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

In the Matter of	)	
	)	
Modernization of the Nation's Alerting Systems	)	PS Docket No. 25-224
	)	
Protecting the Nation's Communications Systems from Cybersecurity Threats	)	PS Docket No. 22-329
	)	
Wireless Emergency Alerts	)	PS Docket No. 15-91
	)	
Amendment of Part 11 of the Commission's Rules Regarding the Emergency Alert System	)	PS Docket No. 15-94

REPORT AND ORDER IN PS DOCKETS 25-224 AND 22-329, AND FURTHER NOTICE OF PROPOSED RULEMAKING IN PS DOCKETS 25-224, 15-94, AND 15-91

Adopted: June 25, 2026 **Released: June 29, 2026**

Comment Date: (30 days after date of publication in Federal Register)
Reply Comment Date: (60 days after date of publication in Federal Register)

By the Commission: Chairman Carr and Commissioner Trusty issuing separate statements

TABLE OF CONTENTS

I. INTRODUCTION

1. Last year, we adopted a *Notice of Proposed Rulemaking* that launched a reexamination of the nation's alerting systems to explore ways to make them more effective, efficient, and better able to serve the public's needs.[1] We asked the public to take a fresh look at whether the Emergency Alert System (EAS) and Wireless Emergency Alerts (WEA) are achieving their goals and to tell us whether these systems should be changed—perhaps fundamentally—to ensure that they are leveraging the latest technology to save lives and not hampered by archaic regulatory requirements. Dozens of commenters responded with a wide range of ideas about alerting systems' strengths, needs, and future potential. The record demonstrates that while EAS and WEA remain effective, there are opportunities to make those systems even more resilient, flexible, and useful.

2. Today, we take steps to modernize EAS and WEA. This *Report and Order* aims to preserve the public's trust in EAS by requiring targeted cybersecurity improvements that will help protect against hijacking by cybercriminals and our nation's adversaries. The accompanying *Further Notice of Proposed Rulemaking* (*Further Notice*) seeks to:

- Improve EAS's integrity by proposing to require the authentication of all alerts before they are transmitted.
- Bolster the reliability of emergency alerts by proposing to establish a universal alert identification number to improve the detection and blocking of duplicate alerts and ensure that WEAs are consistently sent to members of the public who newly enter an alert's delivery area until the emergency ends.
- Improve geographic accuracy by proposing to eliminate outdated WEA geotargeting exceptions that often cause alerts to be received in the wrong locations and expand geotargeting options for EAS.
- Make alerts more effective by seeking comment on requiring EAS and WEA to display symbols that match the type of emergency and improving the ability of earthquake alerts to grab the public's attention.
- Remove outdated and unnecessary alerting requirements by proposing to allow the implementation of EAS capabilities via software instead of hardware and retire the 90-character-maximum versions of WEA messages.

[1] *Modernization of the Nation's Alerting Systems*, PS Docket No. 25-224, Notice of Proposed Rulemaking, 40 FCC Rcd 6695 (2025) (*Alerting Modernization NPRM*).

We believe that these steps will make the nation's alerting systems more helpful to alerting authorities, less unnecessarily burdensome for participating communications providers, and better able to save lives.

II. BACKGROUND

3. The United States' national public alert and warning system provides the President and thousands of authorized federal, state, Tribal, territorial, and local entities (known as alerting authorities) with the ability to send emergency alerts to the public.[2] The system comprises the Integrated Public Alert and Warning System (IPAWS), administered by the Federal Emergency Management Agency (FEMA),[3] and several alerting pathways that include EAS and WEA. Radio and television stations, cable television systems, satellite radio and television services, and wireline video providers (collectively, "EAS Participants") deliver emergency alerts through EAS,[4] while Commercial Mobile Service (CMS) Providers deliver emergency alerts to mobile devices through WEA.[5] When an alerting authority sends an emergency alert, it can choose which alerting pathways it will use to reach the public.

4. EAS Participants receive and disseminate EAS alerts using two methods. EAS Participants receive alerts via the legacy EAS architecture by monitoring for alerts sent by other EAS Participants. These alerts include an audio attention signal as well as audio-encoded tones, commonly referred to as EAS codes, that include information about the alert, including the type of emergency, the targeted geographic area, and the time that the alert expires.[6] EAS Participants use these EAS codes to determine whether the alert should be transmitted to their audiences. This process repeats through a "daisy chain" of EAS Participants until all EAS Participants serving the targeted geographic area have transmitted the alert. EAS Participants also acquire alerts directly from IPAWS over the Internet in an IP-based format called the Common Alerting Protocol (CAP).[7] CAP allows for inclusion of additional data and media, including geographic coordinates that allow for more flexible and precise alert targeting. EAS Participants are required to transmit the CAP versions of alerts when they are available and to include the

[2] *See* 47 CFR § 11.1 (stating that EAS "provides the President with the capability to provide immediate communications and information to the general public at the National, State and Local Area levels during periods of national emergency"); Warning, Alert, and Response Network Act, Title VI of the Security and Accountability for Every Port Act of 2006, 120 Stat. 1884, 1936 (2006) (codified at 47 U.S.C. § 1201 *et seq.*) (WARN Act).

[3] FEMA, *IPAWS 101, Integrated Public Alert & Warning System* (Jan. 2024), https://www.fema.gov/sites/default/files/documents/fema_ipaws_101-slicksheet_042024.pdf. Because IPAWS falls within FEMA's purview, it is outside the scope of this proceeding.

[4] *See* 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").

[5] *See* 47 U.S.C. § 1201(a); 47 CFR § 10.10(d) (defining a CMS Provider as an "FCC licensee providing commercial mobile service as defined in section 332(d)(1) of the Communications Act of 1934"); *see also* 47 CFR § 10.10(a) (defining an "Alert Message" for the purpose of WEA as "a message that is intended to provide the recipient information regarding an emergency, and that meets the requirements for transmission by a Participating Commercial Mobile Service Provider under this part"). Hereinafter, we use the term "WEA message" to refer to Alert Messages, as defined.

[6] *See* 47 CFR § 11.31. Legacy EAS uses six-digit location geocodes that specify the State (SS), County (CCC), and portion of a county (P) where an alert is relevant. 47 CFR § 11.31(c); *see also* FCC, *Federal Information Processing System (FIPS) Codes for States and Counties*, https://transition.fcc.gov/oet/info/maps/census/fips/fips.txt (last visited June 1, 2026). EAS Participants manually program their equipment to retransmit only alerts that specify certain geocodes, which typically reflect the geographic location of their audience.

[7] *See* 47 CFR § 11.56.

legacy EAS codes in their transmission.[8] EAS Participants are currently required to process EAS alerts using purpose-built, FCC-certified EAS equipment.[9]

5. Participating CMS Providers receive WEA messages from IPAWS in CAP that they transmit to mobile devices like cell phones, generally using cell broadcast technology.[10] WEA messages can be up to 360 characters in length, but Participating CMS Providers are also required to transmit less detailed, 90-character-maximum versions of WEA messages to ensure compatibility on legacy networks (e.g., 2G and 3G).[11] Participating CMS Providers are required to use the coordinates included in the WEA message to deliver it to 100 percent of the target area with no more than 0.1 of a mile overshoot.[12] However, there are exceptions to this requirement for legacy networks and mobile devices, as well as for mobile devices that have location services disabled.[13] In such excepted cases, Participating CMS Providers are only required to deliver WEA messages "to an area that best approximates the specified target . . . ."[14] Some, but not all, Participating CMS Providers will retransmit an alert at regular intervals after it is first transmitted to better ensure that it is received by everyone in the target area, including those who travel into the area after the alert is first sent.[15] The public may opt out of receiving WEA messages on their personal devices, except for the National Alert.[16]

6. In the 2022 *Alerting Security NPRM*, the Commission responded to troubling security incidents by proposing sweeping cybersecurity requirements for EAS Participants and Participating CMS Providers.[17] Specifically, the Commission proposed to require: (1) EAS Participants to report

[8] *See* 47 CFR § 11.55(c).

[9] *See* 47 CFR §§ 11.32, 11.33.

[10] *See Wireless Emergency Alerts; Amendments to Part 11 of the Commission's Rules Regarding the Emergency Alert System*, PS Docket Nos. 15-91 and 15-94, Second Report and Order and Second Order on Reconsideration, 33 FCC Rcd 1320, 1322, para. 3 (2018) (*2018 Second WEA R&O*) ("most Participating CMS Providers use cell broadcast technology to transmit WEA Alert Messages to their subscribers."). The Commission maintains rules for mobile devices that Participating CMS Providers market as "WEA-capable," including, among other things, that such mobile devices support requirements related to geotargeting, message length, and duplicate alert suppression. 47 CFR § 10.500(g), (j).

[11] *See Wireless Emergency Alerts; Amendments to Part 11 of the Commission's Rules Regarding the Emergency Alert System*, PS Docket Nos. 15-91 and 15-94, Report and Order and Further Notice of Proposed Rulemaking, 31 FCC Rcd 11112, 11120-25, paras. 11-15 (2016) (*2016 WEA R&O*); 47 CFR § 10.430.

[12] *See* 47 CFR § 10.450(a).

[13] *See 2018 Second WEA R&O*, 33 FCC Rcd at 1324-25, 1327-28, paras. 6, 9 (these exceptions include legacy infrastructure and legacy mobile devices); 47 CFR § 10.450(a).

[14] 47 CFR § 10.450(a). In response to a request from the U.S. Geological Survey (USGS), the Bureau issued a waiver permitting participating wireless providers to forgo enhanced geotargeting for earthquake early warnings and related Public Safety Messages issued by USGS. *See Improving Wireless Emergency Alerts and Community-initiated Alerting*, PS Docket No. 15-91, Order, 34 FCC Rcd 8574 (PSHSB 2019).

[15] *See* Letter from Shellie Blakeney, Director, Federal Regulatory Affairs, T-Mobile USA, Inc. to Lisa M. Fowlkes, Chief, Public Safety and Homeland Security Bureau at 2 (filed Aug. 25, 2021) ("T-Mobile rebroadcast the test message 6 times over its UMTS/4G/5G networks at 5 minute intervals, and 8 times over its GSM network at 4 minute intervals."); Letter from Jamie M. Tan, Director, Federal Regulatory, AT&T Services, Inc. to Lisa M. Fowlkes, Chief, Public Safety and Homeland Security Bureau at 2 (filed Aug. 25, 2021) ("The repetition period for retransmitting WEA messages is once every 60 seconds."); Letter from Robert G. Morse, Associate General Counsel, Federal Regulatory and Legal Affairs, Verizon to Lisa M. Fowlkes, Chief, Public Safety and Homeland Security Bureau at 3 (filed Aug. 25, 2021) ("Verizon retransmits WEA messages one time, 1 minute after the initial message is transmitted.").

[16] *See* 47 CFR § 10.280(a); *see also* 47 U.S.C. § 1201(b)(2)(E).

compromises of their EAS equipment, communications systems, and services to the Commission;[18] (2) EAS Participants and Participating CMS Providers to annually certify to having a cybersecurity risk management plan in place and to implement sufficient security measures to ensure the confidentiality, integrity, and availability of their respective alerting systems;[19] and (3) Participating CMS Providers to take steps to ensure that only valid alerts are displayed on consumer devices.[20] The proposed cybersecurity risk management plans would have been required to include security measures that address changing default passwords prior to operation, installing security updates in a timely manner, and securing equipment behind properly configured firewalls or using other segmentation practices, among other measures.[21] The Commission also sought comment on other ways to strengthen the operational readiness of EAS equipment.[22] The Commission received 27 comments and 15 reply comments in response to these proposals.

7. On March 31, 2025, the National Association of Broadcasters (NAB) filed a Petition for Rulemaking requesting that the Commission clarify or modify its rules to allow EAS Participants to support EAS through software-based technology instead of dedicated physical equipment.[23] With respect to broadcasters, NAB proposes that the software would be located within each broadcaster's facilities and running on certified hardware platforms.[24] NAB argues that broadcasters will work with manufacturers to develop suitable software, as they have before when replacing other legacy hardware systems.[25] NAB also contends that eliminating the requirement to use dedicated EAS hardware systems will promote resiliency and operational readiness by making it easier to implement software updates and patches remotely, without taking devices offline.[26] The Commission received 15 comments and four reply comments in response to NAB's Petition.

8. In August 2025, the Commission adopted a *Notice of Proposed Rulemaking* (*Alerting Modernization NPRM*) that commenced a ground-up review of the nation's alerting systems.[27] The Commission sought comment on broad questions such as what goals these alerting systems should aim to achieve, whether these systems are currently effective at achieving these goals, and what steps the Commission should take to modernize these systems to improve their usefulness and better leverage modern technology while minimizing burdens on stakeholders. The *Alerting Modernization NPRM* also

(Continued from previous page)

[17] *See Amendment of Part 11 of the Commission's Rules Regarding the Emergency Alert System; Wireless Emergency Alerts; Protecting the Nation's Communications Systems from Cybersecurity Threats*, PS Docket Nos. 15-94, 15-91, and 22-329, Notice of Proposed Rulemaking, 37 FCC Rcd 12932, 12934-35, para. 4 (2022) (*Alerting Security NPRM*).

[18] *Alerting Security NPRM*, 37 FCC Rcd at 12939-43, paras. 13-21.

[19] *Id.* at 12942-49, paras. 22-36.

[20] *Id.* at 12949-51, paras. 37-40.

[21] *Id.* at 12945, para. 25.

[22] *Id.* at 12933, 12938-40, paras.1, 9-12.

[23] Petition of the National Association of Broadcasters for Emergency Alert System (EAS) Modernization, PS Docket Nos. 15-94 and 22-329 (filed Mar. 31, 2025), https://www.fcc.gov/ecfs/document/1033123856452/1 (NAB Petition); *see also* National Association of Broadcasters Comments, PS Docket Nos. 15-94, 15-91, and 22-329, at 24-27 (rec. Dec. 23, 2022), https://www.fcc.gov/ecfs/document/122799922742/2 (NAB Alerting Security NPRM Comments) (proposing that the Commission allow EAS software).

[24] NAB Petition at 4.

[25] *Id.* at 5-6.

[26] *Id.* at 6.

[27] *Alerting Modernization NPRM*, 40 FCC Rcd at 6695.

sought comment on the security of EAS and WEA and what security measures these systems should be designed to incorporate.[28] The Commission received 55 comments and 20 replies from a wide range of stakeholders, including communications service providers, equipment manufacturers, trade associations, public safety advocacy organizations, government agencies, and individual members of the public.

III. REPORT AND ORDER

A. Goals of the Nation's Alerting Systems

9. In the *Alerting Modernization NPRM*, we sought comment on the objectives that effective alert and warning systems should serve.[29] Specifically, we sought comment on three possible core goals: (1) alerting systems should provide authorities with the ability to rapidly notify the public of emergencies that may put the public at risk; (2) alerting systems should be capable of delivering instructions that facilitate the protection of life and property; and (3) alerting systems should provide a mechanism for government officials to provide additional authoritative communications with the public before, during, and after an emergency.[30] Commenters generally agree that these should be the overarching goals of the nation's alert and warning systems. The Alliance for Telecommunications Industry Solutions (ATIS) "fully supports these three goals and notes that the industry has continuously evolved WEA to meet these objectives."[31] The Competitive Carriers Association (CCA) believes that these "broad but simple goals proposed for the nation's alerting systems . . . seem appropriate . . . [as they] are worthwhile, important to public safety, and consistent with statutory instructions and intent."[32] North Carolina Emergency Management et al., the Harris County Office of Homeland Security & Emergency Management (Harris County), APCO International (APCO), and the National Weather Service (NWS) also agree with the three stated objectives, with the NWS noting that, "[w]hile a perfect alerting system is not possible, it should have the main goal of being easy to use and available to anyone."[33]

10. The U.S. Geological Survey (USGS) supports the three core goals the Commission proposed for alerting systems, but contends that they "are focused on the capabilities of the system rather than on the public safety outcomes they are intended to achieve."[34] Sonoma County Department of Emergency Management, Snohomish County Department of Emergency Management, former California Office of Emergency Services Director Art Botterrell, and Washington State Emergency Management

[28] *Id.* at 6701, para. 15.

[29] *Id.* at 6698, para. 7.

[30] *See id.*

[31] Alliance for Telecommunications Industry Solutions Comments, PS Docket No. 25-224, at 2 (rec. Sept. 25, 2025) (ATIS Alerting Modernization NPRM Comments).

[32] Competitive Carriers Association Comments, PS Docket No. 25-224, at 2 (rec. Sept. 25, 2025) (CCA Alerting Modernization NPRM Comments).

[33] North Carolina Emergency Management Comments, PS Docket No. 25-224, at 8 (rec. Sept. 25, 2025) ("the Commission has accurately stated three key goals for 'effective alert and warning systems.'"); Harris County Office of Homeland Security & Emergency Management Comments, PS Docket No. 25-224, at 1 (rec. Sept. 4, 2025) (Harris County Alerting Modernization NPRM Comments) ("fully endorses the objectives set forth in the Notice," but cautions that effectiveness requires ensuring that "a national-level alerting system cannot be effective if all residents cannot receive critical information,"); APCO International Reply, PS Docket No. 25-224, at 4-5 (rec. Nov. 18, 2025) (APCO Alerting Modernization NPRM Reply) ("supports the Commission's three goals for emergency alerts. . ."); National Weather Service Comments, PS Docket No. 25-224, at 1 (rec. Sept. 25, 2025) (NWS Alerting Modernization NPRM Comments).

[34] U.S. Geological Survey Comments, PS Docket No. 25-224, at 2-3 (rec. Sept. 17, 2025) (USGS Alerting Modernization NPRM Comments).

Division likewise emphasize that public safety outcomes are of utmost importance.[35] iHeartMedia, Inc. supports the three objectives that we identified, but believes we should consider a fourth: "(4) alerting systems should include resilient and reliable delivery systems proven capable of functioning during emergencies, including when other emergency alerting technologies may be unavailable."[36] The New York City Emergency Management Department (NYCEM) agrees with us that "the speed of notification is a critical component of any alerting system" but proposes the following alternative to our third objective focused on ensuring the ability for authorities to send authoritative alerts to the public: "Alerting systems should be designed and utilized to ensure that all members of the public receive an alert and are aware of actions that they may take to protect life and property. . . . [A]lerting systems should be available in a wide array of languages, able to be displayed on various devices, and include considerations for members of the public with various accessibility needs."[37] Although we understand and appreciate the proposals for additional goals of alerting, we conclude that the three goals we proposed already encompass these important public safety-, resiliency-, and accessibility-focused concerns within the objectives that effective alert and warning systems should serve. For example, while we agree with iHeartMedia, Inc. that alerting systems must be resilient and reliable, and capable of functioning when other emergency alerting technologies may be unavailable, that objective is subsumed within our goal of providing authorities with the ability to rapidly notify the public of emergencies that may put them at risk. NYCEM's view that alerting systems should be available in a wide array of languages and on a variety of devices falls within the core goal of notifying the public of emergencies, as that notification can only occur if recipients can receive and understand the message.

11. Commenters recognize that the Commission should continue to evaluate ways to improve these systems, and we agree.[38] As Sinclair comments: "Ultimately, the nation's alerting systems are critical to the preservation of public health and safety, and examining ways to enhance or improve these systems can save lives."[39] We also find that commenters generally recommend that, while alerting

[35] Washington State Emergency Management Division Comments, PS Docket No. 25-224, at 2 (rec. Sept. 25, 2025) (Washington EMD Alerting Modernization NPRM Comments); County of Sonoma Department of Emergency Management Comments, PS Docket No. 25-224, at 1-2 (rec. Sept 16, 2025) (Sonoma DEM Alerting Modernization NPRM Comments); Snohomish County Department of Emergency Management Comments, PS Docket No. 25-224, at 1 (rec. Sept. 19, 2025) (Snohomish DEM Alerting Modernization NPRM Comments); Art Botterell Comments, PS Docket No. 25-224, at 2 (rec. Aug. 22, 2025) (Botterell Alerting Modernization NPRM Comments).

[36] iHeartMedia, Inc. Comments, PS Docket No. 25-224, at 1 (rec. Sept. 25, 2025).

[37] New York City Emergency Management Department Comments, PS Docket No. 25-224, at 2 (rec. Sept. 19, 2025) (NYCEM Alerting Modernization NPRM Comments); *see also* TDIforAccess, Inc., et al. Comments, PS Docket No. 25-224, at 3 (rec. Sept. 25, 2025) (Accessibility Organizations Alerting Modernization NPRM Comments) (alerts must provide essential information on the emergency; multimedia alerts should provide URL for further information; and alert must be accessible across multiple devices).

[38] *See, e.g.*, CTIA Reply, PS Docket No. 25-224, at 1-2 (rec. Nov. 18, 2025) (CTIA Alerting Modernization NPRM Reply) ("The record demonstrates that the current WEA system is one of the most effective, efficient, and reliable alert and warning tools for public safety and consumers across the country. . . [It is designed as a] bell-ringer system that quickly and efficiently disseminates alerting information in times of emergencies. . . . Rather than pursue a costly redesign of the system—which could undermine its low latency, high reliability, and high penetration rates—the Commission should ensure the WEA system continues to evolve by supporting flexible, stakeholder-led innovation and collaboration."); Madi Wangensteen Reply, PS Docket No. 25-224 (rec. Oct. 8, 2025) ("I support this proposed rule because updating these alert systems is essential to protecting public safety."); National Association of Broadcasters Comments, PS Docket No. 25-224, at 3 (rec. Sept. 25, 2025) (NAB Alerting Modernization NPRM Comments) ("In general, NAB strongly supports innovation of EAS, so long as the existing system that has consistently ensured the EAS system's core public warning function for so many decades is preserved."); Accessibility Organizations Alerting Modernization NPRM Comments at 3 (FCC should "provide resources to help originators improve performance over time").

systems can be improved, we should refrain from making fundamental changes to EAS and WEA.[40] We agree with commenters that these systems generally meet today's alerting objectives,[41] and determine that incremental improvements advance the core goals of the nation's alerting systems. At this time, we therefore decline to overhaul or phase out the legacy EAS architecture.[42] Legacy EAS continues to effectively support public safety by creating alerting pathway redundancy, making alerting more resilient, and by warning the public and informing them about protective actions to take during emergencies.[43] Eliminating it would create a gap in alert delivery that would threaten the achievement of our three goals.[44] Consistent with the record, we take steps to improve EAS and WEA as they exist today.

B. Cybersecurity Requirements Targeting Specific EAS Attack Vectors

12. Central to our effort to modernize the nation's alerting systems is ensuring those systems are secure. Commenters to both the *Alerting Modernization NPRM* and the *Alerting Security NPRM* broadly agree that it is vital to ensure the security of EAS and WEA.[45] Foreign adversaries, criminals,

(Continued from previous page)

[39] Sinclair Inc. Comments, PS Docket No. 25-224, at 1 (rec. Sept. 25, 2025) (Sinclair Alerting Modernization NPRM Comments).

[40] *See* CTIA Alerting Modernization NPRM Reply at 1-2, 29; Motorola Solutions, Inc. Reply, PS Docket No. 25-224, at 1 (rec. Nov. 18, 2025); SpectraRep, LLC Comments, PS Docket No. 25-224, at 1 (rec. Sept. 25, 2025).

[41] *See*, *e.g.*, CTIA Alerting Modernization NPRM Reply at 1; State Broadcasters Associations Reply, PS Docket No. 25-224, at 6-7 (rec. Nov. 18, 2025) (State Broadcasters Associations Alerting Modernization NPRM Reply).

[42] *See* NCTA—The Internet & Television Association Comments, PS Docket No. 25-224, at 3 (rec. Sep. 25, 2025) (NCTA Alerting Modernization NPRM Comments) (noting that the "EAS technology [was] first developed during the Cold War" and "EAS legacy system should be phased out"); Charles Helstein, Ryan Thompson, et al., Comments, PS Docket No. 25-224, at 1 (rec. Sept. 22, 2025).

[43] *See*, *e.g.*, Xperi Inc. Comments, PS Docket No. 25-224, at 3 (rec. Sept. 24, 2025) (Xperi Alerting Modernization NPRM Comments); State Broadcasters Associations Alerting Modernization NPRM Reply at 16.

[44] *See* NAB Alerting Modernization NPRM Comments at 2-3 (arguing that the legacy system "provides critical redundancy when the internet or cell service fail during large disasters."); APCO Alerting Modernization NPRM Reply at 11 (APCO suggests that the FCC "should continue to require support for EAS distribution over the legacy daisy-chain broadcast architecture as a backstop" because it provides "hardened transmission paths [to] over 90 percent of the US population and remain operable during disasters.").

[45] *See* NYCEM Alerting Modernization NPRM Comments at 5 ("NYCEM believes that the security of the nation's alerting systems is critical to maintaining its integrity and avoiding malicious uses."); Digital Alert Systems, Inc. Comments, PS Docket No. 25-224, at 47 (rec. Sept. 25, 2025) (DAS Alerting Modernization NPRM Comments) (DAS "supports the Commission's view that the nation's alerting systems must be secure against cyberattacks from our nation's adversaries. Maintaining trust in these systems is vital for both national security and achieving the nation's alerting goals."); NAB Alerting Modernization NPRM Comments at 16 ("[I]mproving cybersecurity of EAS is important to prevent an adversary from being able to issue a false alert or prevent a real alert from being broadcast."); Colorado Broadcasters Association Comments, PS Docket Nos. 15-94, 15-91, and 22-329, at 1 (rec. Dec. 22, 2022) (CBA Alerting Security NPRM Comments) (explaining that CBA "strongly supports improvements in both the readiness and security of EAS, which would advance the public interest that CBA's members also seek to serve"); National Public Radio, Inc. Reply, PS Docket Nos. 15-94, 15-91, and 22-329, at 4 (rec. Jan. 23, 2023) (NPR Alerting Security NPRM Reply) (explaining that, despite "concerns about the [Alerting Security] NPRM's specific proposals, commenters do agree that the EAS system should be supported and protected" and suggesting "ways EAS Participants, equipment manufacturers, and FCC staff can work together to strengthen EAS security"); Native Public Media Comments, PS Docket Nos. 15-94, 15-91, and 22-329, at 4 (rec. Dec. 23, 2022) (Native Public Media Alerting Security NPRM Comments) (noting that "[t]he integrity of the EAS system is ultimately an issue of national security"); Tim Comments, PS Docket Nos. 15-94, 15-91, and 22-329 (rec. Dec. 9, 2022) ("[T]he threat of cyber attacks will present a significant challenge that must be addressed in order to ensure that the system remains effective and reliable.").

and other bad actors can wreak havoc if they gain access to alerting systems, by sending a false alert that causes public panic or delivers false information about a disaster or crisis, or by preventing a real alert from being transmitted to the public. As one former broadcaster who submitted comments points out, the dissemination of false alerts can also undermine public trust in alerting capabilities, which depends on "ensuring that every message originates from an authorized and verifiable source."[46] Because of these risks, keeping these systems "secure against cyberattacks from our nation's adversaries" and "[m]aintaining trust in these systems is vital for both national security and achieving the nation's alerting goals."[47]

13. Today, we adopt three targeted measures that aim to ensure that EAS Participants secure their equipment to prevent cyberattacks that could result in the transmission of false EAS alerts or disrupt the transmission of legitimate alerts. Specifically, we require EAS Participants to do the following with respect to EAS equipment, studio transmitter link equipment, and any remotely managed equipment that routes, processes, or inserts content into the EAS Participant's programming stream: (1) prior to operation, change any default password, use strong passwords, and change any password if the EAS Participant has reason to believe that the password has been compromised; (2) test and install security patches and security-related software and firmware upgrades issued by equipment manufacturers promptly after those patches or upgrades become available; and (3) use a network firewall or comparable network segmentation practice to limit remote management access to authorized devices and authorized users.

14. These three requirements represent a subset of the six basic cybersecurity hygiene requirements that the Commission proposed to require EAS Participants to implement as part of their cybersecurity risk management plans in the *Alerting Security NPRM*.[48] In the *Alerting Security NPRM*, the Commission proposed to require EAS Participants to implement these cybersecurity measures in the context of their implementation of broader cybersecurity risk management plans.[49] The Commission sought comment on whether that approach "strik[es] the appropriate balance between improving EAS security, complementing EAS Participants' existing cybersecurity activities, and reducing burdens on small EAS Participants?"[50] In response, commenters express concern that compliance with precise cybersecurity risk management requirements would be costly,[51] could hinder their ability to adapt to changing cybersecurity needs,[52] and could subject them to strict liability enforcement in the event an EAS Participant is victimized by a cyberattack.[53] The approach we adopt today responds to those concerns by

[46] Jose Vergara Reply, PS Docket No. 25-224, at 1 (rec. Nov. 13, 2025) (Vergara Alerting Modernization NPRM Reply).

[47] DAS Comments at 47. *See also* Native Public Media Alerting Security NPRM Comments at 4 ("The integrity of the EAS system is ultimately an issue of national security.").

[48] *Alerting Security NPRM*, 37 FCC Rcd at 12945, para. 25 (proposing to require each plan include security measures that address (1) changing default passwords prior to operation; (2) installing security updates in a timely manner; (3) securing equipment behind properly configured firewalls or using other segmentation practices, (4) requiring multifactor authentication where applicable; (5) addressing the replacement of end-of life equipment; and (6) wiping, clearing, or encrypting user information before disposing of old devices).

[49] *Id.* at 12943, para. 23.

[50] *Id.* at 12945, para. 26.

[51] *See* CBA Alerting Security NPRM Comments at 7-8; National Television Association Comments, PS Docket Nos. 15-94, 15-91, and 22-329, at 5 (rec. Dec. 23, 2022) (NTA Alerting Security NPRM Comments) (describing the task of threat identification as "impossible for all but specialists in the field").

[52] *See* NTCA—The Rural Broadband Association Comments, PS Docket Nos. 15-94, 15-91, and 22-329, at 5 (rec. Dec. 23, 2022) (NTCA–The Rural Broadband Association Alerting Security NPRM Comments).

eliminating the broader cybersecurity risk management and threat assessment components of the proposed requirement, as well as the proposed requirements that EAS Participants employ "sufficient security controls to ensure the confidentiality, integrity, and availability of the EAS."[54]

15. The *Alerting Security NPRM* asked whether, "[i]nstead of requiring the use of a risk management plan, should [the Commission] require EAS Participants to take specific steps to secure their EAS equipment?" In addition, the *Alerting Modernization NPRM* asked if there are "specific authentication, validation, and security measures that EAS and WEA should be designed to incorporate?"[55] In response to the *Alerting Modernization NPRM*, APCO and other commenters agree that the Commission should adopt specific security requirements for EAS Participants.[56] As with other commenters to the *Alerting Security NPRM*, National Public Radio (NPR) is concerned about the costs of cybersecurity risk management plan requirements and asks that EAS Participants be required to, instead, only implement the basic security measures that the Commission proposed without requiring the creation of broader risk management plans.[57] REC Networks agrees that "security of EAS equipment is of paramount importance" but asks that smaller EAS Participants be required to "implement a simpler plan of good network operating practices, which involve network configuration, password management and protection, periodic password changes[,] and other 'common sense' methods to assure that EAS equipment is not compromised."[58] The approach we adopt today is consistent with NPR's view that we should require EAS Participants to implement minimum security controls, rather than comprehensive risk management plans, while also respecting REC Networks' view that some of the specific security measures we proposed to require, such as addressing the replacement of end-of-life equipment and wiping, clearing, or encrypting user information before disposing of old devices, may be more complicated than is appropriate to require of some EAS Participants. Other commenters, such as NCTA, express concern that requiring EAS Participants to implement a specific cybersecurity framework would "freeze cybersecurity practices in time and hamper an EAS Participant's ability to develop and implement cybersecurity measures in response to its specific cybersecurity risk profile, to the detriment of public safety."[59] The requirements we adopt today will not hamper an EAS Participant's ability to respond to evolving cybersecurity threats. Rather, they represent a minimum acceptable baseline that will harden critical communications infrastructure against today's threats, while being flexible enough to adapt to changes in the threat environment.[60]

(Continued from previous page)

[53] *See* CBA Alerting Security NPRM Comments at 9.

