clarify the required nature of those reports compared to the voluntary reporting system for the Administrator of FEMA or a State, local, Tribal, or territorial government entity.

38. To help the Commission more fully evaluate the cost of compliance should our proposals be adopted, in the *Notice* we request comments on the cost implications of our proposals and ask whether there are more efficient and less burdensome alternatives for the Commission to address our obligations under the NDAA21. Although the Commission cannot fully quantify the cost of compliance for all small entities impacted by the rules proposed in the *Notice*, we believe our proposed modifications to the WEA and EAS rules are the most efficient and least burdensome approach to codifying the requirements of the NDAA21. We expect the information we receive in comments including cost and benefit analyses, to help the Commission identify and evaluate relevant matters for small entities, including compliance costs and other burdens that may result from the proposals and inquiries we make in the *Notice*.

E. Steps Taken to Minimize the Significant Economic Impact on Small Entities, and Significant Alternatives Considered

39. The RFA requires an agency to describe any significant, specifically small business alternatives that it has considered in reaching its proposed approach, which may include the following four alternatives (among others): "(1) the establishment of differing compliance or reporting requirements or timetables that take into account the resources available to small entities; (2) the clarification, consolidation, or simplification of compliance or reporting requirements under the rule for small entities; (3) the use of performance, rather than design, standards; and (4) and exemption from coverage of the rule, or any part thereof, for small entities."[118]

40. The proposed actions in the *Notice* are designed to be minimally burdensome to all affected entities, including small entities. While the Commission does not expect the proposals to have a significant economic impact on small entities, below we discuss actions that should minimize any significant impact on small entities and some alternatives we considered.

41. The Commission believes that its proposal to replace WEA's existing Presidential Alert class with a National Alert class is the appropriate approach because it would require few, if any, technical changes to be made to participating CMS provider networks or the mobile devices of their subscribers and impose fewer costs than available alternatives. This proposal allows all participating CMS providers' wireless systems currently receiving mandatory Presidential Alerts, to receive "National Alerts" the same way -- distributed automatically as a non-optional alert to the same class of wireless customers that they currently receive Presidential Alerts. This can be effectuated by using the existing WEA handling code for Presidential Alerts along with the name change to "National Alerts," which minimizes costs for participating CMS providers. With respect to our proposal to require participating CMS providers that use WEA header displays that read "Presidential Alert" to change those alert headers to read "National Alert," the Commission's approach grants participating CMS providers flexibility in the

[118] 5 U.S.C. §§ 603(c)(1)-(4).

approach they use to ensure compliance. Specifically, this proposed requirement could be satisfied by any approach that ensures that "Presidential Alert" is not displayed on a user's mobile device, whether by changing the displayed header or not displaying the header at all. The Commission further proposes to reduce the burden on participating CMS providers by exempting from the requirement any network infrastructure that is technically incapable of meeting this requirement, such as situations in which legacy devices or networks cannot be updated to support this functionality. In our efforts to minimize costs and explore other alternatives, we have requested comments on each of these WEA proposals as well as on costs implications and cost estimates for these proposals as well as any alternatives.

42. The proposals to require each SECC to meet not less frequently than annually to review and update its State EAS Plan and certify as much in the updated plan it submits annually to the Commission, should not impose burdens on SECCs. The proposal allows SECCs to meet virtually, thus to the extent any SECC is not already meeting regularly, the annual meeting requirement would only entail greater coordination efforts on the part of such SECC to arrange a mutually agreeable time and meeting platform. While we recognize that the requirement to certify that the SECC has meet by phone, IP-based meeting application, or in person at least once annually, may impose some costs for SECC members, it is likely that many if not most SECCs are already are meeting in some form on a regular basis, and therefore the proposed annual meeting certification likely will certify an activity already being undertaken and documented.

43. In adopting a voluntary reporting process for FEMA or a State, local, Tribal, or territorial government entity to report false EAS or WEA transmissions to the Commission, we believe that our proposal, which provides a reporting system for receipt of false alerts via email directed to the Commission's Operations Center, is the most efficient, least costly, and least onerous method to implement this system. We have also structured this voluntary reporting system to be similar in format to the existing reporting requirement the Commission adopted in the *Alerting Reliability Order and FNPRM*, requiring EAS industry participants to report false EAS alerts to the Commission via email sent to the FCC Operations Center, [119] avoiding the need for duplicative structures.

44. The primary rule modification proposed to provide for repeating EAS alerts issued by the President, the Administrator of FEMA and any other entity determined appropriate under the circumstances by the Commission would not add any burdens to any entity. To the extent the modifications adopted involve adding a new alert originator and/or event code, or other changes to the EAS Protocol or alert processing by the EAS device, such change(s) likely would entail modifying the existing deployed base of EAS devices via software updates, which would entail some minimal installation-related costs.