[54] *Alerting Security NPRM*, 37 FCC Rcd at 12957, Appx. A.

[55] *Alerting Modernization NPRM*, 40 FCC Rcd at 6701, para. 15.

[56] *See* APCO Alerting Modernization NPRM Reply at 10-11; Jonah Kibin Comments, PS Docket No. 25-224, at 1 (rec. Sep. 29, 2025) (Kibin Alerting Modernization NPRM Comments).

[57] National Public Radio Comments, PS Docket Nos. 15-94, 15-91, and 22-329, at 7-8 (rec. Dec. 23, 2022) (NPR Alerting Security NPRM Comments); CrowdStrike Comments, PS Docket Nos. 15-94, 15-91, and 22-329, at 3 (Dec. 23, 2022) (agreeing that the Commission should adopt specific cybersecurity requirements but specifying control frameworks more advanced than those we adopt today).

[58] REC Networks Comments, PS Docket Nos. 15-94, 15-91, and 22-329, at 2 (rec. Dec. 22, 2022) (REC Networks Alerting Security NPRM Comments); *see also id*. at 16-18 (providing an example of a simplified set of cybersecurity requirements).

[59] NCTA Alerting Security NPRM Comments at 5.

[60] *See* Gray Television Reply, PS Docket Nos. 15-94, 15-91, and 22-329, at 4 (rec. Jan. 23, 2023) (Gray Television Alerting Security NPRM Reply) (citing NIST for the premise that organizations must have the flexibility to "determine activities that are important to critical service delivery and can prioritize investments to maximize the impact of each dollar spent"); CBA Alerting Security NPRM Comments at 7 ("[T]he FCC should take a flexible approach regarding EAS Participants' cybersecurity protocols. . . . EAS participants have stations of varying sizes,

(continued….)

16. The cybersecurity requirements we adopt today are narrowly tailored to address vulnerabilities that have been repeatedly exploited through a series of cyberattacks on EAS Participants in recent months. In these attacks, bad actors gained control of radio broadcasters' systems by exploiting improperly secured, remotely accessible equipment in the broadcast signal processing system to transmit unauthorized audio that included EAS alert tones, an offensive song that included racial slurs, and promotional content.[61] In response to the attacks, the Public Safety and Homeland Security Bureau (Bureau) released a Public Notice on November 23, 2025, urging broadcasters to immediately implement basic cybersecurity hygiene best practices to secure their systems and protect EAS, including installing software security patches for broadcast equipment issued by the manufacturer as soon as they become available; upgrading equipment firmware and software to the most recent versions recommended by the manufacturer; changing devices' default passwords and replacing them with robust alternatives; regularly changing passwords to promote continued security; and, where reasonably feasible, installing EAS, studio-transmitter link equipment, and other equipment interconnected to the broadcast signal processing system behind network firewalls.[62] Similar attacks on broadcasters going back more than a decade have included hoax radio broadcasts about a zombie attack[63] and false alerts about a "radiological hazard" sent to cable subscribers through the infiltration of EAS equipment connected to the Internet.[64] The Bureau recently convened a cybersecurity workshop for broadcasters that brought together public and private sector representatives to raise awareness of emerging cybersecurity risks, share and promote the adoption of best practices, and highlight opportunities for public-private partnerships on cybersecurity issues facing broadcasters.[65] Despite our repeated efforts urging EAS Participants to take basic steps to secure their

(Continued from previous page)
with varying levels of sophistication and complexity of their broadcasting systems and equipment."); New York State Division of Homeland Security and Emergency Services Comments, PS Docket No. 25-224 at 3 (rec. Sept. 25, 2025) (NY DHSES Alerting Modernization NPRM Comments) (" . . . [C]ybersecurity can be a fast-evolving threat area, it is important than [*sic*] the systems, technologies, and implementations used in the nation's alerting systems are nimble enough for rapid mitigation of vulnerabilities, including both perceived and actual threats."). Commenters addressing cybersecurity response to the *Alerting Modernization NPRM* address it primarily in the context of the need for authentication for EAS, which we address in the *FNPRM* below.

[61] *See Public Safety and Homeland Security Bureau Reminds Broadcasters to Ensure They Comply With Best Practices to Prevent Cyberattacks*, Public Notice, DA 25-996 (PSHSB 2025), https://docs.fcc.gov/public/attachments/DA-25-996A1.pdf (*PSHSB Reminds Broadcasters of Cybersecurity Best Practices*); *see also*, *e.g.*, Lance Venta, *ESPN 97.5 Houston Victim of Barix Hack* (Nov. 23, 2025), https://radioinsight.com/headlines/321936/espn-97-5-houston-victim-of-barix-hack/; Katelyn Harlow, *NPR affiliate's backup audio signal hacked, 'offensive material' broadcast in Richmond* (Nov. 21, 2025), https://www.wric.com/news/local-news/npr-affiliates-backup-audio-signal-hacked-offensive-material-broadcast-in-richmond-area/; *Apparent Barix Hacks Highlight Gaps in Cybersecurity, This is not the first time hijackers have attacked Barix boxes to stream explicit content*, Elle Kehres (Sept. 10, 2025), https://www.radioworld.com/news-and-business/apparent-barix-hacks-highlight-poor-cybersecurity-practices.

[62] *PSHSB Reminds Broadcasters of Cybersecurity Best Practices*.

[63] *See* Michael Beall, *Police Say Mont. TV Zombie Attacks Likely Linked to Others* (Feb. 13, 2013), http://www.usatoday.com/story/news/nation/2013/02/13/police-believe-zombie-hoax-attacks-linked/1915921; *see also* Susan Ashworth, *Station Hacks Put Focus on Passwords, Security Vulnerabilities* (Apr. 11, 2016), https://www.radioworld.com/news-and-business/station-hacks-put-focus-on-passwords-security-vulnerabilities (explaining that studio transmitter link equipment manufacturer Barix had instructed customers to set new passwords and ensure devices were protected by firewalls in response to incidents in which attackers hijacked broadcast audio streams and transmitted sexually explicit content).

[64] *See* Peninsula Daily News, *False Emergency Alerts Sent to Jefferson County Cable Users*, https://www.peninsuladailynews.com/news/false-emergency-alerts-sent-to-jefferson-county-cable-users/ (last visited Apr. 24, 2026); KOMO News, *Viewers Sent Apparent Hacked Emergency Broadcast Message in Jefferson County*, https://komonews.com/news/local/viewers-sent-apparent-hacked-emergency-broadcast-message-in-jefferson-county (last visited Apr. 24, 2026).

networks, including the November 2025 Public Notice, an August 2022 Public Notice recommending similar steps to those we recommended last year,[66] and an April 2020 email to EAS Participants encouraging them to secure their EAS equipment by installing current security patches,[67] successful attacks have continued into 2026.

17. Because some EAS Participants have not taken adequate steps to remediate these vulnerabilities and address the significant risk posed by a false alert or non-transmission of a real alert, we find that each of the three requirements we adopt today are necessary to protect the security and integrity of EAS.

18. *Password requirements.* Strong password security is essential to protecting EAS equipment, studio-transmitter link equipment, and remotely accessible equipment from unauthorized access that exploits weak or default credentials. Digital Alert Systems, Inc. (DAS) and former broadcaster, Jonah Kibin, caution against using default passwords and recommend changing required credentials upon setup as default passwords, particularly on encoders, "are widely available on the internet and have led to high-profile intrusions of the EAS in the last couple of decades."[68] We require that default passwords for EAS equipment, studio transmitter link equipment, and any remotely managed equipment that routes, processes, or inserts content into the EAS Participant's programming stream be changed prior to any use to broadcast to the public. Passwords used for this equipment must employ a minimum of 15 characters, not use dictionary words (because they can be cracked through brute force), and not be reused for other accounts, equipment, applications, and services that the EAS Participant uses.

19. As an alternative to a strong password, we permit EAS Participants to use alternative authentication measures that are reasonably sufficient to mitigate the risk of unauthorized access. We believe that there are numerous authentication methods available to EAS Participants that would be reasonably sufficient, including methods that have been highlighted by the National Institute of Standards and Technology (NIST) as meeting one of three authentication assurance levels.[69] For example, NIST's guidance provides that authentication properly implemented at Authentication Assurance Level 1 can include, in addition to passwords, look-up secrets, which are "[a] secret determined by the claimant by looking up a prompted value in a list held by the subscriber"; out-of-band devices, consisting of "[a] secret sent or received through a separate communication channel with the subscriber"; single- or multi-factor one-time password devices, in which a one-time secret is obtained from a device or application held by the subscriber, which may or may not require activation by a second authentication factor; and

(Continued from previous page)

[65] *Public Safety And Homeland Security Bureau to Host a Cybersecurity Workshop for Broadcasters on May 14, 2026*, Public Notice, DA 26-334 (PSHSB April 7, 2026); *Cybersecurity Workshop for Broadcasters*, https://www.fcc.gov/news-events/events/2026/05/cybersecurity-workshop-broadcasters [https://perma.cc/3275-DZT2].

[66] *Public Safety and Homeland Security Bureau Urges Emergency Alert System (EAS) Participants to Take Immediate Steps to Secure EAS Equipment*, PS Docket No. 15-94, Public Notice, 37 FCC Rcd 9334 (2022) (*PSHSB Urges EAS Participants to Secure Equipment*); *see also* FCC, *Alerting Security Roundtable* (Oct. 30, 2023), https://www.fcc.gov/news-events/events/2023/10/alerting-security-roundtable; FEMA, IPAWS Advisory: Emergency Alert System Vulnerability (Aug. 1, 2022), https://content.govdelivery.com/accounts/USDHSFEMA/bulletins/3263326 (advisory noting potential vulnerability in certain EAS encoder/decoder devices that have not been updated to most recent software versions and warning of the risk of false alert issuance if devices are not updated).

[67] E-mail from Lisa M. Fowlkes, Chief, PSHSB, FCC to EAS Participants (April 24, 2020 2:03 am EDT).

[68] Kibin Alerting Modernization NPRM Comments; *see also* DAS Alerting Modernization NPRM Comments at 48, 57-58.

[69] *See* NIST, Digital Identity Guidelines: Authentication and Authenticator Management, Special Publication 800-63B-4 (2025) (NIST SP800-63B), https://csrc.nist.gov/pubs/sp/800/63/b/4/final.

single- or multi-factor cryptographic authentication, which entails "[p]roof of possession and control via an authentication protocol of a cryptographic key held by the subscriber," which may or may not require activation by a second authentication factor.[70] We recognize that, were we to simply require use of specifically structured passwords, our rule could preclude the use of other authentication methods offering equal or better security. To ensure our requirements do not result in reducing the security of currently secure systems,[71] the rule we adopt today continues to allow EAS Participants to secure their equipment through means that are equally or more secure than the password requirements we adopt today.

20. As DAS observes, "systemic risks" are created when EAS Participants use "[w]eak passwords [and] shared accounts."[72] These risks are present throughout the industry. As the National Television Association concedes, many EAS Participants "had never changed the default password on their EAS device(s)."[73] A former broadcaster further emphasizes that the use of default passwords to widely owned broadcast equipment—many of which are publicly available—has contributed to multiple high□profile intrusions over the past decade, demonstrating that these risks are neither hypothetical nor isolated.[74] NPR characterizes requirements to change default passwords and secure equipment as reasonable and sound.[75] Prometheus Radio Project supports Low Power FM stations "maintaining a firewall, following password management best practices, and implementing multi-factor authentication."[76] REC Networks supports the immediate changing of default passwords, and includes this as one of the recommendations in its *Practice of Good Network Security for Small Stations*.[77] This requirement aligns with authoritative, industry-recognized cybersecurity standards, including the Cybersecurity & Infrastructure Security Agency's (CISA) Cross-Sector Cybersecurity Performance Goals (CPGs), which are designed for operators of critical infrastructure such as communications networks.[78]

---

[70] NIST SP800-63B at 5.

[71] *See* NCTA—The Internet & Television Association Comments, PS Docket Nos. 15-94, 15-91, and 22-329, at 4 (rec. Dec. 23, 2022) (NCTA Alerting Security NPRM Comments) (requesting that, if the Commission adopts cybersecurity risk management plan requirements, it give EAS Participants flexibility to structure their plans in a manner tailored to their organization); Gray Television Alerting Security NPRM Reply at 4 (arguing that specific requirements for EAS cybersecurity plans would divert the resources of EAS Participants that already have comprehensive cybersecurity plans to ensuring that the plan satisfies the Commission's requirements even though the practices themselves already meet or exceed expectations).

[72] DAS Alerting Modernization NPRM Comments at 48.

[73] NTA Alerting Security NPRM Comments at 6.

[74] *See* Kibin Alerting Modernization NPRM Comments at 1 (urging the Commission to "[r]equire EAS participants change the default password on their encoders [because] these default passwords are widely available on the internet and have led to high-profile intrusions of the EAS in the last couple decades.").

[75] NPR Alerting Security NPRM Comments at 7.

[76] Prometheus Radio Project Comments, PS Docket Nos. 15-94, 15-91, and 22-329, at 3 (rec. Dec. 26, 2022) (Prometheus Alerting Security NPRM Comments).

[77] REC Networks Alerting Security NPRM Comments at 33.

[78] Cybersecurity & Infrastructure Security Agency, *Cross-Sector Cybersecurity Performance Goals and Objectives*, https://www.cisa.gov/cpgs (last visited Apr. 26, 2026). We have elsewhere pointed to the CISA CPGs as an instructive suite of cybersecurity best practices for communications service providers. Today's *Submarine Cable Second Report and Order* adopts certain national security standards that, if met, will presumptively exempt a submarine cable application from referral to the Executive Branch agencies, including that the applicant must affirm, as part of its required cybersecurity and physical security risk management plan certification, that the plan meets a set of established cybersecurity best practices such as the standards and controls set forth in the CISA CPGs. *Review of Submarine Cable Landing License Rules and Procedures to Assess Evolving National Security, Law Enforcement, Foreign Policy, and Trade Policy Risks; Amendment of the Schedule of Application Fees Set Forth in Sections 1.1102*
(continued….)

Specifically, CISA CPG 3.A, "Changing Default Passwords," encourages companies to address the risk that "[a]dversaries might acquire and exploit default account credentials to gain initial access, maintain persistence, escalate privileges, or evade defenses" by "[i]mplement[ing] an organization-wide policy that requires changing default manufacturer passwords for all hardware, software, and firmware before connecting them to any internal or external network."[79] We disagree with NCTA's suggestion that cybersecurity protections should be limited to EAS equipment alone,[80] as this would be insufficient to protect EAS when unprotected studio transmitter link equipment and remotely managed equipment that routes, processes, or inserts content into the EAS Participant's programming stream create similar opportunities to transmit false alerts or disrupt the transmission of real alerts. The password characteristics that we require reflect the CISA and NIST guidance on minimum password strength and unique credentials.[81] We expect compliance with the requirement to be straightforward for EAS Participants, which need only log into each relevant piece of equipment, locate the account-management or security settings, and replace the factory-set default password or existing weak password with a strong, unique password—a process that should be repeated whenever the EAS Participant has reason to believe that the password has been compromised.

21. *Firmware and Software Patching.* Prompt firmware and software patching are key to reducing the risk that bad actors will exploit known vulnerabilities to infiltrate broadcast and cable systems to insert false EAS tones or alerts. The record includes support for requiring EAS Participants to promptly install security patches and firmware and software updates. DAS also points to the failure to apply software updates as a "systemic risk[]" to EAS.[82] One comment submitted by a radio broadcast engineer recommends that the Commission require EAS equipment to automatically query a centralized database to confirm EAS codec firmware and certificate updates.[83] APCO opines that "[t]he Commission should consider rules requiring EAS and WEA participants to maintain current software and replace outdated equipment in a timely manner," citing findings from the Commission's 2023 Nationwide Emergency Alert Test showing that "approximately 23 percent of the EAS equipment units were either using outdated software or operating equipment that was no longer supported with regular software updates."[84] The fact that nearly a quarter of EAS devices may potentially be exposed to known, readily addressed vulnerabilities because they are operating obsolete or out-of-date equipment represents a

(Continued from previous page)
through 1.1109 of the Commission's Rules, OI Docket No. 24-523, MD Docket No. 24-524, Second Report and Order and Second Further Notice of Proposed Rulemaking, FCC 26-42 at 90-91, para. 170 (2026).

[79] CISA, Cross-Sector Cybersecurity Performance Goals Version 2.0 at 18 (2025), https://www.cisa.gov/sites/default/files/2025-12/CPG_Report_2.0_508c.pdf.

[80] Letter from Radhika Bhat, Vice President and Assistant General Counsel, NCTA—The Internet & Television Association, to Marlene H. Dortch, Secretary, FCC, PS Docket No. 15-94 at 2 (filed Aug. 9, 2024).

[81] *See* CISA, *Cross-Sector Cybersecurity Performance Goals Checklist Version 1.0.1*, https://www.cisa.gov/sites/default/files/2023-03/cisa_cpg_checklist_v1.0.1_final.pdf (last visited Apr. 29, 2026). *See also* NIST, Digital Identity Guidelines Special Pub. 800-63B (2025), https://pages.nist.gov/800-63-4/sp800-63b.html at 3.1.1; NIST, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations Special Pub. 800-171 (2024), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r3.pdf; *see also* Center for Internet Security (CIS), CIS Critical Security Controls v8.1 (2025), https://learn.cisecurity.org/cis-controls-v8-1-guide-pdf; CIS, CIS Password Policy Guide (2020), https://www.cisecurity.org/insights/white-papers/cis-password-policy-guide.

[82] DAS Alerting Modernization NPRM Comments at 48.

[83] Aaron Read Reply, PS Docket Nos. 15-94, 15-91, 22-329 at 2 (rec. Dec. 29, 2022).

[84] APCO Alerting Modernization NPRM Reply at 10 (citing Public Safety and Homeland Security Bureau, Report: October 4, 2023 Nationwide Emergency Alert Test, at 14 (2024), https://docs.fcc.gov/public/attachments/DOC-403500A1.pdf).

significant gap in the security of the nation's alerting capacity that poses national security risks. Promptly testing and installing security patches and software and firmware upgrades will also address DAS's concern that "[g]ray-market EAS encoders/decoders (i.e., used equipment sold on auction websites) can ship with outdated firmware and unremoved configurations or credentials, allowing attackers to exploit known vulnerabilities or use retained settings to impersonate sources and inject false alerts."[85] Going forward, EAS Participants will be responsible for ensuring that their EAS devices are properly patched and updated, regardless of the devices' provenance. The requirement to install patches and update software promptly also aligns with CISA's CPGs. Specifically, CISA CPG 2.B encourages companies to "Mitigate Known Vulnerabilities" by "[i]mplement[ing] a vulnerability management program to patch and mitigate misconfigured software in a timely manner" to protect against the risk that "[a]dversaries frequently target unpatched and misconfigured systems, particularly those exposed to the internet," and "often leverage software vulnerabilities, temporary malfunctions, or configuration errors to gain initial access to a network."[86] Here, too, we expect implementation to be simple. Once a security patch, or security-related software or firmware upgrade, becomes available for EAS equipment, studio transmitter link equipment, or any other remotely managed equipment that routes, processes, or inserts content into the EAS Participant's programming, EAS Participants must promptly download and install the patch or upgrade. EAS Participants are permitted to test that patch or upgrade to ensure that it does not introduce performance issues, provided that the testing begins promptly and is completed in a timeframe that is consistent with industry best practices. No commenter specifically opposes prompt patching as a security requirement.

22. *Use of a Firewall or Comparable Network Segmentation.* We require EAS Participants to use a network firewall or comparable network segmentation practices to limit remote management access to authorized devices and authorized users, which will secure EAS and other vulnerable equipment on a private network inaccessible to the public Internet. This requirement addresses a widespread EAS vulnerability. In response to the *Alerting Security NPRM*, REC Networks identified 730 EAS Participant servers through which the password screen for Sage Alerting Systems' ENDEC EAS device was directly exposed.[87] Of those servers, 288 operated on port 80, which is the default port for HTTP web services.[88] It is thus easy and cheap for even low-capability malicious actors to locate EAS Participant equipment. To comply with the requirement we adopt today, EAS Participants must ensure that their EAS equipment is secured behind a firewall or other segmentation mechanism—such as a dedicated Virtual Local Area Network (VLAN), demilitarized zone, or physically isolated management network—with access restricted to only those internal systems and ports necessary for EAS operations.[89] EAS Participants must either deploy a hardware or software firewall with appropriate filters, reconfigure existing routers to block

[85] DAS Alerting Modernization NPRM Comments at 48.

[86] CISA, *Cybersecurity Performance Goals 2.0*, https://www.cisa.gov/cybersecurity-performance-goals-2-0-cpg-2-0 (last visited Apr. 28, 2026); *see also* NIST, SP 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations at 333 (2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf; Center for Internet Security (CIS), CIS Critical Security Controls v8.1 (2025), https://learn.cisecurity.org/cis-controls-v8-1-guide-pdf (recommending automated patch management on a monthly or more frequent basis in CIS safeguards 7.3 and 7.4).

[87] REC Networks Alerting Security NPRM Comments at 14-15 ("This exposure is of concern to REC and should be a concern to the Commission as it means that without having to 'sniff' for the right port, anyone can reach the password screen for these EAS decoders simply by using the IP address.").

[88] *Id.* In contrast with the servers operating on port 80, web services that use the more secure transport layer security (HTTPS) use port 443.

[89] *See DAS Alerting Modernization NPRM Comments* at 57 (recommending isolating EAS devices from business and corporate IT networks by placing the devices behind firewalls or in demilitarized zones with least-privilege access rules).

inbound public internet connectivity to EAS devices, or otherwise isolate EAS equipment from general purpose business networks so that unauthorized external access is not possible.[90] These measures constitute essential, straightforward safeguards that EAS Participants of all sizes can realistically implement.[91] As with the other two requirements we impose, this network segmentation requirement is consistent with established cybersecurity best practices. For example, CISA CPG 3.S calls on companies to "Secure Internet Facing Devices" by "[m]inimiz[ing] internet-facing assets whenever possible" to address the risk that "[a]dversaries might exploit weaknesses in internet-facing hosts or systems to gain initial network access, targeting software bugs, temporary glitches, or misconfigurations," and CISA CPG 3.I recommends that networks should be logically segmented.[92] No commenter specifically opposes network segmentation as a security requirement.

23. Based on commenters' assertions that EAS Participants already implement cybersecurity risk management plans, we suspect that many EAS Participants already implement the baseline cybersecurity requirements we adopt today.[93] But EAS is only as secure as its weakest link. Not only does the hack of even a single EAS Participant's systems potentially expose that entity's audience to false information about an emergency, but also the architecture of legacy EAS means that certain types of EAS Participants could pass a false alert along to other EAS Participants. As DAS explains, "Commission rules can help ensure consistent implementation [of security requirements] across thousands of EAS Participants, preventing weakest-link vulnerabilities."[94] As REC Networks notes, small broadcasters are especially likely not to have implemented basic cybersecurity practices, and would benefit from straightforward and easily implemented rules rather than "an extensive and elaborate cybersecurity plan" requirement, as proposed in the *Alerting Security NPRM*.[95] We accordingly find that the requirements we adopt today are particularly important to protect EAS Participants that are small- and medium-sized businesses.[96] We therefore reject comments that suggest smaller EAS Participants should be exempt from cybersecurity requirements. Native Public Media and other commenters state that small stations typically lack the budget, resources, and expertise to manage IT security responsibilities, noting that many EAS Participants are very small, and are often nonprofit or municipal operations with minimal funding.[97] But

[90] *See* CSRIC VI, Final Report—Security Aspects of Emergency Alerting System (EAS) at 27, 33-34 (2018), https://www.fcc.gov/file/14853/download (CSRIC VI EAS Security Report).

[91] *See id*.

[92] CISA, *Cybersecurity Performance Goals 2.0*, https://www.cisa.gov/cybersecurity-performance-goals-2-0-cpg-2-0 (last visited Apr. 20, 2026). Similarly, CSF Protect element PR.IR-01 protecting from unauthorized logical access and usage implementation example #2 states that only necessary communications should be allowed to enter an organization's network from external networks which should be logically segmented. *Id.*

[93] *See* NCTA Alerting Security NPRM Comments at 4 ("NCTA's members already develop and implement extensive cybersecurity best practices and risk management plans in the normal course of business, including with respect to their participation in EAS"); Gray Television Alerting Security NPRM Reply at 4.

[94] DAS Alerting Modernization NPRM Comments at 49.

[95] REC Networks Comments, PS Docket No. 25-224, at 7 (rec. Sept. 25, 2025) (REC Networks Alerting Modernization NPRM Comments) ("[REC] feel[s] that the overall security policy of EAS is really good[,] [but] [t]he major problem . . . is following good security practices on the station end. We see a lot of this in small stations, especially those who have a remotely located transmitter. . . . Stations need to be responsible and accountable, even if means not making their network visible from the outside.").

[96] *See* Aaron Read Reply, PS Docket Nos. 15-94, 15-91, and 22-329, at 1 (rec. Dec. 29, 2022) (Read Alerting Security NPRM Comments) (stating that "the problem is not that broadcast station owners are aware of the risks of network security and are attempting to comply but, for whatever reason, are failing to do so. The problem is that station owners either aren't aware of the risks at all, or - equally likely - they simply do not care; gambling that the FCC will never actually enforce any rules against them.").

that concern cuts both ways. Smaller broadcasters with fewer security protections in place are often a more attractive target for bad actors, as the recent attacks on small radio broadcasters demonstrate.[98] Moreover, while having limited resources might have made it burdensome to adopt the far-reaching cybersecurity risk management requirements imposed in the *Alerting Security NPRM*, the minimal requirements we adopt today will be far easier and less resource-intensive to implement. We further disagree with Cox Media Group and NAB that the Commission should focus on education of EAS Participants to secure the nation's public alert and warning capability.[99] While we recognize the value of education, we find that it is not sufficient, on its own, to effectively reduce the dynamic and evolving risks posed by cybersecurity threats to emergency alert systems. We conclude that all EAS Participants can and must implement the cybersecurity safeguards we adopt today.

24. While we appreciate DAS's view that EAS equipment manufacturers should be expected to implement security practices in their equipment, including by following secure coding practices, providing digitally signed software and firmware updates, shipping devices with hardened default settings, and supporting role-based access controls,[100] we find that the primary responsibility for securing vulnerable equipment rests with EAS Participants themselves. The vulnerabilities identified in the record stem mainly from insecure password practices, unpatched EAS participant□managed systems, inadequate network segmentation, or exposure of devices to the open Internet—not from defects in underlying equipment design and development. This approach to responsibility for EAS security delineates clear roles. Manufacturers develop, validate, and make available security patches. EAS Participants, in turn, are responsible for applying patches to their equipment, and ensuring their systems are updated.

25. We disagree with NAB that, rather than imposing uniform requirements for EAS Participants to secure their systems, the Commission should engage in targeted outreach to those EAS Participants found to be using outdated software or unsupported equipment.[101] We similarly disagree

(Continued from previous page)

[97] Native Public Media Alerting Security NPRM Comments at 2 ("NPM station members have neither the resources, nor the expertise to shoulder that responsibility properly."); NTA Alerting Security NPRM Comments at 2 ("[T]he that vast majority of EAS Participants are very small operations, operated by nonprofits-municipalities, religions entities, and other similar groups, often on shoestring budgets."); Read Alerting Security NPRM Comments at 1 ("[M]any small stations have near zero budget for any actual I.T. security support."); *see also* NAB Alerting Security NPRM Comments at 21 (discussing the CSRIC IV's findings that the "cost of needed upgrades, security issues and the time it takes to fix problems may pose additional financial and resource challenges for smaller and rural EAS Participants. . . ." (citing CSRIC IV, EAS Security Final Report (2015), https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG3-EAS_SECURITY_FINAL_011316.pdf)).

[98] *See* Kathryn Basinsky, NTIA, Telecommunications Policy Specialist, Alerting Security Roundtable, 1:21:25 (Oct. 30, 2023), https://www.fcc.gov/news-events/events/2023/10/alerting-security-roundtable ("When we were starting out a few years ago, we would hear from these entities that, 'Well, we are so small, we are not a target, we don't need to do the same work these larger tier one suppliers are having to do.' Unfortunately, I don't hear that as frequently because they are being targeted. Either they themselves have experienced an attack, they have seen their competitors and colleagues experience an attack, or they stay on top of the news and have started to see the wave of bankruptcies and fallout from ransomware incidents, among other cyber-attacks. They now have this understanding that they are a target, that they need to take the steps to defend themselves . . . .").

[99] Cox Media Group Reply Comments, PS Docket Nos. 15-94, 15-91, and 22-329, at 2 (rec. Jan. 23, 2023); NAB Alerting Security NPRM Comments at 4 (recommending that the Commission "implement the recommendations of the Communications Security, Reliability, and Interoperability Council (CSRIC) to focus on aiding the most vulnerable subsets of EAS Participants, such as small and medium-sized broadcasters").

[100] DAS Alerting Modernization NPRM Comments at 49-50.

[101] NAB Alerting Security NPRM Comments at 21 (contending that "if the Commission has data showing that some EAS Participants were using outdated software or equipment during that [2021 Nationwide EAS Test] test, the

(continued….)

with security researcher Shawn Merdinger, who suggests that "[w]hat is needed is direct outreach. . . . Someone at the FCC who identifies the EAS device . . . , finds out who the asset owner is, and reaches out to the person running, or in charge of running, that EAS device."[102] We recognize the value of outreach to EAS Participants to identify ways to better secure their systems, and take a variety of actions to promote public-private partnership and voluntary efforts to protect networks and EAS from cybersecurity threats. These include releasing Public Notices warning about recent threat vectors and providing guidance about how EAS Participants can better secure their equipment against such threats;[103] hosting workshops that raise situational awareness of the threat landscape and share best practices for protecting communications networks and incident response;[104] and investigating reports about false EAS alerts that suggest the breach of an EAS device or willful misuse of the EAS tones or Attention Signal.[105] Despite these efforts, cyberattacks on EAS Participant facilities continue to occur with disturbing frequency.[106] It is neither practical, administratively efficient, nor a reasonable use of public funds, for the Commission to respond to these threats by assessing the security status of equipment operated by thousands of EAS Participants across the United States and working with each such participant individually to implement the cybersecurity practices that we have been urging them to adopt for years. Moreover, there is no guarantee that the Commission will be able to identify every EAS Participant whose systems may be vulnerable because of flawed passwords, patching, or network segmentation practices. The far more efficient approach is to impose a minimally burdensome requirement on each EAS Participant to implement the basic security requirements we adopt today for its own equipment.

26. We also disagree with commenters like NCTA that recommend the Commission first focus on modernizing EAS technology prior to considering any additional or updated cybersecurity or resiliency requirements.[107] Maintaining strong passwords, routinely installing security upgrades, and segmenting sensitive equipment from the public Internet are vital to preventing unauthorized access to EAS encoding and decoding functions and unauthorized transmission of EAS header tones and audio messages, irrespective of where in the EAS Participant's signal processing system those functions and transmission may be activated. We decline to wait additional months to secure these systems against cybersecurity vulnerabilities that are actively being exploited.

27. We do not apply the targeted cybersecurity requirements we adopt today to WEA at this time. As discussed above, there is a long history of attackers exploiting vulnerabilities in EAS Participants that have resulted in false EAS alerts reaching the public. While a 2016 report on WEA's

(Continued from previous page)
Commission could reach out and educate these entities, instead of subjecting the entire universe of 27,000+ EAS Participants to difficult, expensive new requirements.").

[102] Shawn Merdinger Reply, PS Docket Nos. 15-94, 15-91, and 22-329, at 2 (rec. Dec. 25, 2022).

[103] *See*, *e.g.*, *Public Safety and Homeland Security Bureau Highlights Best Practices for Defending Against Ransomware Attacks*, Public Notice, DA 26-96, 2026 WL 297782 (PSHSB 2026); *PSHSB Reminds Broadcasters Cybersecurity Best Practices*; *PSHSB Urges EAS Participants to Secure Equipment*.

[104] *See, e.g.*, FCC, *Cybersecurity Workshop for Broadcasters*, https://www.fcc.gov/news-events/events/2026/05/cybersecurity-workshop-broadcasters [https://perma.cc/3275-DZT2] (last visited May 29, 2026); FCC, *Cybersecurity Workshop for Telecommunications Carriers*, https://www.fcc.gov/news-events/events/2026/05/cybersecurity-workshop-telecommunications-carriers [https://perma.cc/T9LU-JT5B] (last visited May 29, 2026).

[105] *See* 47 CFR § 11.45(b), (c).

[106] *See*, *e.g.*, *PSHSB Reminds Broadcasters of Cybersecurity Best Practices*.

[107] NCTA Alerting Modernization NPRM Comments at 6 (encouraging the Commission "to focus first on modernizing the EAS technology and framework before considering any additional cybersecurity or resiliency requirements").

security found risks of blocking valid WEA messages, changing the content of a valid WEA message, injecting false WEA alerts into operator equipment, and sending false alerts from false base stations, there have been no reported instances of those kinds of attacks on WEA being successful.[108] We find this to be evidence, as CTIA and ATIS assert, that additional security requirements are not needed at this time.[109] Consistent with the overarching recommendation of CSRIC V, we find that that best practices, rather than requirements, are currently suitable for addressing cybersecurity threats to WEA.[110] Three alerting authorities and two individuals generally support improvements to WEA's cybersecurity posture, but focus on end-to-end cryptographic authentication, auditing, and other more burdensome security measures.[111] None of these commenters adequately explain how the security benefits of additional WEA requirements would outweigh the costs, particularly when the lack of successful attacks on WEA suggests that the benefits of adding security measures for WEA may currently be limited.

C. Compliance Timeframe

28. We adopt a compliance timeframe for the rule changes adopted in this *Order* of 60 days after the rule's publication in the *Federal Register*, balancing the need to quickly secure vulnerable equipment against known vulnerabilities with the time EAS Participants require to implement the security controls. We find that sixty days provides sufficient time for compliance with these changes. Many EAS Participants and their representative organizations state that EAS Participants have already implemented cybersecurity risk management plans that include these specific security measures,[112] and the Commission and FEMA have repeatedly raised the security of EAS as an urgent priority.[113] EAS Participants that have not already implemented these basic cybersecurity hygiene measures will need only make a handful of straightforward changes to certain equipment to comply with these requirements. Minimal time is required, for instance, to log into the equipment subject to these requirements—which, for many EAS Participants is likely to comprise only a few devices—and change the passwords. Indeed, most Americans routinely manage passwords to a variety of devices and applications as a matter of course, which consumes no more than a few minutes each week. Similarly, it will take little time for most EAS Participants to test and install any currently available patches and updates for equipment subject to the requirement. As DAS explains, installing patches and updating equipment to the latest software version is minimally burdensome, because over-the-air software updates and software patching are both feasible

[108] CSRIC V, Final Report – WEA Security (2016), https://transition.fcc.gov/bureaus/pshs/advisory/csric5/WG2_WEA-Sec-Sub_FinalReport_0316.docx (CSRIC V WEA Security Report).

[109] *See* CTIA Comments, PS Docket No. 15-94, 15-91, and 22-329, at 21-22 (rec. Dec. 23, 2022) (CTIA Alerting Security NPRM Comments) ("WEA is a broadcast transmission conveyed by the cellular network to the device using the message that comes from the FEMA-administered Integrated Public Alert & Warning System ("IPAWS") and the alert originator. This system is simple, secure, and has proven to work very effectively."); Alliance for Telecommunications Industry Solutions Comments, PS Docket Nos. 15-94, 15-91, and 22-329 (rec. Dec. 23, 2022), at 17 (ATIS Alerting Security Comments).

[110] *See* CSRIC V WEA Security Report.

[111] *See* Jessica Lavrov Comments, PS Docket No. 15-94, 15-91, and 22-329, at 1 (rec. Nov. 13, 2025) (Lavrov Alerting Modernization NPRM Reply); Vergara Alerting Modernization NPRM Comments at 1; NY DHSES Alerting Modernization NPRM Comments at 3 ("there must not be the opportunity for malicious actors to alter messages or impersonate alerting authorities. In order to protect infrastructure, multi factor authentication (MFA), logging, alerting, 24x7 monitoring, event escalation, and routine auditing should be considered for incorporation into systems used."); Sonoma DEM Alerting Modernization NPRM Comments at 3; Washington EMD Alerting Modernization NPRM Comments at 8-9.

[112] *See* NCTA Alerting Security NPRM Comments at 4; Gray Television Alerting Security NPRM Reply at 4.

[113] *See PSHSB Urges EAS Participants to Secure Equipment*; *see also* FCC, *Alerting Security Roundtable*, (Oct. 30, 2023), https://www.fcc.gov/news-events/events/2023/10/alerting-security-roundtable.

and supported by modern, Internet-connected EAS equipment.[114] Here, too, the burden is no greater than that experienced by many Americans who routinely install security-related updates to their device operating systems and applications on a regular basis. While installing a firewall may require some EAS Participants to identify a vendor who can configure their systems appropriately, we do not expect that this will be burdensome or time-consuming for EAS Participants to identify because firewalls are widely recognized as a basic and cost-effective cybersecurity safeguard appropriate even for organizations with limited resources.[115]

29. Further, there is an urgency to protect against threats from malicious actors by implementing these security measures as soon as practicable. Cyber threats that we warned EAS Participants about several years ago continue today.[116] At the same time, cyber threat activities are becoming more sophisticated. For example, CISA recently issued an advisory that warned of "China-nexus cyber actors . . . using large scale networks of compromised devices (covert networks) to route their cyber activity."[117] Given the apparent inadequacy of voluntary approaches to implementing basic security safeguards to remediate these threats—and the significant risk posed by a false alert or non-transmission of a real alert—we find that each of the three requirements we adopt today are reasonable and necessary to protect the security and integrity of EAS.

D. Benefits and Costs

30. We find that the targeted rules adopted today will promote EAS security without imposing substantial costs on EAS Participants. These measures are necessary to protect EAS from future false alerts that are damaging to public safety. Improved EAS security will also provide benefits to EAS Participants in the form of avoided reputational harm that may arise from cyberattacks and false alerts being transmitted from their stations. While the new rules may require hiring outside contractors in some cases, EAS Participants will have the flexibility to satisfy this requirement in a manner tailored to their particular business needs.

31. *Costs.* While commenters, including FEMA, Altice, Gray Television, and Sage,[118] raise concerns about the increased costs and burdens that the proposals in the *Alerting Security NPRM* would place on EAS Participants, the basic cybersecurity hygiene practices we adopt today represent a narrow subset of those proposals, which EAS Participants should be able to implement without significant

---

[114] *See* DAS Alerting Modernization NPRM Comments at 47, 50 (explaining that DAS "provides regular security patches; our devices support authenticated, signed updates to ensure integrity" and that "[m]anufacturers can and should implement the measures such as the ability to notify users of needed software updates, . . . commit[ting] to timely patches for critical vulnerabilities and communicate remediation clearly to customers."); *see also* State Broadcasters Associations Comments, PS Docket Nos. 15-94, 15-91, and 22-329, at 17-18 (rec. Dec. 26, 2022) (EAS equipment manufacturers "may already have the ability to directly notify users that have not updated their software of the need to do so . . . ").

[115] *See* NIST, Guidelines on Firewalls and Firewall Policy, NIST SP 800-41 Rev. 1 (2009), https://csrc.nist.gov/pubs/sp/800/41/r1/final.

[116] *See*, *e.g.*, *PSHSB Urges EAS Participants to Secure Equipment*.

[117] CISA, *Defending Against China-Nexus Covert Networks of Compromised Devices* (Apr. 23, 2026), https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-113a; *see also* Office of the Director of National Intelligence, *2026 (U) Annual Threat Assessment of the U.S. Intelligence Community: March 2026* (Mar. 2026) at 16-17, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2026-Unclassified-Report.pdf.

[118] FEMA IPAWS Program Office Comments, PS Docket Nos. Nos. 15-94, 15-91, and 22-329, at 1 (rec. Dec. 16, 2022); NAB Alerting Security NPRM Comments at 2; Altice, USA, Inc. Reply, PS Docket Nos. 15-94, 15-91, and 22-329, at 9 (rec. Jan. 23, 2023) (Altice Alerting Security NPRM Reply); Gray Television Alerting Security NPRM Reply at 4; Letter from Harold Price, President, Sage Alerting Systems, Inc., to Marlene H. Dortch, Secretary, FCC, PS Docket Nos. 15-94, 15-91, and 22-329, at 1 (filed Jan. 25, 2023).

expenditure. For instance, the American Militia Association states that the Commission's estimated total cost of $11,600 per year is "grossly understated [as applied to] legal fees to review new rules and reporting requirements, payments to networking professionals and other costs . . . to ensure compliance."[119] However, the requirements in this *Report and Order* are less burdensome than what was proposed in the *Alerting Security NPRM* as they do not include reporting of unauthorized access incidents, nor do they include creating, updating, or annually certifying to having a sufficient cybersecurity risk management plan that covers a broader range of established best practices.

32. We estimate that the costs of changing and regularly updating default passwords, installing security patches as available, and implementing firewalls or other network segmentation practices will not exceed $26 million.[120] This estimate is adjusted to reflect the requirements adopted today in light of the record. In the *Alerting Security NPRM*, we estimated that EAS Participants would require, on average, 10 hours annually to draft a cybersecurity risk management plan, update the plan, and submit their certification to the Commission, at an overall cost of $21 million.[121] We instead find that 10 hours is a reasonable average burden estimate across all EAS Participants for the three limited requirements that we adopt today. As DAS states, changing default passwords and installing certain security patches can be accomplished in the normal course of business and at little or no additional cost to EAS Participants.[122] Further, NAB points out that many EAS Participants are already taking some or all

[119] American Militia Association Comments, PS Docket Nos. Nos. 15-94, 15-91, and 22-329, at 5 (rec. Jan. 23, 2023).

[120] We estimate the total cost of implementing the EAS security measures as follows: 25,800 entities × (10 hours per entity per year) × ($65 mean hourly wage) × (1 + 7% inflation adjustment) × (1 + 46% benefit mark-up) = $26,198,094 total cost per year, rounded to $26 million. *See* Bureau of Labor Statistics, *Economic News Release: Table 1. National employment and wage data from the Occupational Employment and Wage Statistics survey by occupation, May 2025*, (May 15, 2026), https://www.bls.gov/news.release/ocwage.t01.htm (referencing "General and Operations Manager (11-1021)" hourly mean wage); Federal Reserve Bank of St. Louis, *Average Hourly Earnings of All Employees, Total Private* (*CES0500000003*), https://fred.stlouisfed.org/series/CES0500000003 (last visited May 4, 2026) (showing that according to Bureau of Labor Statistics data the average hourly private wage increased by 7% between May 2024 and March 2026). According to the Bureau of Labor Statistics, as of December 2025, civilian wages and salaries averaged $33.45/hour and benefits averaged $15.33/hour. Total compensation therefore averaged $33.45 + $15.33 = 48.78. *See* Bureau of Labor Statistics, Employer Costs for Employee Compensation – December 2025 (Mar. 20, 2026), https://www.bls.gov/news.release/pdf/ecec.pdf. Using these figures, benefits constitute a markup of $15.33/$33.45 = 46%. We therefore mark up wages by 46% to account for benefits. The figure 25,797 includes 21,658 broadcaster stations and 4,139 headends. With two direct broadcast satellite (DBS) providers and one satellite digital audio radio service (SDARS) provider, the total number of providers is 25,800. *See* FCC, 2024 Communications Marketplace Report at 127 (2024), https://docs.fcc.gov/public/attachments/FCC-24-136A1_Rcd.pdf (stating that Sirius XM is the only SDARS provider and DIRECTV and DISH Network are the only two DBS providers); *Broadcast Station Totals as of June 30, 2025*, Public Notice, DA 25-581 (July 8, 2025), https://docs.fcc.gov/public/attachments/DA-25-581A1.pdf (stating that there were 33,632 broadcast stations in the U.S. as of June, 30, 2025, from which we subtract 11,974 FM translators and boosters, and VHF and UHF translators that do not originate programming, for a total number of affected broadcast stations of 21,658). Based on Commission staff review of the S&P Global Market Intelligence, S&P Capital IQ Pro, U.S. MediaCensus, *Operator Subscribers by Geography* (last visited May 26, 2022), there were 4,139 cable headends in the United States. This methodology likely overestimates the number of radio and television broadcasters that participate in the EAS, as some are exempted from the Commission's rules that govern EAS. For example, if a hub station satisfies the EAS requirements, an analog or digital broadcast satellite station that rebroadcasts 100% of the hub station's programming would not be required to comply with the proposed rules. *See* 47 CFR § 11.11(b).

[121] *Alerting Security NPRM*, 37 FCC Rcd at 12947-48, para. 32. This figure was based on the cost for 25,644 EAS Participants of 10 hours of labor from a General and Operations Manager who is compensated at $82 per hour. *Id.*

[122] *See* Digital Alert Systems, Inc. Reply, PS Docket Nos. 15-94, 15-91, and 22-329, at 2 (rec. Jan. 23, 2023) (DAS Alerting Security NPRM Reply) (agreeing that "[e]ven small operators should consider these [firmware and

(continued….)

of the actions adopted in this *Report and Order*, recommending that "the FCC should target its efforts at the fairly small number of entities that may lag in updating their equipment or software."[123] To the extent that these entities already engage in password security and regular software update practices, we expect that the amount of additional time required to comply with the rules we adopt today would be low. Some EAS Participants may incur costs, however, to implement firewalls or other comparable network segmentation practices to limit remote management access, if they do not already do so. Therefore, we find that the cost estimate we adopt today is very conservative, due to the relatively narrow scope of requirements in this *Report and Order*, but the benefits will outweigh even this overestimated cost.

33. *Benefits.* We find, as suggested in the *Alerting Security NPRM*, that while it is impossible to quantify the precise dollar value of improvements to the public's safety, life, and health, as a general matter,[124] substantial public safety benefits will result from the adoption of robust security requirements for EAS providers, such as the rules adopted today. We agree with the D.C. Homeland Security and Emergency Management Agency that "[o]ne of the most damaging and dangerous impacts we have [of a cybersecurity incident] is that we don't have the ability to launch Wireless Emergency Alerts or push to EAS."[125] The rules we adopt today will help to ensure the security and operability of EAS Participants. Additionally, as the Commission previously found, "a foreign adversary's access to American communications networks could result in hostile actions to disrupt and surveil our communications networks, impacting our nation's economy generally and online commerce specifically, and result in the breach of confidential data."[126] Consistent with the Commission's past analysis, our national gross domestic product (GDP) was over $30 trillion in 2025.[127] As the requirements we adopt today apply narrowly to EAS Participants and their EAS equipment, studio transmitter link equipment, and any other remotely managed equipment that routes, processes, or inserts content into the EAS Participant's programming, rather than the more broad proposals we sought comment on in the *Alerting Security NPRM*, if these requirements prevent even a 0.00009% disruption of our economy, that would offset the costs.[128] Likewise, local radio and television broadcasting, a subset of EAS Participants, supported $1.19 trillion of our GDP in 2025,[129] so preventing the disruption of even 0.0022% would

(Continued from previous page)
software] updates to be the normal cost of doing business"); *see also* Center for Internet Security Comments, PS Docket Nos. 15-94, 15-91, and 22-329, at 6-7 (rec. Jan. 23, 2023) (CIS Alerting Security NPRM Comments) (explaining that the CIS Critical Security Controls, which include the basic cybersecurity hygiene requirements we adopt today, are flexible by design and providing a mapping to guide implementation in Annex 2).

[123] *See* NAB Alerting Security NPRM Comments at 4.

[124] *See Resilient Networks Amendments to Part 4 of the Commission's Rules Concerning Disruptions to Communications New Part 4 of the Commission's Rules Concerning Disruptions to Communications*, PS Docket Nos. 21-346, 15-80, and ET Docket No. 04-35, Report and Order and Further Notice of Proposed Rulemaking, 37 FCC Rcd 8059, 8075, para. 46 (2022) (*Resilient Networks Order*) ("it would be impossible to quantify the precise financial value of these health and safety benefits").

[125] Clint Osborn, D.C. Homeland Security and Emergency Management Agency, Interim Director, Alerting Security Roundtable, 2:32:03 (Oct. 30, 2023), https://www.fcc.gov/news-events/events/2023/10/alerting-security-roundtable.

[126] *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs Huawei Designation ZTE Designation*, WC Docket No. 18-89; PS Docket Nos. 19-351 and 19-352, Report and Order, Further Notice of Proposed Rulemaking, and Order, 34 FCC Rcd 11423, 11465, para. 109 (2019).

[127] U.S. Bureau of Economic Analysis, *Table 1.1.5. Gross Domestic Product*, https://apps.bea.gov/iTable/?reqid=19&step=3&isuri=1&categories=survey&nipa_table_list=5&Series=A&select_all_years=1&_gl=1*16zt8m*_ga*MjY2NzAxMjE1LjE3NzUwNzA3ODk.*_ga_J4698JNNFT*czE3NzUwNzA3ODkkbzEkZzEkdDE3NzUwNzA5ODkkajE3JGwwJGgw (last visited Apr. 1, 2026).

[128] $26,000,000/$30,000,000,000,000 = 0.000087%.

outweigh the costs.[130] As the Commission also noted in the *Alerting Security NPRM*, the cost of malicious cyber activity on the U.S. economy in 2016 was between $57 billion and $109 billion,[131] so reducing this activity (or preventing an expansion of such damage) by even 0.046% (significantly less than the 1% considered in the *Alerting Security NPRM*) would produce benefits that outweigh the costs.[132] We find that our reasoning in the *Alerting Security NPRM* remains applicable to the rules we adopt today, notwithstanding their narrowed scope, because the security measures we adopt today will significantly harden EAS Participants' systems against these types of attack and mitigate the risk of occurrence. Thus, we conclude that the minor costs associated with implementing the targeted security requirements in this *Report and Order* will be more than offset by its public safety and economic benefits.

E. Terminating the 2022 Alerting Security NPRM

34. We believe that the most effective and proportionate path to mitigating threats against EAS Participants and Participating CMS Providers is to address specific, repeatedly exploited cybersecurity vulnerabilities rather than adopting the broader cybersecurity risk management framework proposed in the *Alerting Security NPRM*.[133] We agree with Nexstar Media that the cyber incidents this *Report and Order* is intended to prevent could have been easily avoided by undertaking basic network security measures such as those we require today.[134] After further consideration, we conclude that adopting wide-ranging cybersecurity risk management requirements that apply to all of an EAS Participant or Participating CMS Provider's systems and services would impose extremely high costs that outweigh the security benefits.

35. NPR highlights the high costs of the Commission's proposals by pointing out that the *Alerting Security NPRM's* estimate is "off by a factor of 10 or more – it would take a local General Manager or Operations Manager many hours just to understand the baseline framework involved, not to mention developing and implementing a cybersecurity risk plan."[135] On further consideration, we conclude that costs to EAS Participants and Participating CMS Providers would include not only the creation of a cybersecurity risk management plan, but also the implementation of that plan, which the Commission failed to take into account in designing its proposal. Based on additional evidence and additional consideration, we agree with the view that "compliance with the FCC's proposals in the Notice could easily run into the thousands of dollars, directly impacting a station's bottom line."[136] These costs would be particularly high for small broadcasters.[137] In light of these costs, we disagree with the Center

(Continued from previous page)

[129] Woods & Poole Economics, *Local TV and Radio: Helping Drive the United States Economy* at 1 (2025), https://www.wearebroadcasters.com/documents/2025-NAB-Woods-Pooles-Local-Broadcasting-Publication.pdf.

[130] $26,000,000/$1,190,000,000,000 ~ 0.0022%.

[131] The Council of Economic Advisers, *The Cost of Malicious Cyber Activity to the U.S. Economy* at 36 (Feb. 2018), https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf.

[132] $26,000,000/$57,000,000,000 ~ 0.046%.

[133] *See Alerting Security NPRM*, 37 FCC Rcd at 12942-51, paras. 22-36.

[134] Nexstar Media Reply Comments, PS Docket Nos. 15-94, 15-91, and 22-329, at 3 (rec. Jan. 23, 2023) (Nexstar Alerting Security NPRM Reply).

[135] NPR Alerting Security NPRM Reply at 8.

[136] NAB Alerting Security NPRM Comments at 20; *see also* Native Public Media Alerting Security NPRM Comments at 3 (estimating that developing and implementing a cybersecurity risk management plan would cost tens of thousands of dollars); NTA Alerting Security NPRM Comments at 7 (estimating an annual cybersecurity review cost around $2,000 and an initial assessment of $10,000).

[137] REC Networks Alerting Security NPRM Comments at 18; *see also* CBA Alerting Security NPRM Comments at 2 ("These burdens will have an especially significant impact on smaller broadcasters that have the least available

(continued….)

for Internet Security's view that requiring alerting participants to implement a cybersecurity framework, such as their Critical Security Controls, is appropriate because those requirements would be "narrowly tailored" or "minimally intrusive."[138] On balance, we find that addressing the most immediate threats to EAS Participants by adopting narrowly targeted security requirements to be more cost-effective than adopting the Commission's broad and burdensome proposal.

36. We decline to adopt a rule at this time that would require Participating CMS Providers to take further action to prevent false alerts from fake base stations.[139] No commenter to the *Alerting Security NPRM* supported the Commission's adoption of rules to address this risk. To the contrary, AT&T and CTIA state that the ongoing international standard process is best positioned to address this issue,[140] and ATIS questions whether such an attack on WEA would have a realistic chance of success.[141] We acknowledge that the 3GPP SA3 (Security) working group published a study in 2023 on 5G security enhancements against false base stations, which identifies key issues and multiple candidate solutions.[142] We encourage the 3GPP security working group to continue this work to move from candidate solutions to implementable best practice recommendations.

37. We decline at this time to make changes to the rules that allow for continued operations for a period of 60 days despite having defective equipment that precludes their participation in EAS.[143] The Commission did not receive a sufficient record on this issue in response to the *Alerting Security NPRM* and several commenters were opposed to elimination of the 60-day rule arguing that the 60-day timeframe is necessary to complete repairs on EAS equipment.[144] We note that our proposal in the *Further Notice* to allow EAS Participants to use software to fulfill their EAS obligations could have implications for the ability to receive timely repair and replacement of defective EAS equipment, and we seek comment on this issue below.

38. We also decline to adopt the Commission's proposal that EAS Participants and Participating CMS Providers report any substantial incident of unauthorized access of their systems to the Commission.[145] We agree with commenters that adopting additional cybersecurity incident reporting

(Continued from previous page)
resources for implementation of new technology systems."); Prometheus Alerting Security NPRM Comments at 2; Competitive Carriers Association Comments, PS Docket Nos. 15-94, 15-91, and 22-329, at 5 (rec. Dec. 23, 2022) (CCA Alerting Security NPRM Comments); NPR Alerting Security NPRM Comments at 8 (arguing that the creation of cybersecurity risk management plans "is simply not tenable for many small or noncommercial radio stations"); National Federation of Community Broadcasters Comments, PS Docket Nos. 15-94, 15-91, and 22-329, at 1-3 (rec. Dec. 23, 2022) ("For many community NCE radio stations, meeting the requirements of the Commission's proposed rules would require a significant budgetary impact on stations that already grapple with limited technical and staff resources. . . . [C]ommunity stations would need to reallocate already constrained resources away from programming."); NAB Alerting Security NPRM Comments at 19-20.

[138] CIS Alerting Security NPRM Comments at 4-9.

[139] *Alerting Security NPRM*, 37 FCC Rcd at 12949-50, paras. 37-38.

[140] AT&T Comments, PS Docket No. 15-94, 15-91, and 22-329, at 10-11 (rec. Dec. 23, 2022); CTIA Alerting Security NPRM Comments at 22.

[141] ATIS Alerting Security NPRM Comments at 3-4.

[142] 3GPP, Study on 5G Security Enhancement against False Base Stations, at 14 (2023), https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3539. 3GPP's last published update to this work was in 2023.

[143] *Alerting Security NPRM*, 37 FCC Rcd at 12938, para. 9.

[144] CBA Alerting Security NPRM Comments at 3; *see also* DAS Alerting Security NPRM Reply at 5; Nexstar Alerting Security NPRM Reply at 2; Altice Alerting Security NPRM Reply at 3-5.

requirements for alerting participants would be premature in light of CISA's pending rulemaking implementing the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA).[146] Rather than adopting potentially duplicative incident requirements, we will continue to monitor CISA's work.

39. We decline to remove language from Sections 10.330 and 10.500 of the Commission's rules that provide that WEA functionality, both in Participating CMS Providers' networks and in mobile devices, "are dependent upon the capabilities of the delivery technologies implemented by a Participating CMS Provider" and certain WEA protocols "are defined and controlled by each Participating CMS Provider."[147] The Commission proposed these changes because it was concerned that the rules might "create the mistaken impression that Participating CMS Providers' compliance with the rules . . . , would be conditioned on the Participating CMS Providers' delivery technology."[148] CTIA opposes changing Section 10.330 because "it provides CMSPs the necessary flexibility to develop and deploy network technologies driven by consumer demand"[149] and FEMA opposes changing it because they wanted to preserve Participating CMS Providers' flexibility to use technologies other than cell broadcast to support WEA.[150] No commenter supported the elimination of this language, nor have we observed any non-compliance with the WEA rules attributable to the flexibility this rule provides. For these reasons, we decline to remove the language in question at this time.

40. The actions we take today are consistent with the approach to cybersecurity that we described in the 2025 *CALEA Order on Reconsideration*.[151] The Commission continues to pursue targeted, legally robust regulatory and enforcement measures alongside a collaborative approach that emphasizes public-private partnerships that protect and secure communications networks. For instance, the Commission hosted cybersecurity workshops for broadcasters and telecommunications companies in May 2026 that brought together public- and private-sector representatives to raise awareness of emerging cybersecurity risks, share and promote adoption of best practices, and highlight opportunities for public-private partnership on cybersecurity issues facing communications providers.[152] Unlike the one-size-fits-

(Continued from previous page)

[145] *See Alerting Security NPRM*, 37 FCC Rcd at 12939-42, paras. 13-21.

[146] America's Communications Association Comments, PS Docket Nos. 15-94, 15-91, and 22-329, at 4 (rec. Dec. 23, 2022) (arguing that the Commission cannot know whether the reporting it proposed will align with those proposed by CISA, and arguing that the proposed reporting deviates from CIRCIA's reporting framework); Altice Alerting Security NPRM Reply at 9 (supporting rules that harmonize with CIRCIA); Competitive Carriers Association Reply, PS Docket Nos. 15-94, 15-91, and 22-329, at 2-3 (rec. Jan. 23, 2023) (urging the Commission to work with CISA to ensure the rules it adopts harmonize with CIRCIA); CTIA Reply, PS Docket Nos. 15-94, 15-91, and 22-329, at 12-13 (rec. Jan. 24, 2023) (arguing the Commission's proposed reporting is in conflict with CIRCIA); DAS Alerting Security NPRM Reply at 2 (urging the Commission to work with CISA to ensure its reporting harmonizes with CIRCIA); NAB Alerting Security NPRM Comments at 1 (arguing that, under CIRCIA, CISA will share the information it receives through reporting with other federal agencies); NCTA Alerting Security NPRM Comments at 6-9 (arguing that this reporting is duplicative of the reporting required by CIRCIA); NTCA–The Rural Broadband Association Alerting Security NPRM Comments at 2-3 (urging the Commission to not create rules that conflict with those being developed by CISA); USTelecom Reply, PS Docket Nos. 15-94, 15-91, and 22-329, at 2, 4-8 (rec. Jan. 23, 2023) (arguing this reporting is premature and potentially in conflict with CIRCIA).

[147] *See Alerting Security NPRM*, 37 FCC Rcd at 12951, para. 41; 47 CFR §§ 10.330, 10.500.

[148] *Alerting Security NPRM*, 37 FCC Rcd at 12951, para. 41.

[149] CTIA Alerting Security NPRM Comments at 27; *see also* CCA Alerting Security NPRM Comments at 6-7 ("Removing the existing flexibility offered by the Commission's regulations would again discourage participation by smaller and regional carriers.").

[150] FEMA Comments, PS Docket Nos. 15-94, 15-91, and 22-329, at 5 (rec. Dec. 16, 2022).

[151] *Protecting the Nation's Communications Systems from Cybersecurity Threats*, PS Docket No. 22-329, Order on Reconsideration, 40 FCC Rcd 9582 (2025).

all proposals in the *Alerting Security NPRM*, our flexible and coordinated approach is proven to make networks more secure.[153] For these reasons, we terminate PS Docket No. 22-329.

IV. FURTHER NOTICE OF PROPOSED RULEMAKING

A. Securing EAS Through Message Authentication

41. While the security measures that we require EAS Participants to implement in the accompanying *Report and Order* are necessary to prevent bad actors from exploiting poor security hygiene by EAS Participants, they are not sufficient to prevent our nation's adversaries from originating false alerts. To better secure EAS against cyberattacks, we propose to require EAS Participants to reject CAP EAS messages that do not include a valid digital signature. Digital signatures work by encrypting a hash or "fingerprint" of data with a "private [encryption] key" known only by the signer.[154] The corresponding "public key"—typically made publicly or semi-publicly available—can decrypt a message encrypted using the "private key." Thus, the "public key" ensures that a message encrypted using the corresponding "private key" is authentic (since only the entity that possesses the "private key" could have produced that encrypted message). Effective key management ensures that this process functions properly by controlling the issuance, distribution, and revocation of both public and private keys so that both originator and receiver have the correct valid keys. Public keys are issued as "digital certificates," typically by certificate authorities that issue and manage certificates for public, private, and government entities. For CAP alerts sent through IPAWS, IPAWS maintains the public keys for all alert originators including itself.[155] Because IPAWS digitally signs all alerts it issues, EAS devices acquire IPAWS's digital certificate (with the IPAWS public key) to authenticate alerts issued by IPAWS.[156] While digital signatures are currently required by IPAWS, EAS Participants are only required to reject EAS messages that include an invalid digital signature. Our rules still allow EAS Participants to transmit EAS messages with no digital signature at all.[157]

42. DAS believes that "the FCC's rules should be amended to require authentication and digital signatures for every CAP message received by an EAS CAP device, not just those received from FEMA IPAWS," and advocates for "harden[ing] authentication/authorization throughout the system, to prevent spoofing and maintain confidence in alerts."[158] Washington State Emergency Management

(Continued from previous page)

[152] FCC, *Cybersecurity Workshop for Broadcasters*, https://www.fcc.gov/news-events/events/2026/05/cybersecurity-workshop-broadcasters [https://perma.cc/3275-DZT2] (last visited May 29, 2026); FCC, *Cybersecurity Workshop for Telecommunications Carriers*, https://www.fcc.gov/news-events/events/2026/05/cybersecurity-workshop-telecommunications-carriers [https://perma.cc/T9LU-JT5B] (last visited May 29, 2026).