45. Throughout the *Notice*, the Commission has requested comment on the relative costs and benefits of these various proposed alternatives to ensure it has input from small entities and others to minimize the economic impacts of whatever actions it might take. Nevertheless, in addition to the steps taken by the Commission discussed herein, commenters have been invited to propose steps that the Commission may take to further minimize any economic impact on small entities. Commenters have also been invited to propose alternatives that facilitate the Commission's obligations to implement the NDAA21 provisions.

F. Federal Rules that May Duplicate, Overlap, or Conflict with the Proposed Rules

46. None.

[119] *See In the Matter of Amendment of Part 11 of the Commission's Rules Regarding the Emergency Alert System; Wireless Emergency Alerts*, PS Docket No. 15-94, Report and Order and Further Notice of Proposed Rulemaking, 33 FCC Rcd 7086, 7094-5, paras. 17-18 (2018) (*Alerting Reliability Order and FNPRM*). This reporting requirement is codified in section 11.45(b) of our rules, 47 CFR § 11.45(b).

STATEMENT OF
ACTING CHAIRWOMAN JESSICA ROSENWORCEL

Re: *Amendment of Part 11 of the Commission's Rules Regarding the Emergency Alert System*; *Wireless Emergency Alerts*, PS Docket Nos. 15-94, 15-91, Notice of Proposed Rulemaking and Notice of Inquiry (March 17, 2021)

It may feel like a lifetime ago, but back in January 2018 the people of Hawaii woke to ominous messages flashing on their mobile phones. The same messages lit up their television screens, boomed out from radio stations, and streamed in from social media. They directed all who saw and heard to seek immediate shelter due to a ballistic missile threat. They included the haunting words: "This is not a drill."

But it was. In fact, it was a false missile alert that went horribly wrong. It caused fear and panic throughout a state keenly aware of history and the threats associated with its place in the Pacific.

Later that year, I testified at a United States Senate field hearing in Honolulu that was led by Senator Schatz to investigate what went wrong with this false missile alert and identify ways to make it right. It was a productive effort. I was able to join the Director of Operations of United States Pacific Command, the leadership of the Hawaii Department of Defense, and other public safety officials to offer ideas about how we can prevent a false alert like this from ever happening again.

I put forth two ideas in my testimony. First, I suggested that we set up a system for reporting false alerts, so we can learn from our errors going forward. Second, I suggested that we use the filing of State Emergency Alert System plans at this agency to promote best practices and halt the problems that we saw in Hawaii.

This is important because as it turns out, this false alert exposed some very real problems in the ways that Americans receive emergency alerts. When it went out across Hawaii, some people never got the message on their phones. Others missed it on their televisions and radios. And of course, there was the troubling fact that this even happened in the first place.

So I am pleased that today the Federal Communications Commission will begin to implement the READI Act to help fix these problems. The goal here is making sure that in an emergency the public gets the accurate information it needs as quickly as possible. To this end, we propose rules to ensure that mobile devices cannot opt-out of receiving Wireless Emergency Alerts from the Administrator of the Federal Emergency Management Agency. We also seek to develop ideas to ensure that states review and update their Emergency Alert Plans and that additional stakeholders can report false alerts to the FCC. In addition, we begin an inquiry—as the law requires—to study internet-based alerting efforts.

This action is timely. According to FEMA, our reliance on Wireless Emergency Alerts has increased by almost 300 percent in the last year, thanks largely to the ongoing pandemic. And if you are thinking that what happened in Hawaii can't happen again, just two weeks ago a false alert went out across Kansas and Missouri warning of "imminent extreme danger" from a tornado. So we have work to do.

Thank you to the staff who worked on this item. From the Public Safety and Homeland Security Bureau that's Steve Carpenter, Christina Clearwater, Chris Fedeli, Lisa Fowlkes, Nikki McGinnis, Dave Munson, Austin Randazzo, Renee Roland, Rasoul Safavian, and James Wiley. From the Office of General Counsel that's David Horowitz, Andrea Kearney, Bill Richardson, and Anjali Singh. From the Office of Economics and Analytics that's Chuck Needy and Emily Talaga. From the Wireless Telecommunications Bureau that's Kari Hicks and from the Wireline Competition Bureau that's Pamela

Arluk and Kirk Burgee. From the Consumer and Governmental Affairs Bureau a thank you to Zac Champ and Greg Cooke. From the Media Bureau a thank you to Hillary DeNigro and Evan Morris and from the Enforcement Bureau a thank you to Shannon Lipp, Jeremy Marcus, and Ashley Tyson. Last but not least, from the Office of Communications Business Opportunities thank you to Chana Wilkerson and Sanford Williams.