[153] *Cf. Review of Submarine Cable Landing License Rules and Procedures to Assess Evolving National Security, Law Enforcement, Foreign Policy, and Trade Policy Risks; Amendment of the Schedule of Application Fees Set Forth in Sections 1.1102 through 1.1109 of the Commission's Rules*, OI Docket No. 24-523, MD Docket No. 24-524, Report and Order and Further Notice of Proposed Rulemaking, 40 FCC Rcd 6481, 6540-42, paras. 105-08 (rejecting a proposed rigid, one-size-fits-all requirement for submarine cable licensees and instead adopting a more flexible approach).

[154] CISA, *Understanding Digital Signatures* (Feb. 1, 2021), https://www.cisa.gov/news-events/news/understanding-digital-signatures.

[155] FEMA, *Sign Up to Use IPAWS to Send Public Alerts and Warnings*, https://www.fema.gov/emergency-managers/practitioners/integrated-public-alert-warning-system/public-safety-officials/sign-up (last visited June 1, 2026).

[156] OASIS Open, *Common Alerting Protocol Version 1.2* (July 1, 2010), https://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2-os.html.

[157] 47 § CFR 11.56(c).

Division asserts that "[s]ystems should incorporate end-to-end authentication to prevent spoofing, tampering, or false alerts[,] [includ[ing] digital signatures, secure handoffs between IPAWS and carriers, and safeguards to ensure the alert received by the public matches exactly what the originator sent."[159] These comments reinforce the Communications Security, Reliability, and Interoperability Council (CSRIC) VI's finding that "[t]he importance of high confidence in sender authenticity is especially apparent in a public safety context," and its recommendation that EAS Participants should not be permitted to transmit CAP messages that lack a digital signature.[160] We agree with these commenters and believe that our proposal represents a major step forward in securing CAP EAS alerts. We seek comment on this view. Do alerts that lack digital signatures pose a high risk to EAS, and what kinds of harm could they cause? Are there any other public safety benefits that would arise from all EAS CAP alerts being authenticated? We believe that compliance with this requirement would be technically straightforward for EAS Participants because their EAS equipment already must authenticate signed CAP EAS messages. We seek comment on this view.

43. We seek comment on how this requirement would affect alerting authorities that originate CAP EAS messages. When the Commission required EAS Participants to reject alerts with invalid digital signatures in 2018, it declined to mandate digital signatures for all transmitted CAP EAS alerts because many state and local alerting authorities were not yet using IPAWS or CAP-based digital signatures.[161] Currently, however, we understand that there are more than 2,000 federal, state, local, tribal and territorial alerting authorities that use IPAWS, which requires digital signatures for alerts distributed through its system.[162] Does this mean that most state and local alerting authorities would be unaffected by this requirement since they are already signing alerts for distribution through IPAWS? We seek comment on the extent to which state and local CAP systems other than IPAWS support digital signatures and whether this proposal would undermine the ability of those systems to send alerts. To the extent that these systems do not support alert authentication, we seek comment on the steps that would be required to enable that functionality and how long those steps would take to complete.

44. While there are numerous benefits to alert authentication, there may also be risks. According to CSRIC VI, these risks include delaying alert message delivery and increasing the chance that a valid alert will be rejected as invalid.[163] Have those risks materialized since the Commission required the rejection of CAP EAS alerts with invalid digital signatures in 2018? Have there been any notable cases in which valid alerts have been erroneously delayed or rejected? If we were to require the rejection of CAP EAS alerts that lack digital signatures, would that level of risk stay the same or materially increase? For example, during the 2023 nationwide EAS test, only 23 EAS Participants reported problems related to the CAP EAS alert's digital signature, which is a very low percentage of the 20,682 EAS Participants that took part in the test.[164] Is there any reason to expect that there would be

(Continued from previous page)

[158] DAS Alerting Modernization NPRM Comments at 3, 47.

[159] Washington EMD Alerting Modernization NPRM Comments at 8; *see also* Vergara Alerting Modernization NPRM Reply at 1 (asserting that "authentication must be prioritized . . . [to] ensur[e] that every message originates from an authorized and verifiable source"); Lavrov Alerting Modernization NPRM Reply at 1; NY DHSES Alerting Modernization NPRM Comments at 3; Sonoma DEM Alerting Modernization NPRM Comments at 3.

[160] CSRIC VI EAS Security Report at 27, 33-34.

[161] *Amendment of Part 11 of the Commission's Rules Regarding the Emergency Alert System; Wireless Emergency Alerts*, PS Docket Nos. 15-94 and 15-91, Report and Order and Further Notice of Proposed Rulemaking, 33 FCC Rcd 7086 at 7095-96, paras. 20-21 (2018) (*2018 WEA and EAS Order*).

[162] FEMA, *IPAWS Alerting Authorities - Agencies and Organizations* (July 23, 2025), https://www.fema.gov/emergency-managers/practitioners/integrated-public-alert-warning-system/public-safety-officials/alerting-authorities/agencies-organizations.

[163] CSRIC VI EAS Security Report at 21.

significantly more failures during future tests if we were to adopt our proposal? Are the risks to non-IPAWS EAS CAP messages any different than for IPAWS messages? Should we take any steps to mitigate risks, including the possibility of key management and authentication failures?

45. We also seek comment on the feasibility, effectiveness, and costs of requiring EAS Participants to authenticate (i.e., digitally sign) legacy EAS alerts, which are sent via the EAS Protocol.[165] As explained by CSRIC VI, a digital signature requires two things: (1) a "hash" of the message to be signed, and (2) access to the public key used to decrypt that encrypted hash.[166] When CSRIC VI examined this issue in 2018, it determined that legacy EAS may be vulnerable to attack, but also determined that it faces technical challenges in implementing digital signatures.[167] Unlike CAP alerts, legacy EAS is severely limited in how much data it can convey because the data that comprises the alert is converted into audio for transmission over broadcast.[168] Adding the data necessary for a digital signature would delay alert message transmission and, in turn, delay the public's receipt of emergency alerts.[169] This delay could be significant because unlike CAP alerts received from IPAWS, legacy alerts may be relayed from one EAS Participant to another, and all entities sending the alert would need to create a hash of the alert using their digital signature before repackaging it for rebroadcast. In the legacy EAS "daisy chain" in which EAS Participants monitor one another as sources of alerts, the time it takes to authenticate an alert would likely be multiplied for each EAS Participant in the chain. We seek comment on the extent to which the public's receipt of EAS messages could be delayed as a result of an authentication requirement for legacy EAS.[170]

46. CSRIC VI also raised issues with reliance on the Internet for checking the required public and private encryption key certificates, encryption key management related to managing signing keys for all participants, and interoperability with existing consumer equipment.[171] We seek comment on

(Continued from previous page)

[164] FCC, Report: October 4, 2023 Nationwide Emergency Alert Test at 17 (2024), https://docs.fcc.gov/public/attachments/DOC-403500A1.pdf.

[165] In 2016, the Commission sought "comment on the desirability and feasibility of including a unique message ID and/or authenticator ancillary to the EAS Protocol header codes and . . . on the advantages and disadvantages of including a digital signature in CAP- and EAS Protocol-formatted EAS messages." *Amendment of Part 11 of the Commission's Rules Regarding the Emergency Alert System*; *Wireless Emergency Alerts*, PS Docket Nos. 15-94 and 15-91, Notice of Proposed Rulemaking, 31 FCC Rcd 594, 651, para. 139 (2016). In 2018, the Commission believed "it would be premature to adopt rules pertaining to specific authentication mechanisms for EAS Protocol messages . . . ." *2018 WEA and EAS Order*, 33 FCC Rcd at 7096, para. 22.

[166] CSRIC VI EAS Security Report at 26-29. Hashing refers to a process of scrambling data according to any one of many algorithms designed for that purpose. Hashed data cannot be altered, which ensures the authenticity of the hashed data.

[167] *Id.* at 27.

[168] *Id.* at 27-28 (explaining that whereas a CAP alert can include copious data, including the hashed message, and public and private encryption key certificates required to decrypt and authenticate the incoming hashed message, it is not practical to replicate that approach in legacy EAS).

[169] *Id.* (explaining the time consideration involved in sending an encrypted hash, and showing that adding a digital signature with a key length of 2048 bits would add 8.6 seconds, if sent twice with the header code strings, to the time required to validate and process the alert's header code stings).

[170] *See id.* at 29 (explaining that "[t]o fully implement a digital certificate/hash validation schema, every potential issuer of an EAS message would need to obtain (and be accredited) for an alert origination digital certificate. This could include many EAS Participants themselves," and adding that "[p]resuming the FEMA IPAWS digital certificate was used for this purpose, both FEMA and the broadcast industry would be presented with a requirement to obtain, and maintain, these additional digital credentials.").

how to address these challenges, including the non-conformity of legacy equipment that is no longer supported by software updates. Would the NWS, which originates the vast majority of EAS alerts, be able to digitally sign the alerts it issues over the air via National Oceanic and Atmospheric Administration (NOAA) Weather Radio (NWR)? Would inclusion of a digitally signed hash in a legacy alert impact the operability of the embedded base of consumer and enterprise emergency radios that trigger off of the EAS protocol header codes? Would the audio portion of an EAS message remain susceptible to attacker manipulation and replay attacks even if the alert header itself were to be authenticated? Is the threat that our nation's adversaries may exploit the weaknesses of legacy alerts likely and severe enough to outweigh the difficulty, limitations, and effect on availability associated with solutions?

47. If we were to require EAS Participants to only transmit digitally signed legacy EAS alerts, we seek comment on how to best implement that requirement. Where should the digital signature be placed in relation to the header codes? Could it replace part of the attention signal?[172] What elements of the header code string should be covered by the signature? Could we add the four-digit year to the elements covered by the signature without adding them to the header codes as transmitted? Assuming the data rate of the current AFSK (Audio Frequency-Shift Keying) encoding of the header codes is too slow to include the signature without unacceptable delay of the audio alert, how should the signature be encoded and how many seconds would it take? What specific protocols and standards would need to be developed or modified to add digital signatures to legacy EAS and how long would it take to develop them? How would these changes impact existing systems like consumer, first responder, and enterprise emergency and weather radios, and Alert FM receivers? Are there solutions that would minimize these impacts? Should the Commission take any actions to promote effective management of the key infrastructure needed to digitally sign legacy EAS messages? Sage states that, if the Commission were to require authentication for legacy EAS, every EAS Participant and alerting authority would require its own digital signature to maintain the same capabilities as the current system.[173] Is that accurate, or are there more efficient approaches through which key distribution and updates can be managed? One approach to streamline and simplify key management could be to limit the ability to sign legacy EAS alerts to only certain entities within each state. Could this approach work, and if so, to which entities should it be limited? What is the likelihood that access to signing certificates could be compromised during widespread disaster conditions, widespread IP disruption (e.g., route hijacking, ransomware, or router table poisoning), or during routine use? Is that risk distinct from similar risks to signing certifications for CAP EAS alerts, and if so, how? What, if any, role should the Commission have in mitigating these risks? In the event that we allow EAS Participants to use EAS software, would that create a unique opportunity to introduce legacy EAS authentication at a time when costs could be lowest? To what degree should we consider the potential impact of future quantum computers on any authentication

(Continued from previous page)

[171] *Id.* at 26-29. For the digital certificate/hash validation schema to function properly, the EAS device would require the digital certificate for every EAS Participant and alert originator from which it might receive an alert. Digital certificates typically are valid for one year and therefore are constantly being renewed. Acquiring such certificates requires Internet access and would require regular checking for renewed certificates. Accordingly, loss of internet access could prevent acquisition of current digital certificates necessary for alert validation involving an alert originator or EAS Participant relaying an alert whose certificate has been updated since the last version stored in the EAS device.

[172] *See* 47 CFR § 11.31(a), (c) (defining the transmission of 8-25 seconds of the two-tone attention signal after the three transmissions of preamble and header codes).

[173] Sage Alerting Systems, Inc. Comments, PS Docket No. 25-224, at 3 (rec. Sept. 25, 2025) (Sage Alerting Modernization NPRM Comments).

requirement we impose, and should we account for that risk through post-quantum cryptography?[174] If so, how should that be reflected in our rules?

48. We seek comment on whether there are any alternative ways to address the vulnerability of legacy EAS alerts while preserving the resiliency of EAS and its assurance of availability under widespread outages of normal communications paths. Are there any other common sense, technically feasible steps that we should take to secure EAS?

B. Bolstering the Reliability of Emergency Alerts

49. The *Alerting Modernization NPRM* sought comment on the goals of emergency alerting, which commenters agree should include providing authorities with a reliable way to rapidly notify the public of emergencies that may put them at risk.[175] Commenters emphasized that reliability is fundamental to achieving the core goals of the nation's alerting systems. As Xperi Inc. observes, "[d]uring emergencies, the public needs timely, accurate, and actionable information" to help protect lives and property.[176] Similarly, Washington State Emergency Management Division explains that, in their view, "[a]lerts must be accurate, consistent, and non-duplicative to avoid fatigue and maintain public trust."[177] The issues we seek comment on, and the rules we propose today aim to improve the reliability of the nation's alerting systems to ensure that they meet our core goals and provide enhanced protections to the public.

1. Preventing Duplicate Alerts Through a Universal Identifier

50. When we sought comment on alert originators' expectations for delivery of alerts,[178] several commenters explained that both alert originators and the public expect that alerts will be presented to the subscriber once and that the subscriber will not receive duplicates.[179] As the Washington State Emergency Management Division writes, "[a]lerts must be . . . non-duplicative to avoid fatigue and maintain public trust."[180] We agree, and tentatively find that the goals of the nation's alerting systems are undermined when the public receives duplicate alerts and that EAS and WEA should be designed to better detect and suppress duplicate alerts.

51. To reduce confusion and alert fatigue, we propose to require Participating CMS Providers to identify whether an alert is a duplicate through the use of a common message identifier, or "universal alert message ID," that will be assigned to each WEA message they receive and transmit. Even though section 10.500(g) of the Commission's rules already requires WEA-capable mobile devices to detect and suppress duplicate WEA messages,[181] the Commission still frequently receives complaints that members

---

[174] *See* NIST, *What Is Post-Quantum Cryptography?* (Feb. 27, 2026), https://www.nist.gov/cybersecurity-and-privacy/what-post-quantum-cryptography.

[175] CCA Alerting Modernization NPRM Comments at 2; DAS Alerting Modernization NPRM Comments at 2-3; CTIA Comments, PS Docket No. 25-224,at 2 (rec. Sept. 25, 2025) (CTIA Alerting Modernization NPRM Comments).

[176] Xperi Alerting Modernization NPRM Comments at 2.

[177] Washington EMD Alerting Modernization NPRM Comments at 2.

[178] *Alerting Modernization NPRM*, 40 FCC Rcd at 6700, para. 12.

[179] *See, e.g.*, ATIS Alerting Modernization NPRM Comments at 8-9; Washington EMD Alerting Modernization NPRM Comments at 3; USGS Alerting Modernization NPRM Comments at 1, 6; NWS Alerting Modernization NPRM Comments at 1; Colorado 911 Authorities and Public Safety Agencies Comments, PS Docket No. 25-224, at 3 (rec. Sept. 25, 2025) (Colorado Alerting Modernization NPRM Comments).

[180] Washington EMD Alerting Modernization NPRM Comments at 2.

[181] 47 CFR § 10.500(g).

of the public receive duplicate alerts. In investigating this issue, we have learned that Participating CMS Providers use carrier-specific identification numbers to determine whether an alert already has been received by a mobile device. This means that a mobile device that receives and displays an alert on one provider's network and then later receives the same alert while roaming on a different provider's network will display a duplicate alert. We have also learned that one Participating CMS Provider uses different WEA identification numbers on each generation of wireless network technology it has deployed. When this provider transmits a WEA message, its subscribers are at risk of receiving duplicate alerts when they move between generations of wireless network technology within their own home network. We identified this as a potential source of some of the duplicate alerts during the 2025 Los Angeles County wildfires, which caused confusion and complaints during the height of a life-threatening emergency.[182] We believe that using a universal alert message ID would eliminate many duplicate alerts that are currently received by subscribers. If a WEA message contained the same unique identifier, irrespective of the Participating CMS Provider network from which it was transmitted, mobile devices would be better equipped to identify and suppress duplicates. Would the use of a unique identifier prevent duplicate WEA alerts caused by changes from one generation of equipment to another, or if the mobile device received the alert from a cell repeater? We believe that the introduction of a universal alert message ID will lead to an increase in the public's trust in WEA messages and help prevent consumers from opting out of WEA. We seek comment on this analysis. Are there other situations in which a universal alert message ID could help prevent duplicate alerts? For example, do hybrid satellite-terrestrial networks pose new alert duplication risks that arise from the transmission of alerts from different sources?

52. We seek comment on what the source of a universal alert message ID should be. We believe that universal alert message IDs can be derived from unique identification numbers that IPAWS already assigns to each CAP message it receives. We understand, however, that this unique ID is very long and would add significant data overhead to WEA message transmittals if it were to be included in WEA metadata. We seek comment on whether IPAWS' unique identification number can be shortened in a manner that does not add significant data overhead to WEA message transmittals and yet enables mobile devices to determine if an alert is a duplicate.[183] Are there other uniquely identifying CAP fields that should be used instead or in addition to IPAWS' unique identification number? We believe that it would be feasible to use an appropriate hashing function to generate a fixed-size identifier suitable for use from one or more CAP fields. We seek comment on hashing functions that could do so with minimal collisions (duplicate values for two different inputs) and on the acceptable size of the hash value.[184] In the alternative, we seek comment on other methods that could be used to generate a universal alert message ID that remains truly unique over the twenty-four hour retention period of WEA messages.

53. We seek comment on whether IPAWS should be responsible for creating this universal alert message ID and passing it on to Participating CMS Providers. Are there any technical or practical challenges that weigh against the identifier being created by IPAWS? Alternatively, would it be feasible and more efficient for Participating CMS Providers to receive the existing identifier from IPAWS and use the same technique to shorten it as part of their processing of alerts? Should the universal alert message ID originate in alerting authorities' alert origination software, and if so, how can the identifier be designed

[182] *See* Letter from Brendan Carr, Chairman, FCC, to The Honorable Robert Garcia, U.S. House of Representatives at 2 (Apr. 1, 2025), https://docs.fcc.gov/public/attachments/DOC-413393A2.pdf.

[183] Based on Commission staff review of ATIS, *Wireless Emergency Alert (WEA) 3.0 Mobile Device Behavior (MDB) Specification* at 13 (2019), https://webstore.ansi.org/standards/atis/atis0700036v003?srsltid=AfmBOor9m5vC3glR65Xv4nyALiE9GF0Jy2qZWe-8SxnrOpUHOfEwbv-s, duplication detection is based on Message Identifier and Serial Number, as defined in 3GPP TS 23.041.

[184] *See* Avast, *What is the MD5 Hashing Algorithm and How Does it Work*, https://www.avast.com/c-md5-hashing-algorithm (last visited May 11, 2026).

to ensure that alerts originating from different sources are not duplicating the identifier? Should the design of the universal alert message ID be determined by FEMA or through a collaborative standards development process? We seek comment on any alternatives to a universal message ID that Participating CMS Providers could implement to prevent the presentation of duplicate alerts and how those alternatives could be implemented.

54. We also seek comment on whether the use of a FEMA-IPAWS generated identification number would help enable other lifesaving developments in the alerting ecosystem. For example, would a universal alert message ID help the NWS implement "Threats-in-Motion" alerting that could allow NWS to continually update the target area and message content without generating duplicate alerts or causing alert fatigue?[185] ATIS notes that there are some scenarios that are challenging for WEA, notably "complex, multi-stage emergencies that require dynamic updates at brief intervals due to ongoing changes in the threat itself of the location impacted. . . . [where] updates presented to consumers in a short period of time that are similar in nature may be perceived as duplicates."[186] We seek comment on whether a universal alert message ID could aid in solving this issue. Are there other ways in which a universal alert message ID can expand WEA's potential?

55. We seek comment on whether the universal alert message ID could also be implemented in EAS, and if so, whether it would be useful. For example, could a universal alert message ID help prevent duplicate EAS messages? Today, EAS equipment performs a byte-by-byte comparison between EAS messages to detect duplicates. If any relevant information in the EAS message header is different than the previously received and stored messages, it will not be deemed a duplicate. This can cause duplicate alerts in several scenarios, including when the location codes in legacy EAS alerts and EAS CAP messages do not match.[187] Would using a universal alert message ID to identify duplicate alerts, rather than a byte-by-byte comparison of the relevant information in EAS message headers, help alert originators like NWS prevent the transmission of duplicate alerts? What, if any, other changes would be necessary for EAS to realize the benefits of a universal alert message ID? Would legacy EAS need to be updated to rely solely upon the universal alert message ID for duplicate suppression? What, if any, other benefits would a universal alert message ID have for EAS? We seek comment on whether a universal alert message ID could help realize DAS's "One message, many paths," vision, wherein alert originators can compose a single alert that is distributed to WEA, EAS, and NOAA Weather Radio.[188] What would be the most efficient way to implement a universal alert message ID in EAS? What specific characteristics would the universal alert message ID need to have to minimize implementation costs?

2. Ensuring the Consistent Transmission of WEA Messages

56. To ensure that alerting authorities can rapidly notify the public of emergencies, emergency alerting must be resilient and must not unnecessarily delay the public's receipt of alerts. To better support this goal, we seek comment on whether to require Participating CMS Providers to rebroadcast WEA messages at least once every sixty seconds throughout an alert's active period. The Commission has long been concerned that Participating CMS Providers' inconsistent WEA transmission practices threaten the timely delivery of WEA messages and WEA's resiliency.[189] Among major

---

[185] *See* Gregory Stumpf & Alan Gerard, *National Weather Service Severe Weather Warnings as Threats-in-Motion* (2021), https://repository.library.noaa.gov/view/noaa/28465#:~:text=Description%3A-,Threats%2Din%2DMotion%20(TIM)%20is%20a%20warning%20generation,move%20forward%20with%20a%20storm.

[186] ATIS Alerting Modernization NPRM Comments at 8-9.

[187] *See* CSRIC VII, Report on Recommendations to Resolve Duplicate NWS Alerts at 13-15 (2021), https://www.fcc.gov/file/20608/download.

[188] DAS Alerting Modernization NPRM Comments at 24-25.

Participating CMS Providers, one broadcasts each WEA messages every minute throughout the duration of the alert's active period, some only broadcast each WEA message a single time, while still others broadcast each WEA message a limited number of times after a delay of several minutes.[190] We believe that requiring consistent transmission of WEA messages, as recommended by several commenters, will make WEA more resilient to ephemeral service disruptions that may result in mobile devices not receiving the initial transmission of an alert, as well as ensure that people entering an alert's target area after the initial transmission have a chance to receive it.[191] We seek comment on this belief and the tentative conclusions that support it. Will the routine rebroadcast of WEA messages improve the rate at which people within an alert's target area receive messages that are intended for them? Will it improve the rate at which people entering the target area after the alert's initial transmission receive WEA messages? Will it improve WEA's resilience to ephemeral service disruptions that may coincide with an alert's transmittal?

57. Is at least once every sixty seconds the right periodicity for the rebroadcast of WEA messages, balancing the need for timely, reliable alert delivery against the potential network load? The fact that at least one Participating CMS Provider already rebroadcasts each WEA message every sixty seconds supports our belief that compliance with this requirement would be both technically feasible and reasonable.[192] How do Participating CMS Providers that rebroadcast WEA messages every sixty seconds manage bandwidth resources on the control channel on which they transmit WEA messages, particularly when they receive multiple inbound alerts in quick succession? Are there any circumstances in which Participating CMS Providers should be allowed to retransmit WEAs at a periodicity other than at least once per minute throughout an alert's active period?

58. To further mitigate the risk of duplicate alerts, we seek comment on whether Participating CMS Providers should cease retransmission of WEA messages with a 24-hour active period five minutes before the end of that period. We are aware of incidents in which the transmission of WEA messages near the end of a 24-hour active period has resulted in mobile devices displaying duplicate alerts.[193] In these circumstances, differences between how the CMS network and mobile devices determine the age of

(Continued from previous page)

[189] *See Wireless Emergency Alerts; Amendments to Part 11 of the Commission's Rules Regarding the Emergency Alert System*, PS Docket Nos. 15-91, 15-94, Further Notice of Proposed Rulemaking, 38 FCC Rcd 3739, 3767-68, at para. 54 (2023) (*2023 WEA FNPRM*) ("Should we require Participating CMS Providers to retransmit alert messages at one-minute intervals throughout an alert's active period, as AT&T currently does?").

[190] *See* FCC, Report: August 11, 2021 Nationwide WEA Test at 18-19 (2021), https://docs.fcc.gov/public/attachments/DOC-378907A1.pdf.

[191] *See* Language and Accessibility in Alert & Warning Workgroup Comments, PS Docket Nos. 15-91 and 15-94, at 6 (rec. July 20, 2023) (LAAWW 2023 WEA FNPRM Comments); Verizon Comments, PS Docket Nos. 15-91 and 15-94, at 4 (rec. July 21, 2023) (Verizon 2023 WEA FNPRM Comments); Michigan Operations Management Section Comments, PS Docket No. 15-94, at 5 (rec. July 21, 2023) (Michigan OMS 2023 WEA FNPRM Comments); Alliance for Telecommunications Industry Solutions Comments, PS Docket Nos. 15-91 and 15-94, at 26 (rec. July 21, 2023) (ATIS 2023 WEA FNPRM Comments).

[192] Previous comments in PS Docket Nos. 15-91 and 15-94 support a sixty second interval. ATIS favored rebroadcasting alerts at regular, one-minute intervals, as did Verizon, although Verizon expressed a preference to apply this policy only for "the first 15 minutes of an alert's active period" to "provide alert originators and consumers alike a more consistent experience across different service providers while enabling wireless networks to efficiently manage multiple inbound alerts from" IPAWS. ATIS 2023 WEA FNPRM Comments at 32; Verizon 2023 WEA FNPRM Comments at 4.

[193] On January 5, 2025, the Kansas Department of Emergency Management issued a WEA that was set to expire in twenty-four hours. Just after the alert expired, duplicate alerts were presented on some mobile devices. Carina Branson, *Emergency alert message wasn't supposed to be sent out again* (Jan. 6, 2025), https://www.ksn.com/weather/weather-stories/emergency-alert-message-wasnt-supposed-to-be-sent-out-again/.

an alert can cause devices to purge their memory of 24-hour-old alerts too early and therefore "forget" that they have already displayed an incoming alert to the user. Is stopping retransmission of a WEA message before the end of its active period the best or only way to mitigate this risk of duplicate messages? Is it appropriate for us to permit Participating CMS Providers to implement a buffer period at the end of their retransmission of WEA messages with a 24-hour active period, and if so, is five minutes the right length for that buffer? We seek comment on any public safety or technical concerns that this approach may implicate.

C. Improving the Accuracy of Alert Geotargeting

59. As part of our reexamination of EAS and WEA, we sought comment on which transmission capabilities were needed for an alert and warning system to meet its objectives.[194] Commenters widely recognize that accurate geotargeting is "critical" to accomplishing alerting systems' goals, and they overwhelmingly support improving those capabilities.[195] King County comments that "[w]e strongly agree that geographic targeting is a necessity for a modern alerting system."[196] Sonoma DEM comments: "Geographic targeting is also critical. Alerts should be as precise as possible to reach only those at risk."[197] Art Botterell writes that "[m]embers of the public rarely object to a warning that is relevant to them, at their location and in their circumstances. . . . The best mitigation is to improve the targetability of warning alerts to minimize alert delivery to people for whom the alerts are not relevant."[198]

60. Commenters also suggest that problems with geographic accuracy unfortunately may be undermining alerting objectives, with the Harris County, Texas Office of Homeland Security & Emergency Management (Harris County) observing that the public is being "inundated with messages that are not relevant to them."[199] While the California Governor's Office of Emergency Services states that "[t]his [problem] is particularly evident in cities, where there can be overshoot of messages in densely populated areas,"[200] Alaska resident Shawn Williams observes that geotargeting overshoot can

---

[194] *Alerting Modernization NPRM*, 40 FCC Rcd at 6701, para. 12.

[195] Vergara Alerting Modernization NPRM Reply at 1; *see also* Botterell Alerting Modernization NPRM Comments at 4; Hamilton Bean Comments, PS Docket No. 25-224, at 11 (rec. Aug. 22, 2025) (Bean Alerting Modernization NPRM Comments) ("When accuracy or precision falls short, trust can erode, undermining both system use and public response."); Lavrov Alerting Modernization NPRM Reply at 1; NYCEM Alerting Modernization NPRM Comments at 5; Washington EMD Alerting Modernization NPRM Comments at 6-7; Oregon Department of Emergency Management Comments, PS Docket No. 25-224, at 2 (rec. Sept. 24, 2025) (Oregon DEM Alerting Modernization NPRM Comments); Sonoma DEM Alerting Modernization NPRM Comments at 3; California Governor's Office of Emergency Services Comments, PS Docket No. 25-224, at 2 (rec. Sept. 25, 2025) (Cal OES Alerting Modernization NPRM Comments); King County Office of Emergency Management Comments, PS Docket No. 25-224, at 2 (rec. Sept. 24, 2025) (King OEM Alerting Modernization NPRM Comments); ATIS Alerting Modernization NPRM Comments at 14; Accessibility Organizations Alerting Modernization NPRM Comments at 5.

[196] King OEM Alerting Modernization NPRM Comments at 2.

[197] Sonoma DEM Alerting Modernization NPRM Comments at 3; *see also* Cal OES Alerting Modernization NPRM Comments at 2 ("Improve current geo-target capabilities of alerting during incidents. Alerts don't always reach the right people. This is particularly evident in cities, where there can be overshoot of messages in densely populated areas.").

[198] Botterell Alerting Modernization NPRM Comments at 4; *see also* Vergara Alerting Modernization NPRM Reply at 1 ("[G]eographic precision of alerts is critical." "'Alert fatigue' can cause people to ignore or disable warnings altogether."); Lavrov Alerting Modernization NPRM Reply at 1 ("[G]eo targeting should be precise to reduce alert fatigue. Messages should reach only the affected area with minimal overshoot.").

[199] Harris County Alerting Modernization NPRM Comments at 5.

[200] Cal OES Alerting Modernization NPRM Comments at 2.

be equally pernicious in rural areas.[201] When people are inundated with alerts and warnings that they do not perceive as relevant to them, it can "dilute urgency," "trust can erode," and "alert fatigue" can occur.[202] Consequently, people may ignore EAS and WEA messages that *are* intended for them or disable WEA warnings altogether. APCO states that "alert originators are less likely to use alerting systems" because of the negative consequences of poor geotargeting.[203] The New York City Emergency Management Department's comment stands for the corollary premise that "the more precise . . . [emergency alerting] can be, the more it will be used by alert originators."[204] Similarly, the Sonoma DEM states that the geotargeting of "[a]lerts should be as precise as possible to reach only those at risk, while allowing modest overshoot to capture travelers entering hazardous areas."[205] In light of these concerns, in the sections below, we propose and seek comment on measures to improve the accuracy of geotargeting for both WEA and EAS.

1. Strengthening WEA Geotargeting by Eliminating Outdated Exceptions

61. Commenters offer several suggestions on ways to improve WEA geotargeting.[206] We propose to implement these suggestions by eliminating the existing exceptions to the Commission's WEA geotargeting requirements that allow more than 0.1 of a mile of overshoot in some circumstances.[207] While Participating CMS Providers are required to deliver WEA messages to "100 percent of the target area with no more than 0.1 of a mile overshoot,"[208] our rules allow for exceptions for "network infrastructure [that] is technically incapable of matching the specified target area."[209] The Commission has provided a non-exhaustive list of circumstances in which a Participating CMS Provider's network

[201] Shawn Williams, PS Docket No. 25-224 at 1 (rec. Aug. 11, 2025).

[202] Washington EMD Alerting Modernization NPRM Comments at 6-7; Bean Alerting Modernization NPRM Comments at 11; Vergara Alerting Modernization NPRM Reply at 1; NYCEM Alerting Modernization NPRM Comments at 5; Lavrov Alerting Modernization NPRM Reply at 1; Oregon DEM Alerting Modernization NPRM Comments at 2.

[203] APCO Alerting Modernization NPRM Reply at 11-12.

[204] NYCEM Alerting Modernization NPRM Comments at 5.

[205] Sonoma DEM Alerting Modernization NPRM Comments at 3.

[206] *See* APCO Alerting Modernization FNPRM Reply at 11 (urging the Commission to enforce its existing WEA geo-targeting requirements); County of San Diego Office of Emergency Services Comments, PS Docket Nos. 15-91 and 15-94, at 4 (rec. Jul. 20, 2023) (San Diego OES 2023 WEA FNPRM Comments) (recommending that the Commission sunset "exemptions for legacy mobile equipment/services"); King County Emergency Management Comments, PS Docket Nos. 15-91 and 15-94, at 4 (Jul. 21, 2023) (King OEM 2023 WEA FNPRM Comments); Michigan OMS 2023 WEA FNPRM Comments at 5 (recommending that receipt of a WEA prompt a device to get fresh location data, like it does upon placing a 911 call); Washington EMD Alerting Modernization NPRM Comments at 6-7 (recommending that WEA support native map integration, a requirement that we have already adopted, and that Participating CMS Providers "provide validation and feedback tools so originators can refine their targeting").

[207] *See* 47 CFR § 10.450(a). In 2023, the Commission sought comment on a similar proposal. *2023 WEA FNPRM*, 38 FCC Rcd at 3766, para. 49. This FNPRM remains pending. *See, e.g.*, King OEM 2023 WEA FNPRM Comments at 4; LAAWW 2023 WEA FNPRM Comments at 6 ("LAAWW recommends sunsetting exemptions for legacy mobile equipment/services."); Colorado Alerting Authorities Comments, PS Docket Nos. 15-91 and 15-94, at 6 (rec. July 21, 2023); Michigan OMS 2023 WEA FNPRM Comments at 4; County of San Diego OES 2023 WEA FNPRM Comments at 4-5. *But see* T-Mobile Comments, PS Docket Nos. 15-91 and 15-94, at 11-12 (rec. July 21, 2023); ATIS 2023 WEA FNPRM Comments at 27 (urging the Commission to "consider all implications if it requires location services to always be enabled for WEA" and encouraging the Commission to explore alternatives).

[208] 47 CFR § 10.450(a).

[209] *Id.*

may be considered to be "technically incapable" of matching the target area, including legacy networks and legacy mobile devices and mobile devices with location services disabled.[210] Even though technically incapable networks are nonetheless required to deliver WEA messages to their best approximation of the target area,[211] the Commission and its federal partners frequently receive complaints that WEA messages are being received outside of the target area.[212] As discussed above, this causes alert fatigue and diminishes the usefulness of EAS and WEA. We believe that eliminating these exceptions will reduce overshoot and make WEA more accurate, which, in turn, will make WEA a more predictable tool that will provide greater confidence to alert originators that alerts will be seen by, and only by, the intended audience. We seek comment on these views.

62. *Exemptions for Legacy Networks and Devices*. We propose to eliminate the geotargeting exception for legacy networks and devices. When the Commission adopted the current geotargeting requirements in 2018, it expected that these exceptions would be time-limited as legacy networks shut down and older devices were churned out of the market.[213] We understand that many Participating CMS Providers either have already retired or are actively retiring their 2G and 3G networks.[214] Which, if any, currently deployed networks cannot support geotargeting as currently described in our rules? To what

[210] *Id.* The other listed "exception" is for "when the target area is outside of the Participating CMS Provider's network coverage area." Unlike the exceptions for legacy infrastructure and devices, and locations services being disabled, which allow for overshoot that goes beyond 0.1 of a mile, the exception for "when the target area is outside of the Participating CMS Provider's network coverage area" addresses a separate aspect of the geo-targeting requirement, that WEA messages be delivered to "100% of the target area." Although included as an exception, it would not be reasonable to expect a Participating CMS Provider to deliver WEAs outside its service area. In our proposed rules, we maintain the idea that Participating CMS Providers are not expected to deliver WEAs outside of their coverage areas by limiting the delivery and display requirement to "100 percent of opted-in WEA-capable mobile devices *that are connected to its network* and located in the Alert Message's target area" (emphasis added).

[211] *Id.* ("If some or all of a Participating CMS Provider's network infrastructure is technically incapable of matching the specified target area, then that Participating CMS Provider must deliver the Alert Message to an area that best approximates the specified target area on and only on those aspects of its network infrastructure that are incapable of matching the target area.").

[212] For example, on June 18, 2024, the Massachusetts Emergency Management Agency issued a statewide WEA message regarding a 911 outage. The alert did not specify the originator and was received by people in nearby states, causing authorities in neighboring states to issue their own WEA message stating that the 911 outage did not impact their state. *See e.g.,* Marlene Lenthang, *911 system goes down statewide in Massachusetts* (June 18, 2024), https://www.nbcnews.com/news/us-news/911-system-goes-statewide-massachusetts-rcna157786 ("Some Connecticut, New York and Maine residents erroneously received the same wireless emergency alert notifying them of a 911 outage. Officials from all three states clarified the alerts was exclusively meant for Massachusetts residents."); NBC Connecticut, *Connecticut residents mistakenly receive alert about Massachusetts 911 outage* (June 18, 2024), https://www.nbcconnecticut.com/news/local/connecticut-residents-mistakenly-receive-alert-about-massachusetts-911-outage/3316156/; Ethan Andrews, *Massachusetts emergency text alerts mistakenly sent to Mainers* (June 18, 2024), https://www.bangordailynews.com/2024/06/18/state/state-police-courts/mainers-mistakenly-sent-massachusetts-emergency-text-alerts/.

[213] *See 2018 Second WEA R&O*, 33 FCC Rcd at 1327, para. 9 & n.45 (stating that "[w]e expect network infrastructure constraints to more granular geo-targeting will be a time-limited issue."); *see also 2023 WEA FNPRM*, 38 FCC Rcd at 3766, para. 49.

[214] *See, e.g.*, T-Mobile, *T-Mobile Network Evolution*, https://www.t-mobile.com/support/coverage/t-mobile-network-evolution (last visited Feb. 5, 2026) (indicating performance coverage and performance changes in T-Mobile's 2G network in February 2025, and that T-Mobile and Sprints 3G had been retired in 2022); Mike Dano, *More 2G and 3G shutdowns loom in the US* (Nov. 28, 2023), https://www.lightreading.com/2g-3g-4g/more-2g-and-3g-shutdowns-loom-in-the-us (reporting USCellular was turning off its 3G network on Jan. 14, 2024, Cellcom was shuttering its 2G network in Dec. 2023, and its 3G network in Mar. 2024, AT&T discontinued 2G service in 2017, Verizon discontinued its 2G service in 2020).

extent do Participating CMS Providers and their subscribers continue to rely on these networks for the delivery of WEA messages? If any Participating CMS Providers continue to rely upon networks that still cannot be upgraded to support today's WEA geotargeting requirements, we seek comment on those providers' timelines for sunsetting those networks. To what extent have mobile devices that do not support today's geotargeting requirements already churned out of the market?

63. *Exemption for Disabled Location Services.* We propose to eliminate the geotargeting accuracy exception for devices with location services disabled. As currently implemented, disabling location services on a WEA-capable mobile device will prevent the device from conducting a geofence and will therefore cause it to present every WEA it receives to the subscriber, even if the device is located far outside of the target area.[215] When the Bureau partnered with 37 emergency management agencies across the country to conduct localized WEA tests in 2022, it found that more than two thirds of geofencing-capable devices failed to correctly suppress the alert.[216] The Bureau also found that at least some of these failures likely occurred because devices had location services disabled.[217] Wireless providers confirmed to Bureau staff that the main cause of overshoot in devices that were capable of performing a geofence was the devices' location services being disabled. Are disabled location services a primary cause of targeting failures on devices that are otherwise technically capable of geofencing, as this evidence suggests? If not, what else could account for these failures? Alternatively, is it possible that device-based geofencing, as widely implemented by original equipment manufacturers and Participating CMS Providers, is not capable of consistently meeting the Commission's accuracy requirement?

64. To reduce the number of geotargeting failures, the King County Office of Emergency Management recommends "that location services should be forced on when a device receives a WEA – the same as for 911 calls – to determine whether an alert is applicable to the device holder."[218] We believe that this approach would greatly improve the accuracy of WEA overall and would better align with the expectations of consumers, who likely expect WEA to be accurate regardless of their device's location settings. We seek comment on this view. Would requiring mobile devices to force location services on when a WEA is received reduce WEA overshoot? When users purchase a geofencing capable device and disable location services, do they expect to receive accurate, geographically relevant alerts? Similarly, do purchasers of WEA-capable mobile devices who disable location services have an expectation of privacy that precludes the use of that information for purposes of public safety? Are subscribers aware that turning off location services may result in them receiving WEAs that were not intended for them? Could receiving such geographically irrelevant alerts cause subscribers to opt out of receiving WEA messages? How would mobile devices need to be technically modified to support the ability to turn on location services when a WEA is received?

---

[215] Participating CMS Providers use device-based geofencing to comply with the geographic targeting requirements of Section 10.450(a), which limits overshoot to 0.1 miles on technically capable infrastructure and devices. 47 CFR § 10.450(a). Device-based geofencing compares the mobile device's location with the coordinates included in the WEA message. If the device is within the target area, the device will present the alert. If not, the device will suppress presentation of the alert. If, however, location services are disabled, the device cannot determine its location and cannot perform a geofence. If a geofencing-capable device receives an alert, and it cannot perform a geofence, it will present the alert.

[216] FCC, September 2022 WEA Performance Exercise at 6 (2023), https://docs.fcc.gov/public/attachments/DOC-392829A1.pdf (WEA Performance Exercise Report).

[217] *Id.* at 3 ("To reflect real-world device usage, volunteers were not specifically instructed to enable or disable the Location Services on their mobile device . . . . We note that not having Location Services enabled may account for why some normally-geofencing devices failed to suppress the test alert messages.").

[218] King OEM Alerting Modernization NPRM Comments at 2.

65. Previously, several commenters raised privacy concerns related to eliminating this exception. ATIS states that "[u]nlike 9-1-1, WEA is not a user-initiated request for assistance at the time of the event. . . . consumer trust and privacy, are considerations on always requiring location services to be enabled that may result in consumers' choosing to opt-out of WEA."[219] The Electronic Frontier Foundation echoes this concern, stating that "[a]n individual's ability to opt-out of geolocation services and thus be able to move about daily life without being systematically tracked is also a matter of safety."[220] According to King County Office of Emergency Management, however, "[i]f those location services data are not shared off the device, there would be no privacy concerns."[221] We believe King County is correct that mobile device location data is never shared outside of the device for the purpose of WEA geofencing.[222] Can these concerns be addressed by placing limitations on how location information that is collected for WEA can be used? For example, we propose that when the receipt of a WEA message turns on a device's locations services, the acquired location information would be prohibited from being used for any purpose other than WEA. We also propose to prohibit Participating CMS Providers from transmitting this location information over their networks. We propose that any location information collected to perform a geofence be deleted immediately after the geofence was performed. If WEA were to be able to turn on and access location services even for those people who have disabled location services on their devices, should we require location services to be disabled immediately after the location information was made available for WEA? When users disable the location services on their mobile device, should they receive a disclosure that doing so will reduce the geotargeting accuracy of WEA messages? Would these measures be sufficient to balance the public safety value of ensuring that location information is always available to WEA while protecting consumers' privacy? Are these measures technically feasible? Are there any additional or alternative measures we should consider to protect the privacy of subscribers and balance those privacy concerns against the benefits of getting accurate WEA messages? For example, should consumers be provided with the option to turn on location services solely for WEA? Should consumers receive a disclosure upon switching location services off on their devices letting them know that it may result in them receiving WEA messages that are not relevant to them?

66. We seek comment on any other technical feasibility concerns attendant to receipt of a WEA prompting mobile devices to obtain a fresh location fix. CTIA states that "such an approach may not be technically feasible given differences in the way [9-1-1 and WEA] operate."[223] What specific technical differences between how WEA and 911 operate pose a challenge? Could these challenges be overcome through appropriate standards and mobile device software updates? Apple airs an additional concern about the implication of location services always being on for mobile device battery life, stating that "GPS usage—particularly in areas with weak signals—can be very power intensive" so "if an

---

[219] ATIS 2023 WEA FNPRM Comments at 27; *accord* Apple, Inc. Reply, 15-91, 15-94 at 9-10 (rec. Aug. 21, 2023) (Apple 2023 WEA FNPRM Reply) (stating that the interest in improved WEA geo-targeting should be "balanced against preferences of users who would decide not to receive WEA messages altogether if their location preferences are not respected."); CTIA Comments, PS Docket No. 15-91 and 15-94, at 13-14 (rec. Jul. 21, 2023) (CTIA 2023 WEA FNPRM Comments) ("[D]evice manufacturers, OS vendors, and Participating CMSPs also may need to adjust data collection and access, as well as security and privacy policies.").

[220] Electronic Frontier Foundation Reply, PS Docket Nos. 15-91 and 15-94, at 1-2 (rec. Aug. 18. 2023).

[221] King OEM 2023 WEA FNPRM Comments at 4; *see also* Michigan OMS 2023 WEA FNPRM Comments at 4 (recommending that geo-fencing location data be used for WEA, but that it not be shared with any other party).

[222] King OEM 2023 WEA FNPRM Comments at 4; *see also* FCC, Wireless Emergency Alerts (WEA), https://www.fcc.gov/consumers/guides/wireless-emergency-alerts (last visited May 30, 2026) ("Does WEA track my location? No. WEA is not designed to – and does not – track the location of anyone receiving a WEA alert.").

[223] CTIA 2023 WEA FNPRM Comments at 13 (discussing the Commission's 2023 proposal to require location services for WEA to operate similar to 911 calling).

emergency involves power outages, a consumer might reasonably choose to conserve device battery life over the ability to receive more targeted alerts."[224] We seek comment on whether our proposal to require location services to be disabled immediately after the location information was made available for WEA would address this concern. We seek comment on any refinements to our proposal that might be appropriate to preserve mobile device or network resources while improving WEA geotargeting's performance.

67. *Exemption for Geocodes.* We propose to require WEA messages that geotarget alerts by using FIPS codes, which are also referred to as "geocodes," to achieve the same level of accuracy as alerts sent using a polygon or circle. Today, if an alerting authority targets an alert using a FIPS code instead of a polygon or circle, the Commission's rules do not require the alert to comply with the 0.1 mile limit on geographic overshoot.[225] As a result, according to CTIA, "the alert will not contain the geographic coordinates necessary to activate [device-based geofencing]. . . ."[226] The result will be that any mobile device that receives such a WEA message will present the alert to the subscriber, even if the device is far outside the target area.[227] Requiring WEA messages that use FIPS codes to be as accurately targeted as alerts that use circles or polygons would greatly reduce instances of geographic overshoot, making WEA a more useful tool for alert originators and better ensuring that subscribers only receive alerts that are relevant to them. We seek comment on these views.

68. We believe that it is technically feasible for WEA messages that use FIPS codes to be as accurate as messages that use circles or polygons. When the Commission adopted the enhanced geotargeting requirement, it was persuaded that mobile devices could not yet perform a geofence using a county code because there was no authoritative mapping of U.S. counties to polygon coordinates and because of technical concerns related to the transmission of polygon coordinates that track geocodes and the conversion of geocodes to polygons at the mobile device.[228] Since then, the U.S. Census Bureau has published a mapping of county codes to polygon coordinates.[229] This freely available database may enable IPAWS or participating wireless providers to translate a geocode into a polygon before it reaches a mobile device so that the mobile device can use it for the purpose of geofencing using available polygon smoothing techniques. Would increasing the limit on the number of vertices that can be used to describe a polygon, as requested by the NWS and Colorado 911 Authorities and Public Safety Agencies,[230]

---

[224] Apple 2023 WEA FNPRM Reply at 10.

[225] *See* 47 CFR § 10.450(a).

[226] CTIA Alerting Modernization NPRM Comments at 19; *see* ATIS 2023 WEA FNPRM Comments at 14-15 ("Alerting Authorities should use a polygon or circle, when possible, to define the alert area, rather than specifying the alert area using geocodes, in order to trigger [device-based geofencing] and combat broadcast overshoot.").

[227] *See supra* para. 63 & n.215.

[228] *See* Letter from Thomas Goode, General Counsel, ATIS, to Marlene Dortch, Secretary, FCC, PS Docket No. 15-91, at 1 (filed Jan. 23, 2018) (stating that transmitting polygon coordinates that track geocodes exceed the 100-coordinate limit for the polygon of the message as specified in standards, and doing the conversion at the device would require device storage and periodic updates); Letter from Matthew Gerst, Assistant Vice President, Regulatory Affairs, CTIA, to Marlene Dortch, Secretary, FCC, PS Docket No. 15-91, at 5 (filed Jan. 23, 2018). *But see* National Weather Service Reply, PS Docket No. 15-91, at 2 (rec. Jan. 9, 2017); Letter from Jeffrey Cohen, Chief Counsel, APCO, to Marlene Dortch, Secretary, FCC, PS Docket No. 15-91, at 1-2 (filed Jan. 18, 2018) (supporting the Commission's inclusion of geofencing for WEA messages with the target area specified by a geocode in the public draft of the item).

[229] *See* U.S. Census Bureau, Cartographic Boundary Files – Shapefile, https://www.census.gov/geographies/mapping-files/time-series/geo/carto-boundary-file.html (last visited June 1, 2026); Michael Minn, *Geospatial Data from the US Census Bureau* (Mar. 9, 2026), https://michaelminn.net/tutorials/gis-census/#arcgis-pro-tiger-join.

facilitate converting geocodes into coordinates, as well as make it easier for alert originators to use polygons? What challenges or drawbacks to increasing the number of vertices exist and how could they be addressed? Alternatively, polygons relevant to the user's location could be automatically retrieved, stored locally on mobile devices, and used when a WEA message is received that includes a FIPS code that matches a stored polygon. Would these approaches be successful at improving the accuracy of WEA messages that use FIPS codes? Could available polygon smoothing, simplification, encoding, or compression techniques address any concerns about fitting polygons derived from geocodes in WEA transmissions?[231] How much mobile device storage would be required to maintain a mapping of county geocodes to corresponding polygons? Could industry take steps to minimize this burden, such as by retrieving polygons for geocodes specified in a WEA message upon receipt of the message or as a background task when a mobile device moves into a new region? Are there any additional methods that could be implemented to improve the accuracy of WEA messages that use FIPS codes? What are the benefits and trade-offs of these approaches. Should we require Participating CMS Providers to implement a specific method for improving the accuracy of WEA messages that use FIPS codes, or should we remain agnostic to how accuracy is improved so long as these messages are no longer received more than 0.1 miles outside of the target area?

69. We seek comment on any other causes of geographic overshoot that arise from the design or technical implementation of WEA. What steps can we take to eliminate or mitigate these other causes of geographic overshoot? Are there any additional or alternative steps that we can take to reduce or eliminate instances of geographic overshoot?

2. Incentivizing EAS Geofencing

70. We propose to improve the accuracy of EAS geotargeting by permitting, but not requiring, EAS Participants to take advantage of detailed location information that is often available in CAP EAS messages. Because EAS Participants are currently restricted to targeting alerts by using county codes,[232] it can be difficult for them to identify alerts that are targeted to very small geographic areas. Even if they could identify these situations, EAS Participants transmit EAS alerts to facilities' entire service areas, which are often large.[233] As DAS comments, "[b]y design, once an EAS alert is issued, everyone watching that channel receives it."[234] As REC Networks states, "since EAS was originally intended for national messages, more localized messages are just an afterthought."[235] Alerting authorities and EAS equipment manufacturers take the view that EAS is being underutilized because of these limited geotargeting capabilities.[236] For example, during the January 2025 Los Angeles County wildfires alerting

(Continued from previous page)

[230] NWS Alerting Modernization NPRM Comments at 2; Colorado Alerting Modernization NPRM Comments at 6.

[231] *See*, *e.g.*, Martin Fleischmann, *Line simplification algorithms* (Apr. 27, 2020), https://martinfleischmann.net/line-simplification-algorithms/; Chandrajit L. Bjaj & Daniel R. Schikore, *Topology preserving data simplification with error bounds*, 22 Computers. & Graphics 3 (1998), https://www.sciencedirect.com/science/article/abs/pii/S0097849397000794.

[232] 47 CFR § 11.31(e).

[233] *See* REC Networks Alerting Modernization NPRM Comments at 4-5.

[234] DAS Alerting Modernization NPRM Comments at 30; *see also* Sage Alerting Systems, Inc. Reply, PS Docket No. 25-224, at 1 (rec. Nov. 17, 2025) (Sage Alerting Modernization NPRM Reply).

[235] REC Networks Alerting Modernization NPRM Comments at 6.

[236] *See* DAS Alerting Modernization NPRM Comments at 21; Sage Alerting Modernization NPRM Reply at 1; Botterell Alerting Modernization NPRM Comments at 2; Snohomish DEM Alerting Modernization NPRM Comments at 2 ("[EAS] may not be the most effective choice due to the nature of our regional emergencies. For instance, in Snohomish County, issuing a Tsunami alert through EAS would require notifying the entire county,

(continued….)

authorities did not use EAS to transmit evacuation orders to avoid delivering the alert to people for whom it was not intended, which could have caused unnecessary panic and potentially moved people into—rather than out of—harm's way. King County Office of Emergency Management "would like to see similar [WEA-like geotargeting] capabilities developed for EAS. Currently sending an EAS in our area would alert six counties, theoretically reaching over 8,000 square miles and 4.5 million people. This is far too broad for any practical purpose."[237] DAS states that improvements to EAS geotargeting "could reduce alert fatigue and make alerts more relevant."[238] Because many CAP EAS messages include WEA-supported circles or polygons in addition to county codes,[239] we believe that the most immediate approach to improving EAS geotargeting would be to allow EAS Participants to use those circles and polygons as an alternative to county codes.

71. We believe this approach will allow EAS Participants to more precisely identify the geographic area to which a given CAP EAS alert is relevant and be better informed as to whether it makes sense to transmit the alert to their audiences. This helps EAS Participants strike a balance between transmitting EAS messages to affected communities while minimizing the deleterious effects of alert fatigue. We seek comment on this view. Do EAS Participants have an interest in using circles and polygons when making decisions about which state or local alerts to transmit? How would EAS Participants integrate circular and polygonal targets into their decision-making about whether to transmit an alert? Will permitting targeting via polygons encourage innovation and lead to the deployment of new capabilities that can potentially make alerts more accurate? If so, what kinds of capabilities might be developed? Can circles and polygons assist EAS Participants in delivering alerts to only a portion of their audience instead of all of it, and if so, are there types of EAS Participants that are better positioned to accomplish this than others? Do EAS equipment manufacturers believe that there is sufficient interest in these capabilities to financially justify bringing those capabilities to market? Do the proposed changes to our rules provide sufficient flexibility to EAS Participants that may want to consider using the coordinates in a CAP message to determine whether to broadcast an EAS alert? If not, what alterations are necessary to facilitate and encourage EAS Participants to take advantage of the coordinate information in CAP-based EAS alerts? As an alternative approach, should the Commission require, instead of merely allow, EAS Participants to use circles and polygons when targeting alerts?

72. Several commenters tout the broadcast television standard ATSC 3.0 as a means of improving emergency alert geotargeting. When the Commission authorized ATSC 3.0 as the next generation broadcast television standard in 2017, it observed that the standard would offer enhanced geotargeting of emergency alerts and required ATSC 3.0 broadcasters to comply with the EAS rules.[240] The Advanced Warning and Response Network (AWARN) Alliance, ATSC: The Broadcast Standards Association, Sinclair, Inc., NAB, and the Oregon Department of Emergency Management advocate for increased use of ATSC 3.0 as a way to transmit geotargeted emergency alerts.[241] Would our proposal

(Continued from previous page)
which may not be necessary or efficient in certain situations. This limitation makes it challenging to use EAS for targeted alerts fully.").

[237] King OEM Alerting Modernization NPRM Comments at 3.

[238] DAS Alerting Modernization NPRM Comments at 23.

[239] Legacy EAS messages do not contain geo-targeting information more accurate than the county codes.

[240] *See Authorizing Permissive Use of the "Next Generation" Broadcast Television Standard*, GN Docket No. 16-142, Report and Order and Further Notice of Proposed Rulemaking, 32 FCC Rcd 9930, 9971, para. 80 (2017); 47 CFR § 73.3801(b)(1) ("The programming aired on the ATSC 1.0 simulcast signal must be 'substantially similar' to that aired on the ATSC 3.0 primary video programming stream . . . " except for enhanced capabilities, including "[h]yper-localized content (e.g., geo-targeted weather, targeted emergency alerts . . . ").

[241] AWARN Alliance Comments, PS Docket No. 25-224, at 2-3 (rec. Sep. 23, 2025); ATSC: The Broadcast Standards Association Comments, PS Docket No. 25-224, at 2 (rec. Sept. 25, 2025); Oregon DEM Alerting
(continued….)

improve the ability of EAS Participants relying on ATSC 3.0 to more accurately target alerts to audience members in specific geographic areas? If so, how would these EAS Participants conduct this targeting?

73. *Improving Target Area Descriptions in EAS Alerts—Partial County Alerting.* We propose to delegate authority to the Public Safety and Homeland Security Bureau to consider and adopt new EAS location codes that will make EAS messages more understandable to local communities.[242] NWS has expressed concerns that existing location names can be potentially confusing or misleading to the public.[243] For example, in Monroe County, Florida the "southwest" subcounty code might be used for alerts relevant to Key West.[244] People in Key West, however, would be confused by an EAS message that described the target area as "Southwest Monroe County" because they may not associate that description with Key West. To provide greater flexibility to alerting authorities, additional location names could be encoded and transmitted in legacy EAS messages using currently unused combinations of EAS location codes.[245] For example, the American National Standards Institute (ANSI) standard and the Commission's EAS rules establish that the code for Monroe County, Florida is "12087."[246] The code "12088," on the other hand, is currently unused and could potentially be assigned to "Key West" for EAS purposes.

74. We expect that this approach will increase the authoritativeness and effectiveness of EAS messages by providing alerting authorities with a more flexible list of locations for targeting alerts. More commonly used location names would be less likely to confuse alert recipients about whether an alert is intended for them and would likely provide greater certainty about whether a received alert is intended for the recipient. We seek comment on our proposal and these views. In what other scenarios might it be beneficial for alerting authorities to be able to use more flexible location codes? Are these scenarios common enough to justify creating a streamlined process for adopting new location codes? What risks arise from creating location codes for EAS in this fashion? Should we consider an alternative technical implementation, such as expanding the county subdivision character of six-digit geocodes to allow the use of letters, which could then be assigned to specific locations? Are there more effective ways to reduce consumer confusion about the locations to which EAS messages are targeted that we should consider?

75. We believe that delegating authority to the Bureau to seek comment on and adopt new EAS location codes will promote efficiency. Under this process, alerting authorities or State Emergency

(Continued from previous page)
Modernization NPRM Comments at 4-5; Sinclair Alerting Modernization NPRM Comments at 1 ("ATSC 3.0 also allows alerts to be geotargeted so only those who are in harm's way receive an alert"); NAB Reply, PS Docket No. 25-224, at 15 (rec. Nov. 18, 2025); *see also* Digital Alert Systems, Inc. Reply, PS Docket No. 25-224, at 3-4 (rec. Nov. 13, 2025) (DAS Alerting Modernization NPRM Reply) (" . . . the Commission should endorse the permissive use of ATSC 3.0's . . . [Advanced Emergency Information (AEI)] service as a voluntary enhancement layer, promote interoperability testing with EAS/WEA, and ensure that any deployment remains voluntary."); Kibin Alerting Modernization NPRM Comments at 1 ("Replace the Cell Broadcast technology for the WEA with the ATSC 3.0 data transmission technology . . . Consider merging WEA into the EAS system with ATSC 3.0 technology.").

[242] *See* 47 CFR §11.31(c).

[243] National Weather Service, *NWS Partial County Alerting information* https://www.weather.gov/pca/ (last visited Apr. 27, 2026).

[244] *See* 47 CFR §11.31(c) (explaining the "PSSCCC" format of EAS geocodes and noting that "P defines county subdivisions as follows: 0 = all or an unspecified portion of a county, 1 = Northwest, 2 = North, 3 = Northeast, 4 = West, 5 = Central, 6 = East, 7 = Southwest, 8 = South, 9 = Southeast").

[245] *See id.*

[246] *See* FCC, *Federal Information Processing System (FIPS) Codes for States and Counties* https://transition.fcc.gov/oet/info/maps/census/fips/fips.txt (last visited Apr. 27, 2026); *see also* U.S. Census Bureau, *American National Standards Institute (ANSI), Federal Information Processing Series (FIPS), and Other Standardized Geographic Codes* (May 1, 2023), https://www.census.gov/library/reference/code-lists/ansi.html.

Communications Committees would request that the Bureau create a new EAS code for a particular location. We propose that request would be required to include a map with a circle or polygon to identify the geographic area to which the new code would apply, provide reasons why the new code should be created, and explain why the existing location codes are inadequate for members of the public that would receive alerts in that location. The Bureau would request comment on these requests by way of a Public Notice and act upon each request based on the merits presented. We seek comment on this approach.

D. Enhancing Alert Effectiveness

76. In the *Alerting Modernization NPRM*, we sought comment on the kinds of information the nation's alerting system should convey to the public to ensure people take appropriate protective actions, and asked whether there are changes that should be made to how alerts are presented to make them easier for people to understand.[247] We believe that emergency alerts will be most effective when they provide people with information that they can quickly and easily understand. Harris County is "strongly in favor of allowing for the inclusion of visual media in WEA messages [as recommended by CSRIC IV because they] enhance understanding and help bridge accessibility gaps."[248] Several other commenters generally support enhanced emergency messaging that includes visual media and recognize its public safety value, which provides additional information, expands accessibility, and improves understanding of how to stay safe, but note that speed and security must come first.[249] The Snohomish DEM cautions that creating and transmitting multimedia content could delay alert delivery.[250]

77. We agree with commenters that using modern technology to enhance alert message content beyond traditional text and audio will benefit public safety but also agree that these enhancements should not come at the expense of other important aspects of emergency alerting. Accordingly, we take a modest first step toward enhanced media emergency alerting by seeking comment on whether to require EAS and WEA messages to include a simple, easily recognizable symbol representing the underlying emergency event. We also seek comment on the USGS's recommendation that the receipt of a WEA earthquake alert should trigger an announcement of the alert message text using text-to-speech.[251]

1. Promoting the Use of Symbols for Alerts

78. We seek comment on whether to require EAS and WEA messages to display standardized symbology that identifies the threat type. We expect that the use of symbols could potentially improve comprehension for people with disabilities and people with limited English reading proficiency, hasten public reactions to alerts, and reduce milling.[252] For example, Notify NYC & Cornell

---

[247] *Alerting Modernization NPRM*, 40 FCC Rcd at 6701, 6703, para. 16.

[248] *See* Harris County Alerting Modernization NPRM Comments at 1, 4; CSRIC IV, Geographic Targeting, Message Content and Character Limitation Subgroup Report (2014), https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_CMAS_Geo-Target_Msg_Content_Msg_Len_Rpt_Final.pdf.

[249] *See* Washington EMD Alerting Modernization NPRM Comments at 9-10; America's Public Television Stations and Public Broadcasting Service Comments, PS Docket No. 25-224, at 19 (rec. Sept. 25, 2025); DAS Alerting Modernization NPRM Comments at 26; Accessibility Organizations Alerting Modernization NPRM Comments at 3 ("Alerts should use plain language that avoids jargon or unexplained acronyms. Multimedia alerts should include audio descriptions, alternate text, a URL link with further information, and ASL resources where appropriate.").

[250] *See* Snohomish DEM Alerting Modernization NPRM Comments at 3.

[251] USGS is the Federal agency responsible for monitoring and notification of earthquakes, volcanic activity, and landslides in the United States and is tasked with providing public warnings of imminent strong earthquake shaking. USGS provides earthquake emergency notices through its earthquake early warning (EEW) system called ShakeAlert® in the states of Washington, Oregon, and California with plans to expand to system to Alaska. In addition to being sent through their proprietary system, ShakeAlert earthquake alerts are also sent via WEA.

Tech have previously found that the use of incident-specific symbols doubled participant comprehension and literacy.[253] We seek comment on these views. The Language & Accessibility for Alerts & Warnings Workgroup, the Oregon Department of Emergency Management, North Carolina Emergency Management et al., and NWS support the inclusion of standardized symbology in EAS and WEA messages.[254] DAS acknowledges that while EAS and WEA function effectively, additional features could enhance the systems and "the Commission should rather look at steps towards including more modest multimedia resources with alerting . . . [which] could consist of further introducing standardized symbology/iconography to accompany EAS and WEA alerts, as well as basic images and graphics that may be carried on an optional basis by appropriate services."[255] DAS further states that "EAS modernization should include supplemental lightweight visuals, such as static graphics, such as the [Visually Integrated Display Symbology (VIDS)] iconography, which add clarity. Static VIDS graphics and symbology offer the greatest increase in relevance for the least additional expense" and that its "experience demonstrates that these enhancements are technically feasible; DASDEC devices already aggregate media and support symbology."[256] FEMA has previously argued that the use of graphical symbols could improve alert message interpretation by individuals with limited English proficiency.[257]

79. DAS and the State Broadcasters Associations recommend a voluntary approach to applying symbols to emergency alerts. DAS believes multimedia enhancements, including standardized symbology, should remain optional in order to preserve the timeliness and reliability of emergency alerts.[258] We seek comment on whether the inclusion of symbols in EAS or WEA messages would necessarily delay or potentially prevent the public's receipt of those messages and, if so, to what extent. Are there implementation approaches to supporting symbols in EAS and WEA messages, such as having them preloaded on end-user devices rather than transmitted along with message text as NWS and Verizon have suggested, that are technically feasible and that could mitigate latency and reliability concerns?[259]

(Continued from previous page)

[252] "Milling behavior includes actions like searching for information regarding the event, talking to others about what to do, and deciding if the alert relates to a danger serious enough to take action." Georgia Tech, *First FEMA PrepTalk: Modernizing Public Warning Messaging* (Mar. 29, 2018), https://wirelessrerc.gatech.edu/first-fema-preptalk-modernizing-public-warning-messaging.html.

[253] *See* New York City Emergency Management Department Comments, PS Docket Nos. 15-91 and 15-94, at 2 (rec. Jul. 20, 2023) ("Soon after these findings, NYCEM began publishing 12 different hazard symbols in 12 different languages via Notify NYC.").

[254] LAAWW Reply, PS Docket No. 25-224, at 2 (rec. Nov. 13, 2025); Oregon DEM Alerting Modernization NPRM Comments at 2; North Carolina Emergency Management et al. Reply, PS Docket No. 25-224, at 2 (rec. Oct. 10, 2025); NWS Alerting Modernization NPRM Comments at 1; *see also* Telecommunications for the Deaf and Hard of Hearing, Inc. et al. Comments, PS Docket Nos. 15-91 and 15-94 at 6-7 (rec. Jul. 21, 2023) ("Including symbols (in addition to or in place of other multimedia content) would 'allow for quicker comprehension and therefore increase accessibility, including for individuals who are deaf, hard of hearing, deafblind, and deaf with mobility issues,'" quoting Telecommunications for the Deaf and Hard of Hearing, Inc. et al, Reply, PS Docket Nos. 15-91 and 15-94, at 5 (filed Jan. 9, 2017)); APCO Comments, PS Docket Nos. 15-91 and 15-94 at 2-3 (rec. July 21, 2023); Regional Disaster Preparedness Organization of the Portland-Vancouver Metro Region, Comments, PS Docket Nos. 15-91 and 15-94 at 3 (rec. Jul. 20, 2023).

[255] DAS Alerting Modernization NPRM Comments at 26; DAS Alerting Modernization NPRM Reply at 3 (arguing enhanced features, including standardized symbology, should remain optional).

[256] DAS Alerting Modernization NPRM Comments at 61-62.

[257] *See 2016 WEA R&O*, 31 FCC Rcd at 11194, para. 131; Letter from Wade Witmer, Deputy Director, IPAWS Division, FEMA, to Marlene Dortch, Secretary, FCC, PS Docket No. 15-91 at 2 (filed June 18, 2015).

[258] DAS Alerting Modernization NPRM Reply at 3.

[259] National Weather Service Comments, PS Docket No. 15-91, at 2 (rec. Jul. 21, 2023) (NWS 2023 WEA FNPRM Comments); Verizon Comments, PS Docket No. 15-91, at 5 (rec. Jul. 21, 2023) ("Verizon also agrees that use of

(continued….)

The State Broadcasters Associations state that "comments [filed in this proceeding] demonstrate that the broadcast industry is continuing to evolve its emergency communications capabilities . . . perhaps in ways alert originators do not yet know or anticipate. These innovations have the potential to add pictorial or video content to broadcast EAS alerts and emergency messages . . ."[260] They recommend the broadcast industry be allowed to evolve public alerting capabilities through continued industry innovation, rather than rulemaking. We seek comment on any innovations EAS Participants or Participating CMS Providers have implemented that may contribute to the potential to include emergency alert symbols in EAS and WEA messages. On what timeframe do EAS Participants and Participating CMS Providers believe that the display of symbols or multimedia content alongside alert messages will become widespread?

80. If we were to require EAS and WEA to integrate a standardized symbol set, we seek comment on which symbol set we should rely upon. For example, should EAS and WEA symbols be based on the National Alliance for Public Safety GIS (NAPSG) Foundation symbol library,[261] which is publicly available at no cost and is supported by FEMA?[262] What other symbol sets should we consider? What are the benefits and drawbacks of each? The Rehabilitation Engineering Research Center for Wireless Inclusive Technologies previously found that, among sixteen "people who were Deaf and primarily used ASL for communication,"[263] the presence of NAPSG symbology did not improve the participants' understanding of either the event or the recommended protective action.[264] Is this representative of what we should expect for the effect on the public generally? We invite commenters to submit into the record any other studies conducted about the use of symbols or iconography in emergency alerts.

81. We also ask commenters to address presentation guidelines for symbols in EAS and WEA, respectively. Is there value in creating a common look and feel among EAS and WEA messages such that the same or similar presentation guidelines should apply to both systems? Or are EAS and WEA so technologically distinct that a similar look and feel for symbols presented via these systems would be impracticable to achieve? We seek comment on how emergency alert symbols should be presented along with EAS and WEA messages. Where should emergency alert symbols be located relative to the display and the alert message text? What size should the symbols be relative to the display? Should symbols have some transparency, particularly for EAS, where the programming content behind them could otherwise be unnecessarily obscured? For how long should an emergency alert symbol persist on an emergency alert display? How should symbols be displayed when there are different types of emergencies pending for the same geographic area simultaneously? Should symbols appear with alert message text and disappear at the end of the visual crawl or when the user dismisses the message? Or should a symbol persist on the display for the entirety of an alert's active period in a discrete but visible location, such as in the corner of the television screen or on a mobile device's lock screen or home screen? We seek comment on whether the persistent presentation of an emergency alert symbol could

(Continued from previous page)
pre-installed infographics and symbols at the device level has merit—though, again, input and engagement from handset manufacturers and solution vendors will be critical.").

[260] State Broadcasters Associations Alerting Modernization NPRM Reply at 3.

[261] NAPSG Foundation, *Symbol Library*, https://www.napsgfoundation.org/all-resources/symbology-library/ (last visited May 6, 2026).

[262] FEMA, *Integrated Public Alert & Warning System (IPAWS) Tips; TIP 36: The IPAWS Symbol Set* (Apr. 2021) https://www.fema.gov/sites/default/files/documents/fema_tip-36-symbology.pdf; NWS 2023 WEA FNPRM Comments at 2 (stating that the NAPSG symbol set could be a useful starting point for studying the effectiveness of emergency alerting symbols).

[263] Georgia Tech et al. Comments, PS Docket No 15-91, at 9 (rec. Apr. 8, 2024).

[264] *Id.* at 11.

bring the existence of an emergency condition to the awareness of people that could otherwise miss it, such as television viewers that tune in during an EAS message's active period but after the EAS visual crawl has already completed and the broadcast has returned to regularly scheduled programming.

82. We seek comment on technical considerations relevant to the presentation of emergency alert symbols. Could this functionality be enabled on WEA-capable mobile devices through a software update? What EAS Participant systems would be involved in the process of displaying an EAS-related symbol on a television screen, and how would those systems display it? What steps would need to be taken for these systems to support this capability? Would any changes to standards be needed to enable symbols to persist on-screen for the duration of the alert's active period?

2. Amplifying WEA Earthquake Alerts

83. The faster the public understands an alert, the faster they can react.[265] This is particularly important during events that occur without prior notice or predication.[266] Accordingly, we seek comment on USGS's recommendation that the receipt of a WEA earthquake alert should trigger a verbal announcement using text-to-speech.[267] While WEA's attention signal and vibration cadence are intended to quickly grab subscribers' attention,[268] no information about the nature of the underlying emergency event is communicated during that time unless a subscriber accesses their device to read the text of the message. Having additional seconds to react can make a significant difference in public safety outcomes during the most time-sensitive, no-notice emergencies, such as earthquakes. USGS believes a text-to-speech verbal announcement of imminent earthquake shaking would provide the fast, actionable information consumers need to take protective action during an earthquake. In support for this view, USGS identifies precedent for spoken emergency alerts from the National Fire Alarm and Signaling Code, which requires in-building private mass notification system emergency alerts (e.g., fire alerts) to include an intelligible audio message along with a visible notification recommendation.[269] USGS argues that social science supports the finding that people respond to speech-based auditory icons and text-to-speech faster than they respond to attention sounds that are not based on speech, which USGS says is key for effective earthquake warnings.[270] We seek comment on USGS's recommendation. If spoken emergency alerts hasten protective actions relative to a generic attention signal in response to in-building fire alerts, does it stand to reason that spoken emergency alerts would similarly hasten protective actions in response to WEA messages? Should we consider requiring additional types of WEA messages to be

[265] *See* USGS Alerting Modernization NPRM Comments at 1 ("The effectiveness of the ShakeAlert system for public safety depends on . . . its human interface, that is the ability to rapidly and reliably communicate alerts to the public and to motivate protective action.").

[266] *See id.* at 2 ("Among the limitations of IPAWS/WEA/EAS the significantly hinder ShakeAlert's effectiveness are delivery latency, language and media content constraints, and the absence of a unique attention signal for [Earthquake Early Warning (EEW)] . . . to enable user recognition and action without reading a text message. Ideally, the delivery time of ShakeAlert messages would not exceed 5 seconds . . . ").

[267] *Id.* at 8-9; *see also* Letter from Douglas Given, Earthquake Early Warning Coordinator, U.S. Geological Survey, to Marlene H. Dortch, Secretary, FCC, PS Docket Nos. 15-91 and 15-94, at 4 (filed July 27, 2023) (USGS *Ex Parte*).

[268] *See* 47 CFR §§ 10.520(d), 10.530.

[269] USGS Alerting Modernization NPRM Comments at 9 (referencing NFPA 72, the National Fire Alarm and Signaling Code).

[270] USGS *Ex Parte* at 4; *see also* Edin Šabić, Jing Chen, & Justin MacDonald, *Toward a Better Understanding of In-Vehicle Auditory Warnings and Background Noise*, 53 Human Factors 312 (2019), https://journals.sagepub.com/doi/10.1177/0018720819879311.

automatically spoken by default, such as the most common and most imminent WEA messages, for which we have created standard templates?[271]

84. Can text-to-speech produce speech that is accurate, audible, and comprehensible to most listeners? Earthquake alerts may be a good candidate for text-to-speech functionality because they always contain the same, authoritative text: "*Earthquake! Expect shaking. Drop, Cover, Hold On. Protect yourself now. -USGS ShakeAlert.*"[272] We seek comment on this belief. USGS states that, in addition to hastening protective actions for all alert recipients, text-to-speech provides critical information to people with access and functional needs (e.g., visual impairments).[273] How should WEA text-to-speech interact with mobile devices connected to screen readers or other accessibility tools? Are there other discrete consumer groups that would benefit from the availability of text-to-speech for WEA messages, such as people with limited literacy skills? We also invite commenters to address whether Participating CMS Providers could support this functionality in English, Spanish, and other languages.[274] If so, should we require WEA earthquake alerts to include text-to-speech announcements in Spanish and other languages? Would text-to-speech make WEA messages more effective or less effective for subscribers in crowded environments wherein several devices may receive an alert at the same time? Would text-to-speech for earthquake alerts lead consumers to opt out of WEA?

85. We seek comment on the technical implementation issues around text-to-speech for WEA. To what extent do WEA-capable mobile devices already support text-to-speech? Can consumers already enable text-to-speech for WEA on certain makes and models of devices, and if so, how? What, if any, technical changes would be required to enable mobile devices, whether or not they are already capable of text-to-speech, to automatically use text-to-speech to read WEA messages, including earthquake alerts? If we were to require Participating CMS Providers to support text-to-speech for earthquake alerts, should the presentation of that speech begin immediately after a mobile device's presentation of the WEA audio attention signal, or should it replace the audio attention signal? Should users receive that speech by default or should we require that they would need to affirmatively opt in to receive WEAs via text-to-speech, either through their mobile device settings or through an option presented along with the text of the message itself?

86. In addition, we seek comment on USGS's recommendation that we require a unique audio attention signal to accompany earthquake alerts, rather than the standard common audio attention signal associated with all WEA messages.[275] We seek comment on how consumers would react to a unique audio attention signal for earthquake alerts. Is the danger posed by earthquakes unique enough to warrant a specialized attention signal? Would consumers respond to an alert with a unique attention signal more quickly, or would it cause consumer confusion? Social science suggests that people's understanding of emergency alerts is generally low,[276] and significant public education would be required

---

[271] *See* National Federation of the Blind Comments, PS Docket No. 25-224, at 1-2 (rec. Sept. 19, 2025) (NFB Alerting Modernization NPRM Comments) (supporting improvements to end user devices that would offer text-to-speech for EAS and WEA alerts); *see also* FCC, *Multilingual Wireless Emergency Alerts*, https://www.fcc.gov/multilingual-wireless-emergency-alerts (last visited May 11, 2026).

[272] USGS *Ex Parte* at 3.

[273] *Id.*

[274] *See* FCC, *Multilingual Wireless Emergency Alerts*, https://www.fcc.gov/multilingual-wireless-emergency-alerts (last visited Apr. 7, 2026).

[275] *See* 47 CFR § 10.580.

[276] *See* Hamilton Bean & Nels Grevstad, *Wireless emergency alerts: Public understanding, trust, and preferences following the 2021 US nationwide test,* 31 J. Contingencies & Crisis Mgmt. 3 (2022), https://www.researchgate.net/publication/365702760_Wireless_emergency_alerts_Public_understanding_trust_and_preferences_following_the_2021_US_nationwide_test; National Academies, *Emergency Alert and Warning*

(continued….)

to teach people to recognize a distinct attention signal for earthquake early warnings. We seek comment on these findings. We also seek comment on whether the addition of a new attention signal may increase consumer frustration with the alerting system as a whole by generating an additional form of an audio signal that they already find to be intrusive. If we were to require the use of a unique audio attention signal, what should that signal be?

E. Removing Unnecessary Alerting Requirements

87. In the *Alerting Modernization NPRM*, we sought comment on ways the Commission should modernize the nation's alerting systems to improve their usefulness and better leverage modern technology while minimizing burdens on stakeholders.[277] Many commenters argue that removing unnecessary alerting requirements is an essential step in ensuring that alerting remains efficient, reliable, and aligned with the core objectives of alerting. With respect to WEA, for instance, CCA encourages the Commission to "take actions to reduce the cumulative regulatory burdens of the program on smaller and rural providers" in particular, because "simplify[ing] the WEA program . . . [will] promote maximum participation in the program."[278] CCA asks that this proceeding build upon the Commission's *Delete, Delete, Delete* proceeding.[279] Similarly, with respect to EAS, NCTA argues that "it is time to comprehensively reexamine alerting, including the regulatory obligations for cable operators and other EAS Participants, to better reflect modern technology and consumer preferences."[280] ACA Connects likewise urges the Commission to "reduce, rather than expand, the burdens of participation in EAS for smaller cable operators," to reduce the risk that unfunded mandates will drive small cable operators out of the cable video business.[281] In light of these concerns, we advance the following proposals to reduce burdens on EAS and WEA participants while ensuring that these systems continue to advance with modern technologies and consumer expectations.

1. Approving the Use of EAS Software

88. *NAB's Petition for Rulemaking.* We grant NAB's petition to initiate a rulemaking proceeding on its proposal to permit use of software for EAS alert processing as an alternative to the requirement to use dedicated hardware. The petition has made the showing required for such petitions,[282] and we find that it discloses sufficient reasons in support of the action requested to justify the institution of a rulemaking proceeding.[283] At the outset, we observe that among the core purposes that Congress established for the Commission are "promoting safety of life and property through the use of wire and radio communications," promoting "rapid [and] efficient" wireline and wireless services,[284] and

(Continued from previous page)
Systems: Current Knowledge and Future Research Directions (2018), https://www.nationalacademies.org/read/24935/chapter/3.

[277] *Alerting Modernization NPRM*, 40 FCC Rcd at 6696, para. 1.

[278] CCA Alerting Modernization NPRM Comments at 2-3; *see also* CTIA Alerting Modernization NPRM Comments at 4 (asking the Commission to reduce the regulatory burden on all Participating CMS Providers).

[279] CCA Alerting Modernization NPRM Comments at 4; *see also Delete, Delete, Delete*, GN Docket No. 25-133, Direct Final Rule, 40 FCC Rcd 9569 (2025) (eliminating EAS and WEA rules that have outlived their usefulness, among others).

[280] NCTA Alerting Modernization NPRM Comments at 1.

[281] America's Communications Association Comments, PS Docket No. 25-224, at 5 (rec. Sep. 25, 2025).

[282] *See* 47 CFR § 1.401(c) ("The petition shall set forth the text or substance of the proposed rule, amendment, or rule to be repealed, together with all facts, views, arguments and data deemed to support the action requested, and shall indicate how the interests of petitioner will be affected.").

[283] *See* 47 CFR § 1.407.

"encourag[ing] the provision of new technologies and services to the public."[285] Today, EAS still depends heavily on stand□alone hardware located outside the core processing systems that broadcast, cable, and satellite services now use daily. We believe that as the industry shifts toward IP□centric architectures, it is important that the Commission consider whether there is an opportunity to modernize EAS processing to better support public safety and to improve operational efficiency for EAS Participants.

89. We agree with the majority of commenters that granting NAB's petition will provide an opportunity to align the EAS rules with modern technologies and potentially reduce unnecessary burdens on EAS Participants. For example, Sage states that the EAS rules requirements are based on outdated assumptions "no longer correct for many, and possibly most, devices in modern usage."[286] Furthermore, Sage notes that "[s]oftware-only EAS would not preclude the use of a traditional standalone hardware device, but would allow for closer integration of EAS into radio and TV broadcast chains where EAS is made to work within the system, rather than trying to force the existing system to accommodate EAS."[287] NCTA indicates that "NAB's proposal to permit EAS Participants to elect software-based EAS solutions may present the Commission with another opportunity to ensure that emergency alerting keeps pace with modern technology," and "may be of use to cable EAS Participants as well."[288]

90. We also agree with commenters like CMG that argue that the Commission should explore the technical and operational benefits that may arise from the use of EAS software, "includ[ing] streamlined operations, improved remote maintenance and control, and increased security of EAS

(Continued from previous page)
[284] 47 U.S.C. § 151.

[285] 47 U.S.C. § 157(a) ("It shall be the policy of the United States to encourage the provision of new technologies and services to the public.").

[286] Sage Alerting Systems, Inc. Comments, PS Docket No. 15-94, at 2 (rec. Apr. 4, 2025) (Sage NAB Petition Comments) ("Part 11 requirements make certain assumptions about the circumstances in which EAS devices will be used: 1) that there is an operator stationed near the EAS equipment who will need all of these status indications and 2) that the device will be placed near the transmitter, and 3) that the device is analog in nature. These assumptions are no longer correct for many, and possibly most, devices in modern usage. These requirements increase the cost of every EAS device on the market.").

[287] Sage NAB Petition Comments at 2; *see also* Nautel Maine Inc. Comments, PS Docket No. 15-94, at 2 (rec. Apr. 29, 2025) (Nautel NAB Petition Comments) ("Trusted audio over IP routing rather than legacy audio inline insertion provides a practical interface to software-based air chain components that are virtualized," and "provides the flexibility to interface with any EAS implementation."); Society of Broadcast Engineers, Inc. Comments, PS Docket Nos. 15-94 and 22-329, at 5 (rec. May 2, 2025) (SBE NAB Petition Comments) ("[H]armonizing broadcast EAS equipment with the other software-based components of broadcast infrastructure may open up additional possibilities for stations to more comprehensively incorporate alerting into the broadcast airchain."); Aldon Caron Comments, PS Docket Nos. 22-329 and 15-94, (rec. Apr. 29, 2025) ("Converting to a software-based model allows for more flexibility and decisions based on the needs of the station or station group."); Letter from Kyle Kratoville, Craven County SBA, Inc, to Marlene H. Dortch, Secretary, FCC, PS Docket No. 15-94 at 1, (filed May 15, 2025) (Craven County *Ex Parte*) ("Approving a compliant, software-defined EAS solution would reflect how stations actually operate today," and "provide greater flexibility, make redundancy easier to implement, and help lower costs for broadcasters—particularly for smaller stations and new entrants."); New York Public Radio, University Radio Foundation, Inc., and J. Paxton Durham Comments, PS Docket Nos. 15-94 and 22-329, at 1 (rec. May 2, 2025) (Public Radio Joint NAB Petition Comments) (supporting the NAB Petition as "an important modernizing step that will improve EAS's efficiency and reliability without compromising the system's effectiveness."); CMG Media Corporation Comments, PS Docket Nos. 15-94 and 22-329, at 2 (rec. May 2, 2025) (CMG NAB Petition Comments) ("[S]oftware-based EAS technology provides a practical option for broadcasters to choose from different service offerings, as opposed to being stuck with one outdated legacy option.").

[288] NCTA—The Internet & Television Association Comments, PS Docket Nos. 15-94 and 22-329, at 2 (rec. May 2, 2025) (NCTA NAB Petition Comments).

equipment."[289] Commenters emphasize that the existing hardware‐based EAS poses significant repair delays and reliability challenges, while a software‐based approach could streamline maintenance and improve overall system performance. The Society of Broadcast Engineers (SBE) notes that when dedicated EAS equipment malfunctions "stations often have to locate, schedule, and deploy a contract engineer to physically diagnose and repair the malfunction. Additionally, the equipment must sometimes be physically shipped all the way back to the manufacturer for repair (or to be manually updated)."[290] NTCA–The Rural Broadband Association states "that the shipping time, distance between locations and the availability (or unavailability) of parts for older equipment can all contribute to delays in repairing EAS equipment,"[291] and NCTA further states "there are occasionally defects that are more difficult to address or instances in which equipment takes longer to replace due to inventory limitations, for which the Commission's current rule provides necessary time."[292] The Joint Commenters contend that software-based EAS could "improve the [EAS] system's effectiveness: for instance, by enabling systems to be repaired and updated much more efficiently through a software update or remote fix rather than factory repair of a physical device; by eliminating single points of failure through multiple instances of EAS software in diverse locations; and by facilitating the routing and targeting."[293] We believe that these are all appropriate reasons to explore whether the EAS rules can be improved by allowing EAS Participants to rely on EAS software.

91. Opposing commenters fail to convince us that the issue is not ripe for consideration or that rulemaking sought by NAB would conflict with the public interest, particularly given Congress's historic policy of considering the use of new technologies.[294] DAS argues that the NAB Petition "offers no discussion of how such software-based systems would be verified, authorized, or audited for compliance with existing Commission rules,"[295] adding that there is no "FCC process for certifying software-only EAS solutions."[296] DAS further comments that the NAB Petition does not address cybersecurity, and that "[t]here is currently no robust FCC cybersecurity standard tailored to EAS software platforms."[297] We observe that the need to develop equipment certification or approval requirements appears to be anticipated in the NAB Petition,[298] and by its supporters.[299] As Sage puts it,

[289] CMG NAB Petition Comments at 2.

[290] SBE NAB Petition Comments at 4.

[291] NTCA–The Rural Broadband Association Alerting Security NPRM Comments at 6-7.

[292] NCTA Alerting Security NPRM Comments at 10.

[293] Public Radio Joint NAB Petition Comments at 2; *see also* SBE NAB Petition Comments at 4 ("SBE agrees with NAB that a flexible software-based approach could meaningfully alleviate delays and other difficulties many broadcasters currently face when dealing with EAS equipment maintenance and repair.").

[294] *See* 47 U.S.C. § 157(a) ("Any person or party (other than the Commission) who opposes a new technology or service proposed to be permitted under this chapter shall have the burden to demonstrate that such proposal is inconsistent with the public interest.").

[295] Digital Alert Systems, Inc. Comments, PS Docket Nos. 15-94 and 22-329, at 5 (rec. May 2, 2025) (DAS NAB Petition Comments); *see also* Letter from Barry Mishkind & Richard Rudman, Broadcast Warning Working Group, to Marlene H. Dortch, Secretary, FCC, PS Docket Nos. 15-94 and 22-329, at 3-6 (filed May 19, 2025) (BWWG *Ex Parte*).

[296] DAS NAB Petition Comments at 6. DAS further contends that the "underlying premise" of the NAB Petition is that "software-based EAS systems should not be subject to the same FCC certification standards under § 11.34," that would "subject[] similarly situated parties to inconsistent regulatory treatment," and "the emergence of incompatible, vendor-specific implementations that lack uniform validation and testing," among other things. *Id*. at 15-16.

[297] *Id*. at 9; *see also* BWWG *Ex Parte* at 5-6.

"[c]ybersecurity is an issue that needs to be taken into account; however, the issues are known, and are not fundamentally different than any other IT component of a broadcast facility."[300] In any event, we agree that certification and security are important aspects to be resolved with respect to the NAB Petition's proposal, but we also agree with NAB that these issues "are properly considered within a rulemaking proceeding," and we address these issues below.[301]

92. We also reject DAS's argument that NAB's proposal "may confer greater relative benefits on radio broadcasters — particularly those with simpler technical operations — than on television or cable operators, which already rely heavily on integrated, IP-capable workflows," which DAS concludes "undermines the foundational principle that any revision to Part 11 must serve the public interest equitably across all EAS Participants."[302] Even assuming that DAS's assumptions about the benefits of NAB's proposals are accurate, the possibility that some EAS Participants might be able to implement a software-based EAS approach more easily than others would not be adequate grounds for declining to consider the issue.

93. DAS also argues that "[a] central tenet of the Commission's rulemaking authority under the Communications Act of 1934, as amended, is the requirement that any new regulation — or deregulation — must advance the public interest, convenience, and necessity,"[303] adding that, "[i]n the context of emergency communications, the standard is even more stringent: Proposals must demonstrably enhance the reliability, reach, or effectiveness of life-saving public safety information."[304] DAS contends in this regard that "the Petition is silent as to how its request to allow software-based EAS solutions would achieve any tangible improvement in how alerts are received or understood by the public."[305] We observe that, as stated above, the NAB Petition has made the showing required for Petitions for Rulemaking,[306] and discloses sufficient reasons to justify the institution of a rulemaking proceeding.[307] Moreover, as the NAB Petition described it, software-performed EAS might enable "an

(Continued from previous page)

[298] *See* NAB Petition at 6 ("We envision a similar development cycle that would include testing and certification of an integrated software solution for EAS.").

[299] SBE NAB Petition Comments at 6; Sage NAB Petition Comments at 2; Letter from Harold Price, President, Sage Alerting Systems, Inc., to Marlene H. Dortch, Secretary, FCC, PS Docket No. 15-94, at 2 (filed May 16, 2025) (Sage May 2025 *Ex Parte*).

[300] Letter from Harold Price, President, Sage Alerting Systems, Inc. to Marlene H. Dortch, Secretary, FCC, PS Docket No. 15-94 (filed June 9, 2025) (Sage June 2025 *Ex Parte*); *see also* Nautel NAB Petition Comments at 2 ("Audio over IP can be secured using standard IT practices commonly used for critical infrastructure.").

[301] Letter from Larry Walke, Associate General Counsel, National Association of Broadcasters, to Marlene H. Dortch, Secretary, FCC, PS Docket Nos. 15-94 and 22-329, at 5 (filed May 19, 2025) (NAB May 2025 *Ex Parte*).

[302] DAS NAB Petition Comments at 19-20.

[303] *Id.* at 32 (citing 47 U.S.C. §§ 151, 303(r)).

[304] *Id.*

[305] *Id.*

[306] *See* 47 CFR § 1.401(c).

[307] *See* 47 CFR § 1.407 ("If the Commission determines that the petition discloses sufficient reasons in support of the action requested to justify the institution of a rulemaking proceeding, and notice and public procedure thereon are required or deemed desirable by the Commission, an appropriate notice of proposed rule making will be issued."). Accordingly, whereas DAS argues "Without any comparative [relative to dedicated "modern EAS devices" (emphasis removed)] benefit to the public in terms of either cost, performance, or accessibility, the proposed rule change [to allow use of EAS software to meet EAS obligations in part 11 of the FCC rules] lacks a compelling public interest justification," we observe that no such showing is required under our rules. DAS NAB Petition Comments at 34. In any event, the NAB Petition indicates that, in the context of broadcast facilities, EAS (continued….)

immediate fail-over of functionality" to backup EAS software operating on systems in other locations.[308] The NAB Petition adds, "[t]his feature is critical as many broadcasters have been forced to evacuate facilities due to environmental disasters and relocate to auxiliary facilities, abandoning their hardware-based EAS equipment when the public needs emergency messaging the most."[309] These functions strike us as potentially enhancing the reliability, availability and, potentially in times of outages, the reach of the EAS.[310]

94. *Implementing EAS Software.* Consistent with NAB's petition, we propose to permit, but not require, EAS Participants to use software-based EAS encoder/decoder technology instead of a dedicated EAS hardware device to process EAS alerts.[311] As outlined above, the record developed in response to the NAB Petition demonstrates broad support for the concept of using software to perform EAS functions in place of dedicated EAS equipment.[312] We tentatively agree with the Society of Broadcast Engineers that "permitting broadcasters to implement flexible software-based EAS equipment if they so choose allows EAS equipment to evolve, helps provide a potential lifeline to stations whose dedicated EAS hardware is no longer being manufactured, and spurs meaningful beneficial developments in the EAS ecosystem both at the station level and overall."[313] We anticipate that allowing use of software-based EAS would enable expeditious repairs, security updates, and compliance upgrades to an EAS Participant's provision of EAS alerting, as well as more easily enabling backup EAS coverage when the primary software-based EAS source becomes unavailable, as commenters have asserted.[314] These

(Continued from previous page)
software is superior to dedicated EAS equipment in terms of performance and flexibility, to the benefit of both EAS Participants and the public. *See* NAB Petition at 6-7. For this reason, we also find DAS's assertions that "the Petition proposes to remove key regulatory guardrails in the EAS ecosystem without demonstrating any measurable gain for the American public," and that "[t]hat failure alone is grounds for denying, or at least deferring, the Petition until a full record is developed," to be factually incorrect. DAS NAB Petition Comments at 34. We agree that a full record needs to be developed, but the procedurally proper regulatory vehicle for developing that record is the rulemaking proceeding we initiate here – not the limited proceeding associated with making the bare determination of whether to grant a petition to initiate such proceeding. Finally, whereas DAS "hope[s] the Commission will not act on [] unsupported assertions [of "widespread supply chain disruptions"] to revise long-standing certification requirements, potentially risking arbitrary and capricious rulemaking," we observe that the decision to grant a Petition for Rulemaking is not a rulemaking proceeding. *Id.* at 38.

[308] NAB Petition at 6-7.

[309] *Id.* at 7.

[310] We observe that the effectiveness of alerts is the purview of alert originators and the Commission, which establishes EAS requirements, not EAS Participants who are charged with issuing alerts in conformance with such requirements. For this reason, we find DAS's assertion that the NAB Petition "offers no evidence that software implementations would, among other things: Improve clarity of alert displays[;] Enhance accessibility for individuals with disabilities;[] Reduce latency in alert dissemination[;] Enable new formats or languages for at-risk populations[;] [and] Provide greater reliability under stress or during outages" to be misplaced. DAS NAB Petition Comments at 33.

[311] *See* NAB Petition at 1.

[312] *See, e.g.*, CMG NAB Petition Comments at 2; Nautel NAB Petition Comments at 1; Sage NAB Petition Comments at 3; Public Radio Joint NAB Petition Comments at 1.

[313] SBE NAB Petition Comments at 5; *see also* Sage NAB Petition Comments at 2 ("Software-only EAS would not preclude the use of a traditional standalone hardware device, but would allow for closer integration of EAS into radio and TV broadcast chains where EAS is made to work within the system, rather than trying to force the existing system to accommodate EAS."); NCTA Alerting Modernization NPRM Comments at 2 ("Although NAB's proposal discusses the use of a software-based EAS encoder/decoder in the context of broadcast station operations, such a solution may be of use to cable EAS Participants as well.").

beneficial aspects of EAS software should increase EAS availability, and potentially EAS security, which furthers our goal of providing alert originators with the ability to rapidly notify the public of emergencies. Enabling automatic fail-over to a backup EAS source would further our goal of providing communications during and after emergencies, when power and/or internet outages can impede or prevent regular EAS operations and other forms of communication to the public. NAB argues that "[t]his feature is critical as many broadcasters have been forced to evacuate facilities due to environmental disasters and relocate to auxiliary facilities, abandoning their hardware-based EAS equipment when the public needs emergency messaging the most."[315] We seek comment on these expectations.

95. More broadly, we anticipate that EAS software would be adaptable and could help support or drive the adoption of advanced alerting capabilities. To that end, we seek comment on whether there are aspects of EAS software or its integration within an EAS Participant's service delivery system that would better allow EAS Participants to voluntarily analyze, process, and present audio/visual messages, photos, maps, or other information provided or linked in a CAP EAS alert? Would software EAS be adept at performing geotargeting calculations, text-to-speech, speech-to-text, or other alerting functions? Would EAS software be capable of generating or passing through CAP alerts over secondary channels or subcarriers for consumption by end user devices capable of processing them?[316] Are there any specific functions that EAS software could provide that are not available to EAS hardware devices and would be particularly beneficial to alert originators?

96. Flexibility is an important part of our proposal. We propose to allow EAS Participants to install EAS software in a single device (e.g., a server or computer) that manages EAS functions within the EAS Participant's signal processing system. Alternatively, we propose to allow EAS software to be installed across multiple components within that system, thus enabling integration of different EAS functions across multiple system components. SBE, for example, contends that "[t]he Commission's rules should provide broadcasters with the flexibility necessary for them to implement the best EAS solution for their station's specific operational circumstances."[317] In addition to the benefits described above, we believe that enabling flexibility in EAS software deployment may make compliance with EAS obligations easier to manage, and reduce costs for those EAS Participants that elect to use EAS software. We also anticipate that our approach may spur innovation in EAS alert capabilities by RF transmission system (and possibly cable system) equipment providers who integrate encoder/decoder software into their self-contained transmitter/signal processing systems.[318] We seek comment on this proposal and our

(Continued from previous page)

[314] *See*, *e.g.*, NAB Petition at 6-7; Public Radio Joint NAB Petition Comments at 2; CMG NAB Petition Comments at 2.

[315] NAB Petition at 7.

[316] The National Federation of the Blind addresses the concept of end user devices relaying alerts directly to connected Braille display stating, "[t]he ability to connect a Braille display, either directly or through another connected "smart" device, is unquestionably the most effective way to reach deafblind individuals, who not only cannot see an emergency alert on a television or smartphone, but also cannot hear the audible details of the alert, which may contain life-saving information like evacuation routes or instructions to shelter in place." National Federation of the Blind Comments, PS Docket No. 25-224, at 2 (rec. Sept. 19, 2025).

[317] SBE NAB Petition Comments at 1; *see also* Sage NAB Petition Comments at 2 ("Removing specific hardware requirements will allow users to select an EAS solution that fits their needs, and potentially runs in equipment they already have."); NAB May 2025 *Ex Parte* at 3.

[318] *See*, *e.g.*, Nautel NAB Petition Comments at 2 ("Nautel and other industry participants have the technical capability to architect transmitters that can participate in a fully software-based or software/hardware hybrid virtual approach."); Letter from Ben Barber, President/CEO, Inovonics, Inc., to Marlene H. Dortch, Secretary, FCC, PS Docket Nos. 15-94 and 22-329, at 1 (filed May 19, 2025) (" . . . we support all implementations of EAS, hardware and virtual.").

related analysis. Are there additional benefits that EAS software could provide that would further the goals we set out for the EAS and WEA alerting systems in the *Alerting Modernization NPRM*?[319]

97. While providing flexibility is important, this goal needs to be balanced against the necessity of ensuring the reliability of the EAS. In the *Alerting Modernization NPRM*, we asked, among other things, whether alerting systems should also incorporate resilience to common causes of disruption to communications.[320] In general, alert originators responding to these questions observed that ensuring delivery of alerts is critically important. As the Washington State Emergency Management Division put it, "[p]ublic warning must be reliable even during worst-case conditions."[321] Many of these commenters stressed the need for redundancy in the delivery of alerts. The New York State Division of Homeland Security and Emergency Services, for example, stated "[a]lerting systems should have a high degree of resilience, incorporating redundant systems and pathways to ensure that alerts are actually received by the public."[322]

98. To that end, we propose to require that EAS software – however it is integrated into or across the EAS Participant's signal processing system – be located at the EAS Participant's local facility used to provide service. For a broadcaster this would mean that EAS software would be required to be installed at the studio or transmitter site associated with its licensed service area.[323] For a cable communications service provider, this would mean that EAS software would have to be installed at the headend facility. We observe that this proposal would prohibit EAS from being generated within cloud-based systems or cloud-based third-party EAS services. Our proposal is grounded in concerns about the resilience of IP-based connections in the alerting context. With IP-based systems, functions previously performed on local equipment can be carried out anywhere in the world relying on Internet or wide area networks to connect them. EAS software potentially has the same capability, relying on IP networks to bring in monitored audio sources and to output EAS alerts for insertion into programming at other locations. However, this reliance on IP networks could cause EAS Participants to be cut off from their EAS capabilities during emergencies that involve power outages or infrastructure damage, which are types of emergencies for which EAS has historically demonstrated to be useful. As MITRE states in a 2025 white paper, critical infrastructure sectors' emergency communications planning "should assume all standard commercial IP traffic and communications are unavailable in a wide area,"[324] which would be inconsistent with installing EAS software at distant facilities. We further observe that our approach is consistent with the NAB Petition, wherein NAB states that it "is not seeking an off-premises, fully cloud-based approach."[325] DAS and NCTA also express concern that remote hosting and EAS software processing may diminish the Commission's capacity for oversight and enforcement.[326]

---

[319] *Alerting Modernization NPRM*, 40 FCC Rcd at 6698, para. 7.

[320] *Id.* at 6700-01, para. 13.

[321] Washington EMD Alerting Modernization NPRM Comments at 7.

[322] NY DHSES Alerting Modernization NPRM Comments at 2.

[323] By "studio," we mean the local physical facility wherein programming is generated and/or compiled and processed for transmission.

[324] Chris Sledjeski & Mark Bristow, MITRE Corporation, Building PACE Capabilities for the Current Threat Environment, at 4 (2025), https://www.mitre.org/sites/default/files/2026-01/PR-25-2966-building-pace-capabilities-for-the-current-threat-environment_0.pdf.

[325] NAB Petition at 4.

[326] *See*, *e.g.*, DAS NAB Petition Comments at 10 ("Software-based EAS solutions could very well be hosted or maintained on equipment from third-party international companies. The FCC may lack the ability or authority to directly regulate these vendors or mandate technical disclosures."); NCTA Alerting Modernization NPRM

(continued….)

99. We seek comment on limitations. Would our approach sufficiently mitigate risks associated with IP network failures? Are there other locations at which we should permit the use of EAS software that allow EAS to retain its signature resilience? Should we allow EAS software to be installed anywhere so long as the EAS Participant also locates and operates EAS software at the transmitter as a fail-over location? If we allow these kinds of network designs that require EAS software to be located at the transmitter as the fail-over location, should we also require that monitored sources be received at the same location so they also avoid being blocked by inoperable IP connections? Would some or all of these measures sufficiently ensure that EAS Participants using EAS software would be able to receive and transmit legacy and/or CAP alerts during most emergency situations when alert originators and the public need them the most? Are there additional or alternative requirements for the use of EAS software that we should adopt to ensure resiliency and fulfillment of the alerting goals discussed above? How should any of these requirements be effectively reflected in the language of our rules?

100. We also observe that some commenters raise market-based justifications for allowing use of EAS software. The NAB Petition, for example, argues that "the recent decision of Sage Alerting Systems, one of the two remaining EAS device vendors, to cease production of its [encoder/decoder] device due in large part to supply-chain problems acquiring legacy parts for original EAS hardware-only designs" illuminates the need to consider its EAS software proposal.[327] The NAB Petition further contends that "[u]nder NAB's proposed approach, such manufacturing issues will not be a significant concern because the software will be able to operate on multiple existing hardware appliances or software processes already in use within broadcasting."[328] CMG argues that "[a]s time goes on the [supply chain] problem will worsen, and the Commission must consider what happens if the last vendor can no longer manufacture the required device or if a repair backlog results in communities missing crucial EAS messages."[329] CMG adds "[t]he Commission should not force broadcasters to rely on one vendor to provide EAS service or upgrade their devices when there are viable alternatives that can relieve pressure, modernize EAS overall, and potentially save lives."[330]

101. DAS, however, argues that the NAB Petition's "inferred focus on [Sage's] specific legacy technology should not be taken to suggest a broader industry challenge, whether that be in terms of supply chain, product availability, or capabilities to serve modern advanced air chain requirements."[331] To that end, DAS argues that "[m]odern EAS encoder/decoder systems . . . have already adapted to the requirements of contemporary broadcast facilities . . . [and] do not face the same integration challenges that may affect older or end-of-life devices."[332] DAS argues "[i]f, as the Petition suggests, certain EAS Participants are encountering operational friction due to outdated EAS infrastructure or legacy EAS workflows, that should be addressed through narrowly tailored policy mechanisms — such as limited waivers, technical guidance, or updates to certification criteria — rather than a sweeping rule change."[333] DAS also asserts "[i]n the absence of continuing demand for hardware-based EAS systems, manufacturers may redirect their resources away from research and development (R&D) for physical

(Continued from previous page)
Comments at 2 ("NCTA agrees with NAB that any [EAS software] solution should not be directly exposed to the internet or be fully cloud-based.").

[327] NAB Petition at 3.

[328] *Id.*; *see also* SBE NAB Petition Comments at 3-4; NCTA Alerting Modernization NPRM Comments at 2.

[329] CMG NAB Petition Comments at 3.

[330] *Id.*

[331] DAS NAB Petition Comments at 29.

[332] *Id.*

[333] *Id.* at 30.

equipment[,]" thus potentially "stifling innovation in areas such as hardware security, system resilience, and compatibility with new standards (e.g., ATSC 3.0)."[334]

102. We seek comment on these views.[335] Is there reason to believe that EAS software solutions would not be affected by supply chain shortages that would affect manufacturers of stand-alone encoder/decoder devices generally? What impacts would EAS software solutions have on the market for EAS encoder/decoder solutions? We observe that the equipment certification requirements we seek comment on (below) are intended to ensure regulatory parity between EAS software and stand-alone EAS encoder/decoder devices. With that in mind, should we take into account the competitive impacts, if any, that EAS software might have on the production or continued development of stand-alone EAS encoder/decoder devices?

103. DAS also argues that "[EAS software] developers must now account for potential IP landmines that could stall or complicate product viability."[336] DAS indicates it has been "made aware of several published patents and provisional patents that appear to cover key aspects of the software-based EAS model."[337] To that end, DAS asserts that "[u]ndisclosed intellectual property may introduce significant concerns related to policy and competition in the marketplace."[338] We seek comment on whether the use of EAS software would implicate any intellectual property considerations, and the extent to which those differ from any such considerations that may apply to stand-alone EAS encoder/decoder devices. Are any elements of EAS software functionality patented? If so, who holds those patents and will these patents discourage or prevent vendors from entering the EAS software market and creating competition?

104. *EAS Software Certification*. At the outset, we tentatively agree with commenters that EAS software must be subject to a rigorous certification or other approval process before it can be allowed to be marketed and used.[339] As DAS observes, "[w]ithout such a framework, software solutions could vary significantly in quality, security, and functionality, with no clear method for regulators or users to determine compliance," adding that such result would "dilute the integrity of the EAS ecosystem and impose an untenable oversight burden on the Commission."[340] We seek comment on what certification or other approval framework should apply to EAS software.

---

[334] *Id.* at 21. More broadly, DAS argues that "[t]he shift away from traditional, certified physical systems in favor of less-regulated software alternatives may disrupt the established market dynamics, potentially leading to long-term negative effects on industry stability, innovation, and overall system reliability." *Id.*

[335] We observe that there currently are three EAS device manufacturers producing, marketing, servicing and updating stand-alone EAS encoder/decoder devices: DAS (https://www.digitalalertsystems.com); VIAVI Solutions (https://www.viavisolutions.com/en-us), and Gorman-Redlich Mfg. Co. (http://www.gorman-redlich.com). Sage has indicated that it no longer manufactures new EAS devices, but will continue to service, support and develop updates for the deployed base of Sage encoder/decoder devices currently in use. Sage NAB Petition Comments at 3.

[336] DAS NAB Petition Comments at 28.

[337] Letter from Edward Czarnecki, Ph.D., Vice President, Government and International, Digital Alert Systems, Inc., to Marlene H. Dortch, Secretary, FCC, PS Docket Nos. 15-94, 22-329, at 1 (filed May 25, 2025). DAS added that "Several published patents appear to describe systems and methods that relate to the architecture and functional elements of a software-based EAS model." *Id*.

[338] *Id.* at 2.

[339] *See*, *e.g.*, DAS NAB Petition Comments at 6, 8; SBE NAB Petition Comments at 3-5; Sage May 2025 *Ex Parte* at 2.

[340] DAS NAB Petition Comments at 8.

105. The EAS rules currently require dedicated EAS equipment to be certified in accordance with the Commission's equipment certification procedures in part 2 of the Commission's rules.[341] Equipment certification involves device testing to ensure that the device meets the performance requirements that apply to it. Certification approval is required before that device model can be marketed. The responsible party (typically the manufacturer)[342] for the device handles the various administrative requirements, arranges for device testing by an accredited FCC-recognized test laboratory, and submits the certification application to a telecommunication certification body (TCB), which reviews the test report and other application materials, and issues the certification on behalf of the FCC. This framework is well-established, but historically is geared towards testing and authorization of licensed and unlicensed intentional radiators (e.g., broadcast transmitters, mobile handsets and garage door openers) and unintentional radiating equipment (e.g., personal computers and other digital devices that emit emissions as a byproduct of their digital clock circuity) with easily measurable in-band, out-of-band and harmonic radio frequency (RF) emissions levels. Certifying or otherwise approving EAS software represents a different challenge, that may require an alternative approach.

106. Commenters addressing this issue generally support subjecting EAS software to certification, and generally frame their discussions around our existing equipment authorization rules and procedures. SBE, for example, comments that certification is necessary "to ensure that flexible software-based EAS solutions enjoy at least the same level of security and reliability as current dedicated hardware solutions."[343] DAS raises concerns that EAS software certification is necessary, but that "there is no [], widely accepted FCC process for certifying software-only EAS solutions."[344] We tentatively conclude that requiring EAS software to be certified under a conformity assessment scheme that is architecturally similar or identical to that under which EAS equipment is certified today is necessary to preserve the reliability of EAS, i.e., EAS software would be submitted to an approved entity for testing and then to a certification body for approval. We seek comment on this view. Noting that test labs are generally focused on measuring equipment emissions, power, bandwidth, etc., are such test labs equipped with personnel and equipment to conduct detailed software testing for EAS? Are there accreditation standards that test labs would need to comply with and be approved for? If EAS software is required to be certified, how should the certification requirement be implemented? Can the existing certification framework in part 2 be applied to ensure that EAS software works correctly? Would modifications to the existing part 2 framework be necessary to support this testing? If so, what changes are needed and how would those changes fit into the current test lab and TCB approval process? Are there alternative approaches to testing and certification that achieve similar or better outcomes? For example, would some combination of the existing part 2 device certification framework and a third-party conformity assessment regime geared towards software be a suitable approach, and if so, how would those be integrated? Should the certification framework be completely independent of part 2, and if so, how should it be structured? In

[341] *See* 47 CFR §§ 11.34(a)-(c), 2.907. While sections 11.34(a) and 11.34(b), 47 CFR § 11.34(a), (b), covering encoders and decoders, respectively, require demonstration of compliance with the requirements in part 11 and the requirements in the part 15 rules for digital devices, we do not propose to extend the part 15 compliance requirement to EAS software, which we anticipate will be installed in various off-the-shelf and custom equipment of other manufacturers that already will have competed any applicable FCC equipment authorization processes.

[342] *See* 47 CFR § 2.909 ("In the case of equipment that requires the issuance of a grant of certification, the party to whom that grant of certification is issued is responsible for the compliance of the equipment with the applicable technical and other requirements.").

[343] SBE NAB Petition Comments at 5; *see also* DAS NAB Petition Comments at 5-6, 14, 17; BWWG *Ex Parte* at 3-5; Sage NAB Petition Comments at 3.

[344] DAS NAB Petition Comments at 6 (further commenting that the Commission must clarify "[w]hether software updates would trigger re-certification under § 11.34[; h]ow configuration changes will be documented, audited, and enforced[; h]ow compliance will be ensured across diverse software and hardware environments[.]").

such a case, what types of entities have capability for such testing and approvals? Would such an entity be expected to issue certification or similar approval on the Commission's behalf, similar to the role TCBs currently have in the equipment certification process?

107. We seek comment on what functions should be tested and what procedures should be followed when certifying or otherwise approving EAS software. Currently, dedicated EAS equipment is tested to ensure compliance with the encoder and decoder requirements in sections 11.32 (and 11.31 as cross-referenced therein) and 11.33 using oscilloscopes and other radio frequency (RF) analyzing instruments, as well as compliance with some non-electrical requirements.[345] Are the existing methods for testing compliance with these requirements sufficient to ensure compliance for both EAS hardware and software (as installed in hardware)? Sage observes that "TCBs do not check for most elements of EAS processing," adding "we need (and have always needed) a set of tests similar to the 2011 FEMA Conformity Assessment."[346] Regardless of what certification regime EAS software or hardware might be certified or otherwise approved under, are there specific aspects of alert processing or other part 11 functionalities that are not currently tested as part of the FCC's EAS equipment certification process, but should be, and if so, what testing procedures should apply? Given the potential for widespread variety in EAS software configurations, should the Commission or independent standards bodies develop a more comprehensive test procedure for EAS equipment and EAS software? Should the IPAWS Conformity Assessment's pass/fail testing approach be applied to EAS software, and if so, should it be applied as-is or as modified in some way? Could that approach be updated and standardized to cover not just CAP-to-legacy conversion, but any other alert processing functionalities that are not currently tested but should be? What additional functionalities should be included? Who should develop such a standard? Would a reconstituted ECIG or other industry group be best-positioned to develop such standard? Are there certain testing requirements or procedures that should be different for EAS equipment and EAS software to reflect their differing characteristics, or should EAS equipment and EAS software always be subject to the same requirements and procedures? Are TCBs equipped to perform testing on EAS software following the pass/fail approach used for testing compliance with the ECIG Implementation Guide? If not, what entities are best suited to perform such testing, and what accreditation scheme, if any, should apply? Are there existing third-party testing programs that could accommodate such testing?

---

[345] For example, testing includes causing the encoder to generate a header code string and using an oscilloscope to confirm that the string conformed to the Audio Frequency Shift Keying modulation specifications at 11.31(a)(1); inputting an alert to confirm storage of the audio message per 11.33(a)(3)(i); and inputting an EAN alert while the encoder is playing out a non-EAN alert and confirming that the EAN overrides the non-EAN alert in progress. *See*, *e.g.*, Emissions Test Report for Sage Alerting Systems Inc., Endec Model: 3644, available at https://apps.fcc.gov/oetcf/eas/reports/ViewExhibitReport.cfm?mode=Exhibits&RequestTimeout=500&calledFromFrame=N&application_id=b%2F%2FrMD5AMxxtz5%2B0GOdYRw%3D%3D&fcc_id=V2W3644; Test Report for the Digital Alert Systems DASDEC-III , available at https://apps.fcc.gov/oetcf/eas/reports/ViewExhibitReport.cfm?mode=Exhibits&RequestTimeout=500&calledFromFrame=N&application_id=OKhPlnNwdDvQGKgWoMpxVg%3D%3D&fcc_id=R8VG3DAS01.

[346] Sage May 2025 *Ex Parte* at 2. The procedures for processing CAP-formatted EAS alerts are set forth in the EAS-CAP Industry Group (ECIG) Implementation Guide. *See* 47 CFR § 11.56(a)(2) (referencing EAS-CAP Industry Group, ECIG Recommendations for a CAP EAS Implementation Guide, Version 1.0, (2010), http://eas-cap.org/ECIG-CAP-to-EAS_Implementation_Guide-V1-0.pdf). The Commission has established that compliance with the ECIG Implementation Guide can be demonstrated by EAS devices following the test procedures developed by FEMA for its IPAWS Conformity Assessment program (discontinued in 2011). *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; Randy Gehman Petition for Rulemaking*, EB Docket No. 04-296, Fifth Report and Order, 27 FCC Rcd 642, 700-02, paras. 165-68 (2012). This testing involves inputting CAP-formatted alerts into the device and confirming CAP Profile data is correctly extracted and internally processed in accordance with the ECIG Implementation Guide on a pass/fail basis.

108. We observe that several requirements in the Commission's EAS encoder and decoder rule sections set forth physical and electrical specifications that apply to the hardware aspects of the equipment, as well as the emissions profile of the radiofrequency signals they generate.[347] Sage notes, for example, that "[p]art 11 requires an alphanumeric display, a speaker, visual indication of alert status, 'data ports', two or more audio inputs, and one or more audio outputs," adding that "requirements for temperature and humidity, supply voltage variations, and operation in 10 V/m AM and 0.5 V/m FM [also] must be met."[348] Sage further observes, "[a]s a practical matter, this requires a separate box for certification."[349] At the time these and other encoder and decoder requirements were developed in the early 1990s, it was assumed that these functions would be performed in a stand-alone device built for this purpose. Does this assumption still make sense today, given the current state of technology? Do these requirements still make sense as applied to either EAS software or standalone equipment built for EAS purposes?[350] We seek comment on whether any or all of the physical and electrical specifications that apply to the hardware aspects of dedicated EAS equipment should be applied to EAS software, as installed whichever representative configuration applies (e.g., the off-the-shelf server in which the EAS software is installed).[351] We observe that application of some of these requirements to EAS software can be achieved through minor revisions to some of these provisions, as contained in Appendix B of this *Further Notice*.[352] We seek comment on the sufficiency of these proposed revisions.

109. With respect to how the EAS software must be configured for testing, we propose that EAS software must be tested as installed in hardware that is representative of that which it is intended and marketed to be used. As a result, the certification that EAS software would receive would apply only to that EAS software as installed and operated in a representative server or computer configuration. Pursuant to this approach, standalone EAS software that is intended to be installed and operated in an off-the-shelf server or computer would be tested as installed by the software manufacturer in any representative server or computer. EAS software that is intended to be installed and operated in a manufacturer's custom-designed product—for example, a signal processing system component that performs one or more signal processing functions and may include a central processing unit (CPU) utilizing custom or generic operating system software, but which is not itself a stand-alone server or computer—would have to be tested as installed in such custom-designed component, since there is no representative device for such a custom-designed product. In this case, the manufacturer of the custom-designed product typically would be responsible for certification, and the EAS software certification testing would be performed at the same time as the custom-designed product's conformity assessment testing.[353] EAS software that is installed and integrated across multiple system components would have

[347] *See*, *e.g.*, 47 CFR § 11.32(c) (requiring that "Encoders shall be capable of complying with the requirements of this section during a variation in primary supply voltage of 85 percent to 115 percent of its rated value."); 47 CFR § 11.33(a)(4) (requiring that decoders be configured with a physical display allowing alerts to be "fully displayed on the decoder and readable in normal light and darkness."); *see also* 47 CFR § 11.32(a)(2), (a)(3), (a)(7)-(9), (b), (d); 47 CFR § 11.33(a)(1), (a)(3), (a)(5), (a)(7), (b) (cross-referencing 47 CFR § 11.32(b)-(d)).

[348] *See* Sage NAB Petition Comments at 2.

[349] *Id.*

[350] *Id.* ("These and other Part 11 requirements make certain assumptions about the circumstances in which EAS devices will be used: 1) that there is an operator stationed near the EAS equipment who will need all of these status indications and 2) that the device will be placed near the transmitter, and 3) that the device is analog in nature. . . . These assumptions are no longer correct for many, and possibly most, devices in modern usage, [and] increase the cost of every EAS device on the market.")

[351] *See* 47 CFR § 11.32(a)(2), (a)(3), (a)(7)-(9), (b)-(d); 47 CFR § 11.33(a)(1), (a)(3)-(5), (a)(7),(b).

[352] *See infra* Appx. B (47 CFR §§ 11.32, 11.33).

to be tested as so installed and integrated (typically on an *in situ* basis). Because this also is a custom configuration, the manufacturer of the system components typically would be responsible for certification. We observe that the representative testing model proposed above is currently applied to most device testing under our equipment authorization rules because it is neither practical nor necessary to test each and every device produced in a product model line manufactured for sale to the public. We seek comment on whether this would be an effective testing framework for EAS software. Are there any unique applications or considerations involving EAS software that might not be accounted for under this framework? Are there any alternatives methods to this representative testing approach we should consider? Commenters that offer alternatives should comment on benefits and burdens for EAS software vendors, EAS Participants, and Commissions staff.

110. We also seek comment on whether and which modifications to certified EAS software should require recertification. If we were to apply the part 2 certification framework to EAS software, section 2.1043 of the Commission's rules delineates the types of modifications (or permissive changes) that manufacturers can make to previously certified equipment without requiring equipment recertification.[354] The permissive change rules primarily apply to changes involving electrical and RF circuitry, but include provisions covering changes to software installed in software-defined radios (SDR), which are treated as Class III permissive changes.[355] These provisions trigger where the software modification "changes the frequency range, modulation type or maximum output power (either radiated or conducted) outside the parameters previously approved, or that change the circumstances under which the transmitter operates in accordance with Commission rules."[356] We seek comment on whether, regardless of what equipment certification or approval framework might be applied to EAS software, a similar approach makes sense for EAS software, and what modifications, if any, to EAS software — and by extension, EAS performance — should require resubmission of certification information (test data, etc.) as the equivalent to a Class II permissive change.[357] We also seek comment on whether software is sufficiently different from physical hardware that it should require a periodic recertification throughout its life cycle, which would represent a fundamentally different approach from the current equipment authorization model. We note that, unlike a physical device that may never be modified, software is typically updated many times, and users sometimes continue to run software after it is no longer supported by the vendor. Updates may address critical and necessary security issues that emerge after initial approval, but such updates can unintentionally disrupt system functions and introduce new and unexpected faults. The use of software that is no longer supported can introduce functional and cybersecurity risks. Parties who support such an approach should discuss how a periodic reapproval process could be implemented, as well as what procedures we might adopt for automatically cancelling certification or approval when software is not recertified within the required time interval. If a certification or approval is automatically cancelled for software, what responsibilities should fall on the developer to notify impacted users and regulatory bodies? Additionally, what actions should be taken to ensure that system integrity and reliability are maintained during and after this process?

(Continued from previous page)

[353] More specifically, the EAS software certification would be a component of and subsumed under the custom-designed product's certification.

[354] *See* 47 CFR § 2.1043. In addition, section 11.34(f) specifies that modifications to existing authorized EAS equipment that are necessary to implement revisions to the EAS codes (set forth in section 11.31) or to implement the selective displaying and logging feature (set forth in section 11.33(a)(4)) are Class I permissive changes. *See* 47 CFR § 11.34(f).

[355] *See* 47 CFR § 2.1043(a), (b)(3).

[356] *Id*.

[357] *See* 47 CFR § 2.1043(b)(2)(i).

111. *Cybersecurity*. We acknowledge concerns raised by commenters responding to the NAB Petition regarding potential risks that EAS software may pose to EAS security. DAS, for example, observes that "[s]oftware systems — especially network-dependent platforms — tend to be far more exposed to cybersecurity threats than standalone hardware."[358] DAS further observes that "[u]nlike physical devices, software platforms have large attack surfaces, including APIs, databases, and remote access points."[359] Sage acknowledges that "[c]ybersecurity is an issue that needs to be taken into account," but disagrees that EAS software poses a unique risk, stating that "the issues are known, and are not fundamentally different than any other IT component of a broadcast facility."[360] Cybersecurity is plainly a cause for concern in the EAS environment, as exemplified by the many hacking incidents that have resulted in false alerts, and in the process, prevented the transmission of legitimate, lifesaving alerts, documented in the above *Report and Order*. We tentatively agree with the Broadcast Warning Working Group that uniformity in EAS performance, regulatory certainty, and overall EAS security are critical to any EAS software configuration.[361] We also tentatively agree with DAS that "[a]s the digital landscape continues to evolve, ensuring the security and integrity of systems involved in the EAS becomes increasingly vital."[362] We seek comment on these views.

112. Accordingly, we propose that, before EAS software can be marketed or used, the responsible party seeking its certification should be required to demonstrate to the Commission that it has taken appropriate steps to secure the software. We seek comment on the most effective way in which we can implement this requirement. Should a Declaration of Conformity with specific standards or best practices, a cybersecurity audit or test report, or other evidence be required to be included in the EAS software's certification application?[363] If so, what specific cybersecurity criteria should the software satisfy? We observe that there are several existing cybersecurity certification programs for software, each with different focuses.[364] Would a certification from one of these programs be best suited to demonstrating the cybersecurity of EAS software? For example, would one or more of the National Information Assurance Partnership's (NIAP) Approved Protection Profiles provide such a set of standards or would an additional profile for EAS software be needed, either alone or in combination with existing profiles? If a new profile is required, how should it be developed, and how long would it take to develop? Additionally, should we require vendors of EAS software to participate in CISA's Secure by Design program?[365] Would cybersecurity certification of EAS software alone be sufficient to ensure the

[358] DAS NAB Petition Comments at 9.

[359] *Id.*; *see also* BWWG NAB Petition Reply Comments at 9 ("[I]f the FCC is going to consider allowing such systems, there needs to be a clear and thoughtful path for certification, cybersecurity compliance, and oversight based on real needs and real risks.").

[360] Sage June 2025 *Ex Parte*.

[361] BWWG *Ex Parte* at 9 ("The BWWG is not opposed to exploring software-based approaches to EAS. But if the FCC is going to consider allowing such systems, there needs to be a clear and thoughtful path for certification, cybersecurity compliance, and oversight based on real needs and real risks.").

[362] DAS NAB Petition Comments at 9.

[363] In general, a Declaration of Conformity is an attestation from the responsible party that the equipment or software has been shown to comply with the applicable technical standards and other applicable requirements of the conformity assessment regime against which it is being issued. *See*, *e.g.*, 47 CFR §§ 2.906, 2.1072, 2.1077.

[364] For example, the National Information Assurance Partnership's Approved Protection Profiles provide a set of standards for assessing software vulnerabilities. *See* Common Criteria Recognition Arrangement, *About Us*, https://www.niap-ccevs.org/ccra (last visited May 30, 2026).

[365] CISA's Secure by Design program encourages self-attestation by software manufacturers whose products and services have been developed in a cybersecurity-aware design process. CISA, *Secure By Design*, https://www.cisa.gov/securebydesign (last visited May 30, 2026).

cybersecurity of the EAS, taken together with the cybersecurity requirements we adopt today? If we were to adopt cybersecurity requirements for EAS software, should we also impose cybersecurity requirements on standalone EAS equipment on a going-forward basis in order to ensure parity? If so, should the cybersecurity criteria for equipment be different than software? Should foreign-produced EAS software be subject to importation and use prohibitions where national security is implicated, for example, where the software designer, manufacturer, or responsible party for certification is on the Covered List?[366]

113. DAS asserts that EAS software will shift many of the responsibilities for implementing secure hardware configurations, maintaining firmware integrity, performing vulnerability testing, and ensuring end-to-end system hardening, which standalone EAS equipment manufacturers handle today, onto EAS Participants, "many of whom may lack the technical expertise or resources to manage them effectively."[367] We seek comment on this view. Does the successful use and maintenance of EAS software require EAS Participants to have more technical and cybersecurity expertise than when using standalone EAS equipment? Do EAS Participants generally have this expertise, or will the use of EAS software by the average EAS Participant introduce serious risks to EAS's performance? Are there any characteristics or features that EAS software should be required to reduce the level of expertise that the EAS Participant would need to have in order to use it successfully? Should we limit the use of EAS software only to certain EAS Participants, and if so, how would EAS Participants demonstrate that they qualify to use it?

114. *Operational Readiness*. We propose to lessen the time that would be afforded to EAS Participants to repair or replace defective EAS software before notifying the Commission from 60 days to 72 hours.[368] Under the current rules, EAS Participants may operate without defective equipment pending its repair or replacement for 60 days without further FCC authority.[369] We observe that 60 days is an amount of time that in most cases may be sufficient for manual repair and shipping of defective equipment to and from the manufacturer.[370] As noted above, however, the record indicates that one of EAS software's main benefits is that it can be expeditiously repaired with rapid fail-over to backup EAS software in an auxiliary location. As the NAB Petition states, "maintenance of a station's EAS system and the time needed to recover from a hardware component malfunction would be greatly reduced because a system repair could now be implemented through a software update, patch, or other remote fix, eliminating the down-time needed to ship the legacy physical device to a manufacturer for factory repair."[371] Based on the record, we believe that EAS software is unlikely to be defective for very long and in many cases, EAS can continue to be provided by backup EAS software. In addition, we believe that EAS software may be more prone to cyberattack by virtue of its IP interconnectedness. Accordingly, there is a heightened need for Commission awareness of lingering EAS software defects that may derive from ransomware, viruses, or other cyberattacks. For these reasons, we tentatively conclude that 72 hours is a reasonable amount of time for an EAS Participant using EAS software to either effectuate repairs or switch over to backup EAS software to ensure EAS is still available until repairs of the EAS software in its main facility are completed. We seek comment on these views. Is 72 hours a reasonable amount of

[366] *See*, *e.g.*, 47 CFR § 2.902.

[367] DAS NAB Petition Comments at 11; *see also* BWWG *Ex Parte* at 5.

[368] *See infra* Appx. B (47 CFR § 11.35(b)).

[369] 47 CFR § 11.35(b).

[370] *See* SBE NAB Petition Comments at 4 ("[E]quipment must sometimes be physically shipped all the way back to the manufacturer for repair (or to be manually updated)."); NTCA Alerting Security NPRM Comments at 6-9 ("[T]he shipping time, distance between locations and the availability (or unavailability) of parts for older equipment can all contribute to delays in repairing EAS equipment.").

[371] NAB Petition at 6. NAB also indicates that EAS software may enable "immediate fail-over functionality," which might prevent operational downtime. *Id.*

time to complete repairs of defective EAS software? Should this amount of time be lowered or increased, and why? What impact would providing more or less time have on the Commission's situational awareness about the state of EAS operational readiness nationwide?

115. We invite commenters to recommend any additional or alternative requirements, changes, or limitations that may be needed to enable the Commission to assure EAS stakeholders and the public that EAS software can reliably meet or exceed all existing EAS operational requirements. Are the requirements we propose today sufficient, overall, to ensure EAS software meets or exceeds the reliability, security, and availability provided by current EAS equipment?[372] If changes to the overall certification and cybersecurity framework for EAS software about which we seek comment above would be beneficial, how should the Commission implement them? Commenters that offer alternatives should comment on benefits and burdens for EAS software vendors, EAS Participants, and Commissions staff.

116. We previously observed that, according to the Bureau's last nationwide EAS test report, an appreciable number of EAS Participants were unable to participate in testing due to equipment failure – despite advance notice that such test was to take place – suggesting that equipment failures are not addressed by EAS Participants as swiftly as reasonably possible and that more needs to be done to improve EAS operational readiness.[373] As discussed above, we believe that allowing the use of EAS Software could expedite repairs. Would allowing the use of EAS software also have an effect on the average amount of time needed to repair dedicated EAS devices? For example, would the entry of EAS software into the market reduce the number of EAS devices that need to be repaired at any given time, improve the availability of vendors' repair teams, and therefore reduce wait times and repair speed? If so, should we modify our operational readiness rules for dedicated EAS devices to reflect that less repair time is needed?

117. Finally, we observe that section 11.35(c) currently requires EAS Participants who require more than 60 days to repair or replace defective EAS equipment to submit an informal request for additional time to the Regional Director of the FCC field office serving the area in which the EAS Participant is located, or in the case of DBS and SDARS providers, to the Regional Director of the FCC field office serving the area where their headquarters is located.[374] To simplify this process for EAS Participants, we propose to require EAS Participants to file such informal request with the Public Safety and Homeland Security Bureau instead of the Regional Director of the FCC field office for their area. We believe this modification will make filing such requests far simpler for affected EAS Participants and improve the Bureau's situational awareness of EAS outages across the country. We seek comment on this proposal.

2. Retiring 90-character WEA Messages

118. To reduce outdated and unnecessary compliance burdens for WEA, we propose to retire the requirement that Participating CMS Providers support transmission of an 90-character-maximum Alert Message "on and only on those elements of its network incapable of supporting a 360 character Alert Message."[375] This requirement is in addition to the 360-character maximum version.[376] As a

[372] *See infra* Appx. B (Proposed Rules).

[373] *Alerting Security NPRM*, 37 FCC Rcd at 12938, para. 9 (*citing* FCC, Report: August 11, 2021 Nationwide EAS Test at 14-16, 19 (2021), https://docs.fcc.gov/public/attachments/DOC-378861A1.pdf (describing that, out of 19,174 test participants in an August 11, 2021 nationwide test of EAS conducted by FEMA in coordination with the Commission, 389 test participants reported equipment performance issues on receipt and 565 on retransmission, with these participants generally reporting that equipment was out for repair, failed during the test, was missing, or malfunctioned)).

[374] 47 CFR § 11.35(c).

[375] 47 CFR § 10.430 ("A Participating CMS Provider must support transmission of an Alert Message that contains a maximum of 360 characters of alphanumeric text. If, however, some or all of a Participating CMS Provider's (continued….)

practical matter, this rule has meant that alerting authorities *must* submit a 90-character-maximum version of each WEA they transmit to ensure their alert can transit all networks and *may* also initiate a 360-character-maximum version to improve readability.[377] The Santa Barbara County Office of Emergency Management recommends that we sunset the requirement to transmit a 90-character-maximum version of WEA messages because its length is "insufficient for modern public alerting," and "[i]ts continued existence creates inconsistency in public messaging and hampers our ability to clearly convey life-saving information during time-sensitive emergencies."[378] The King County, Washington Office of Emergency Management echoes this concern, adding that "[t]he five mandatory elements in a WEA message can be very difficult to fit into an understandable 90-character text."[379] The New York State Division of Homeland Security and Emergency Management's comment suggests that the requirement to support two versions of every WEA message risks confusion for alerting authorities.[380] We believe that retiring the 90-character alert will empower alerting authorities to stop creating two versions of each alert message and would save time and resources during emergencies in which every second matters. We seek comment on these views. Are there other ways in which retiring 90-character WEA messages will benefit alerting authorities? We also seek comment on whether retiring 90-character WEA messages would have benefits for other WEA stakeholders as well. For example, we anticipate that our proposal will allow Participating CMS Providers to conserve network resources when transmitting WEA messages. Would any benefits to public safety arise from conserving these resources during emergencies? Will conserving these resources help Participating CMS Providers better support future opportunities to improve WEA? Are there any other network resource-conserving changes to the Commission's WEA rules that we should consider?

119. We seek comment on the extent to which legacy networks that were incapable of being upgraded to support 360-character-maximum WEA messages in 2016 remain in service today. When the Commission adopted the current requirement in 2016, it found that "[a] 360-character maximum Alert Message length balances emergency managers' needs to communicate more clearly with their communities with the technical limitations of CMS networks."[381] The Commission noted that it should continue to allow Participating CMS Providers to transmit 90-character-maximum Alert Messages on legacy networks until those networks are retired.[382] We understand that many Participating CMS Providers either have already retired or are actively retiring their 2G and 3G networks.[383] According to

(Continued from previous page)
network infrastructure is technically incapable of supporting the transmission of a 360-character maximum Alert Message, then that Participating CMS Provider must support transmission of an Alert Message that contains a maximum of 90 characters of alphanumeric text on and only on those elements of its network incapable of supporting a 360 character Alert Message.").

[376] 47 CFR § 10.430. In 2023, the Commission sought comment on whether it should sunset the requirement to transmit a 90-character maximum version of a WEA alert. *2023 WEA FNPRM*, 38 FCC Rcd at 3753, para. 24. Several parties submitted comments on this proposal. *See*, *e.g.*, San Diego OES Comments at 2-3.

[377] *See* Snohomish DEM Alerting Modernization NPRM Comments at 2 (explaining challenges with the existing 90- and 360-character limits).

[378] Santa Barbara County Office of Emergency Management Comments, PS Docket No 25-224, at 2 (rec. Sept. 25, 2025); *see also* USGS Alerting Modernization NPRM Comments at 7 (stating that 90 characters of text has always been inadequate).

[379] King OEM Alerting Modernization NPRM Comments at 3; *see also* USGS Alerting Modernization NPRM Comments at 2-3 ("[T]he original 90-character text message size in the WEA system was inadequate and had to be increased to 360 characters . . . ").

[380] NY DHSES Alerting Modernization NPRM Comments at 3.

[381] *2016 WEA R&O*, 31 FCC Rcd at 11120, para. 11.

[382] *Id.* at 11122, para. 13.

the Master WEA Registry and the FCC's Broadband Data Collection, however, at least some wireless providers continue to operate 3G networks, primarily in the U.S. territories.[384] Which, if any, currently deployed networks can still only support 90-character maximum WEA messages? To what extent do Participating CMS Providers and their subscribers continue to rely on these networks for the delivery of WEA messages? If any Participating CMS Providers continue to rely upon networks that still cannot be upgraded to support 360-character-maximum WEA messages, we seek comment on those providers' timelines for sunsetting those networks. Understanding when small- and medium-sized businesses, in particular, plan to sunset any such network would allow us to consider setting an effective date for the elimination of this requirement that fits into planned business cycles. Alternatively, what consequences might result if we were to eliminate the requirement to transmit 90-character-maximum versions of WEA messages before all deployed networks are able to support 360-character-maximum messages? To what extent could this diminish the availability of WEA? Would there be specific geographic regions in which those impacts would be experienced most acutely? How should we weigh these concerns against the communication limitations of 90-character-maximum messages?

120. We seek comment on whether, as a result of eliminating this requirement, some mobile devices may also no longer be able to receive WEAs at all. To what extent have mobile devices that only support 90-character messages already churned out of the market? Data from the 2023 nationwide WEA test found that 2.2% of devices only supported a 90-character-maximum alert.[385] We seek comment on whether the proportion of legacy devices in the field has further declined since October 2023, when the test was conducted. Could any other negative impacts result from sunsetting 90-character-maximum WEA messages? To the extent that WEA may not be available in some geographic areas as a result of this change, would it significantly reduce the ability of alerting authorities to reach the public in those areas? Are reasonable substitutes available for WEA in those areas, such as EAS, private mass notification systems, highway signs, social media, and public news reports? Should we recognize any cost to Participating CMS Providers in needing to update systems and standards to end the transmission of 90-character WEA messages?

F. Analysis of Costs and Benefits

1. Benefits

121. We seek comment on the benefits of the proposals in this *Further Notice*. While these benefits are difficult to quantify,[386] we believe the proposals to modernize the nation's alerting systems

(Continued from previous page)

[383] *See*, *e.g.*, T-Mobile, *T-Mobile Network Evolution*, https://www.t-mobile.com/support/coverage/t-mobile-network-evolution (last visited Feb. 5, 2026); Mike Dano, *More 2G and 3G shutdowns loom in the US* (Nov. 28, 2023), https://www.lightreading.com/2g-3g-4g/more-2g-and-3g-shutdowns-loom-in-the-us.

[384] *See* Master WEA Registry (Nov. 2023), https://www.fcc.gov/sites/default/files/WEA-MasterRegistry11212023.xlsx (reflecting that Vitelcom Cellular dba Innovative Wireless, GCI Communication Corp, NE Colorado Cellular dba Viaero Wireless, Smith Bagley, Inc. dba CellularOne, Puerto Rico Telephone Company, Inc. dba CLARO, AST Telecom, LLC dba Blue Sky Communication, and Union Telephone Company participate in WEA); *see also* FCC, Broadband Data Collection, https://www.fcc.gov/BroadbandData (last visited Jun. 1, 2026) (reflecting that these companies also continue to operate 3G networks).

[385] Andrew Parker et al., RAND Homeland Security Operational Analysis Center (HSOAC), Assessing Public Reach of the 2023 National Test of the Wireless Emergency Alerts (WEA) System at 36 (2024), https://www.rand.org/content/dam/rand/pubs/research_reports/RRA2400/RRA2451-1/RAND_RRA2451-1.pdf (listing 17% of devices' WEA capability as "[u]ncharacterized," which also may include some WEA 1.0 devices). In the Bureau's 2022 WEA testing—which was conducted on a voluntary basis and thus may not have been an entirely representative cross-sample—only 1.1% of devices were of the type that is solely capable of supporting 90-character maximum messages, while 98.9% of devices supported 360-character maximum messages. *See* WEA Performance Exercise Report at 7.

will result in greater prevention of property damage, injuries, and loss of life. We seek comment on this assessment and whether any enhancements to our proposals would make our nation's alerting systems more resilient and more likely to save lives, prevent injuries, or protect property.

122. *Securing EAS Through Message Authentication.* We tentatively conclude that our proposal to secure EAS through message authentication will further enhance EAS security beyond the protections offered by the rules we adopt today in the *Report and Order*. We believe our proposal to require EAS Participants to reject unauthenticated EAS messages (where there is no valid digital signature) would prevent false alerts in three ways that would further our core objective of ensuring that alerting authorities can rapidly notify the public of emergencies. First, allowing EAS Participants to only transmit authenticated EAS messages would prevent malicious actors from injecting false information into an alerting authority's message; second, it would prevent malicious actors from modifying, or tampering with, the content of an otherwise valid alert without authorization; and third, it would prevent malicious actors from posing as (or spoofing) a valid alerting authority to trick an EAS Participant into broadcasting a false alert. Protecting against these false injections, tampering, and/or spoofing would help protect life and property. We seek comment on this assessment.

123. As we reasoned in the accompanying *Report and Order*, false EAS messages can disrupt the U.S. economy. The economic benefits of preventing even a 0.00043% disruption of the U.S. economy in a single year through EAS authentication would offset the one-time EAS software update costs that we discuss below.[387] Likewise, the local radio and television broadcasting sector a subset of EAS Participants, supported $1.19 trillion of the nation's GDP in 2025,[388] so preventing a disruption of even 0.0011% in a single year would offset the one-time EAS software update costs.[389] Are there other ways to quantify the benefits to EAS security that message authentication would deliver?

124. *Bolstering the Reliability of Emergency Alerts.* We believe our proposals to bolster the reliability of emergency alerts will advance our goal of rapidly notifying the public of emergencies that may put them at risk. We believe they will do so by minimizing delays in receipt and increasing consumer awareness and action in response to alerts. We tentatively conclude that requiring alerting participants to use a universal alert message identifier and ensuring consistent transmission of WEA messages will allow for more timely delivery of alerts and minimize unnecessary duplicate alerts. Especially during fast-moving disasters such as a wildfire or a flash flood, we believe these proposals will improve alerting authorities' ability to reach people in targeted areas by using EAS and WEA and help ensure that the public is receiving alerts that are relevant to them. This, in turn, will maximize the likelihood that people will take protective action that may be necessary to save lives and property. We also believe a universal alert message identifier for both EAS and WEA would have the added benefit of minimizing duplicate alerts and avoiding alert fatigue. We seek comment on these conclusions and on other ways to quantify the impact of more narrowly tailored emergency alerts for faster and more effective protective actions taken by the public during disasters, as well as decreased alert fatigue.

(Continued from previous page)

[386] *See Resilient Networks Order*, 37 FCC Rcd at 8075, para. 46 ("it would be impossible to quantify the precise financial value of these health and safety benefits"); *2018 WEA and EAS Order*, 33 FCC Rcd at 7100, para. 34 ("To provide an estimate of the value of the benefits of the rules we adopt today, we turn to the overall value of the EAS. Scholars agree that public safety in the United States has improved over the years because its early warning systems for recurring hazards such as lightning, floods, storms and heat waves are continually improving.").

[387] $13,000,000/$30,000,000,000,000 ~ 0.000043%.

[388] Woods & Poole Economics, *Local TV and Radio: Helping Drive the United States Economy* at 1 (2025), https://www.wearebroadcasters.com/documents/2025-NAB-Woods-Pooles-Local-Broadcasting-Publication.pdf.

[389] $13,000,000/$1,190,000,000,000 ~ 0.0011%.

125. *Improving the Accuracy of Alert Geotargeting.* Our proposals to improve geotargeting support our goal of providing alerting authorities with the ability to rapidly notify the public of emergencies that may put the public at risk. As we have previously concluded, we believe strengthening alert geotargeting will prevent alert fatigue, minimize consumer opt-out, increase consumer trust in alerting systems by preventing alerts from being delivered to consumers for whom the message is not relevant, and reduce the number of calls to 911 and therefore reduce the number of emergency responses.[390] When consumers receive a geotargeted message in an emergency situation, they may have time to reach a safe location or take other action to avoid the need for 911 assistance. This will benefit first responders, who will be able reduce emergency deployments and direct their efforts to other critical areas.[391] We continue to believe that improving geotargeting will make it more likely that alerting authorities will use EAS and WEA in situations where it can save lives and prevent injuries.[392] Over three recent years (2022-2024), there were a total of 3,401 fatalities and a total of 5,648 injuries from weather events in the United States.[393] If enhancements to alert geotargeting resulted in even a 0.1% reduction in fatalities, injuries, and emergency response costs during 2022-2024, these enhancements could have resulted in, on average, a life saved each year.[394] As of 2011, first responders were deployed at least 456,250 times per year in the United States at a cost of approximately $3,500 per deployment.[395] A one percent reduction in emergency response costs, over the first three years these rules are in effect, would save at least $48 million pursuant to these 2011 figures, so we believe the current cost is likely higher.[396] As discussed below, this is greater than the one-time compliance cost to update the standards and software necessary to comply with the WEA-related proposals. We seek comment on the applicability of this analysis to the enhanced geotargeting proposals at issue in this item. We also seek comment on ways to quantify these benefits. Are there other benefits related to enhanced geotargeting of WEA and EAS that we should consider?

126. *Enhancing Alert Effectiveness.* We believe our proposals to ensure that alerts are quickly and easily understandable advance our core alerting goals to deliver instructions that protect life and property, as well as to provide additional authoritative communications with the public before, during, and after an emergency. Specifically, we believe that requirements to establish a common symbology for alerts and amplify the perceived urgency of WEA earthquake alerts, if adopted, would hasten protective

---

[390] *See 2018 Second WEA R&O*, 33 FCC Rcd at 1343-47, paras. 38-46 (quantifying the benefits on enhancing WEA geo-targeting the last time the Commission took action to do so).

[391] *See id.*

[392] *See id.*

[393] National Weather Service, *Summary of Natural Hazard Statistics for 2024 in the United States* (March 24, 2026), https://www.weather.gov/media/hazstat/sum24.pdf (1,428 fatalities and 1084 injuries); National Weather Service, *Summary of Natural Hazard Statistics for 2023 in the United States* (Dec. 5, 2024), https://www.weather.gov/media/hazstat/sum23.pdf (1050 fatalities and 3,364 injuries); National Weather Service, *Summary of Natural Hazard Statistics for 2022 in the United States* (Feb, 2, 2024), https://www.weather.gov/media/hazstat/sum22.pdf (860 fatalities and 1200 injuries). 1,428 + 1050 + 869 = 3,401 fatalities. 3,401 / 3 = an average of 1,134 fatalities per year. 1084 + 3364 + 1200 = 5,648 injuries. 5,648 / 3 = 1,883.

[394] 1,428 (2024 fatalities) + 1050 (2023 fatalities) + 869 (2022 fatalities) = 3,401 total fatalities (2022-2024). 3,401 total fatalities × 0.1% ~ 3 lives saved during this 3-year period of time.

[395] *See 2018 Second WEA R&O*, 33 FCC Rcd at 1346, para. 45; Alex Tabarrok, *Firefighters Don't Fight Fires* (Jul. 18, 2012), http://marginalrevolution.com/marginalrevolution/2012/07/firefighters-dont-fight-fires.html (citing John Donovan, *Fire Department Takes Medical Calls in Stride* (Mar. 24, 2010), http://abcnews.go.com/Nightline/firefighters-medical-calls-health-costs/story?id=10181852#.UABoKB3yw1e).

[396] $48,000,000 ~ 3 years × 456,250 deployments per year × $3,500 per deployment.

actions in situations where life and property are at risk, especially for people with disabilities or limited English proficiency. We seek comment on this assessment. We also seek comment on ways to quantify the benefits associated with faster recognition and understanding of alerts through the use of common, standardized symbology, and of earthquake alerts, in particular.

127. *Removing Unnecessary Alerting Requirements.* We tentatively conclude that allowing EAS Participants to replace their dedicated EAS equipment with EAS software and retiring the 90-character-maximum WEA message will advance the core goal of providing alerting authorities with the ability to rapidly notify the public of emergencies. As discussed above with regard to other security enhancing proposals, as EAS software becomes more accessible, we expect EAS Participants that choose to implement it may be able to avoid costly cyberattacks that disrupt their business and require investments in mitigation and recovery. Additionally, we believe installing EAS software as an alternative to stand-alone EAS equipment may make it easier for EAS Participants to stay up to date with security patches, performance updates, and other software updates to enhance the resiliency and reliability of their systems. We seek comment on this assessment. We also agree with commenters that having a software-only option would save EAS Participants the higher cost of maintaining dedicated EAS decoder equipment.[397] We seek comment on how to quantify those cost savings. What are the average maintenance and upgrade costs associated with maintaining dedicated EAS hardware? Will the exit of a major EAS equipment manufacturer from the market affect these costs going forward?[398] If so, how? Moreover, the *Further Notice* seeks comment on adopting NAB's approach to make software-based EAS permissive and therefore does not impose mandatory costs. As such, EAS Participants whose costs would outweigh the benefits of installing EAS software would not be required to do so. We seek comment on these tentative conclusions.

128. Further, we believe that retiring the requirement to support 90-character-maximum messages would enable alerting authorities to avoid redundancies and send one single version of a WEA message more quickly, rather than a 90-character-maximum message and a 360-character-maximum message. We believe eliminating the requirement that, as a practical matter, forces alerting authorities to create two WEA messages would lessen the burden on alerting authorities and shorten the time it takes alerting authorities to issue an alert, which is particularly important in emergency situations when giving people a few seconds more time to respond could make a significant difference. We also believe that this will reduce burdens on Participating CMS Providers because their networks will no longer need to parse multiple versions of alerts for distribution among various generations of wireless technology. We seek comment on ways to quantify these benefits. We also seek comment on the public safety benefits.

2. Costs

129. We seek comment on the costs that alerting participants would expect to incur to comply with the rule changes proposed in this *Further Notice*. We believe the costs associated with each of these proposed rules will fall into one of the following categories: EAS software updates, EAS software authorization, EAS-related hardware replacement, WEA standards and testing, and WEA-related network configuration changes. We estimate that, taken together, these costs will not exceed $52.5 million.[399] Even accounting for the estimated economic benefits of just one proposal, EAS authentication, discussed above, we believe the benefits of the proposals in this *Further Notice* will far outweigh the costs.

---

[397] *See* Daniel Brown Comments, PS Docket No. 15-94 (rec. Apr. 4, 2025); Letter from Jeff Schefke to Marlene H. Dortch, Secretary, FCC, PS Docket No. 15-94, at 1 (filed May 15, 2025); Craven County *Ex Parte*, at 1 .

[398] *See* Sage Alerting Systems, *ENDEC 3644 Hardware* (Apr. 24, 2024), https://www.sagealertingsystems.com/.

[399] The $52.5 million one-time cost includes $13 million in EAS software updates and $39.5 million in WEA updates.

130. *EAS Software Updates.* We estimate that EAS Participants would incur no more than $13 million in one-time costs to make the necessary software updates to comply with the proposed changes to CAP authentication and add new locations codes as adopted by the Bureau. If we were to require adoption of a universal alert message identifier and common symbology for CAP-based EAS messages, those costs would also be included in this estimate, insofar as those software updates could also be implemented at the same time. With respect to changes involving software modifications to EAS equipment, the Commission has previously conducted a cost estimate that we believe is relevant.[400] In the *MEP Report and Order*, which established a dedicated Missing and Endangered Persons (MEP) event code for EAS, the Commission adopted a ceiling of five hours of labor to implement EAS event code rule changes.[401] We also note that incremental EAS software update costs could be avoided by implementing the relevant changes in conjunction with previously scheduled software updates.[402] Thus, assuming software updates to EAS equipment that update CAP authentication settings, add location codes, use a universal alert message identifier, or support common symbology can also be implemented in the normal course of business,[403] we estimate that implementation costs for one-time necessary EAS software updates would not exceed $13 million, adjusted for inflation.[404] We seek comment on this analysis and on the cost to EAS equipment manufacturers to create these updates.

131. If we were to require EAS Participants to display EAS-related symbols on television screens, we expect that EAS Participants would need to make additional changes to their systems beyond updating their EAS equipment. What systems or equipment would EAS Participants need to modify to

[400] *See Wireless Emergency Alerts; Amendments to Part 11 of the Commission's Rules Regarding the Emergency Alert System*, PS Docket Nos. 15-91, 15-94, Report and Order, 39 FCC Rcd 9150, 9168-69, paras. 48-49 (2024) (*MEP Report and Order*); *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, 10824-25, para. 25 (2017) (*BLU Report and Order*).

[401] *MEP Report and Order*, 39 FCC Rcd at 9168-69, paras. 48-49; *Wireless Emergency Alerts; Amendments to Part 11 of the Commission's Rules Regarding the Emergency Alert System*, PS Docket Nos. 15-91, 15-94, Notice of Proposed Rulemaking, 39 FCC Rcd 2788, 2800, para 35 & n.78 (2024) (*MEP NPRM*).

[402] *See MEP Report and Order*, 39 FCC Rcd at 9168-69, para. 48; *MEP NPRM* 39 FCC Rcd at 2800-01, paras. 34-35 *BLU Report and Order*, 32 FCC Rcd at 10824-25, para. 25.

[403] *See Amendment of Part 11 of the Commission's Rules Regarding the Emergency Alert System*, PS Docket No. 15-94, Report and Order, 37 FCC Rcd 11844, 11867-68, para. 61 (2022) (finding, with respect to the header code changes adopted in that item, that "most EAS Participants will have sufficient time to avoid [] labor cost by downloading the required software changes together with their general software upgrades . . . most of which can be bundled with 'normally scheduled software releases' and performed at the same time . . . ").

[404] We calculate the total cost as follows: $99.24/hour × 5 hours × 25,800 broadcasters, cable headends, SDARS, and DBS providers = $12,801,964, which we round to $13 million. Using an average hourly wage of $63.53 for software and web developers, programmers, and testers, and factoring in a 46% markup of hourly wage for benefits ($63.53 × 46% = $29.22), and a 7% inflation adjustment between 2024 and 2026, we estimate an hourly compensation of $99.24/hour. *See* Bureau of Labor Statistics, *Table 1. National employment and wage data from the Occupational Employment and Wage Statistics survey by occupation, May 2025*, https://www.bls.gov/news.release/ocwage.t01.htm (showing that the hourly median wage for software and web developers, programmers, and testers is $63.53). According to the Bureau of Labor Statistics, as of December 2025, civilian wages and salaries averaged $33.45/hour and benefits averaged $15.33/hour. Bureau of Labor Statistics, *Employer Costs for Employee Compensation – December 2025* (Mar. 20, 2026), https://www.bls.gov/news.release/pdf/ecec.pdf. Total compensation therefore averaged $33.45 + $15.33 = $48.78. Using these figures, benefits constitute a markup of $15.33/$33.45 = 46%. We therefore markup wages by 46% to account for benefits. Adjusting for inflation, the hourly compensation is approximately $99.24 (= ($63.53 + $29.22) × 107%). *See* Federal Reserve Bank of St. Louis, *Average Hourly Earnings of All Employees, Total Private* (*CES0500000003)*, https://fred.stlouisfed.org/series/CES0500000003 (last visited Mar. 27, 2026) (*Inflation Adjustment*) (showing that according to Bureau of Labor Statistics data the average hourly private wage increased by 7% between May 2024 and March 2026).

support the display of EAS-related symbols on television screens? How would they need to be modified, and how should the cost of those modifications be quantified? Are there differing costs associated with different ways of displaying symbols on the screen? If so, what would be the most cost-effective approach to displaying symbols? Are there steps that the Commission can take or changes it can make to its proposal to mitigate implementation costs?

132. *EAS Software Certification*. We seek comment on the costs to EAS software vendors that would arise from requiring them to obtain Commission authorization prior to selling or EAS Participants using their software. What is the cost associated with seeking Commission authorization for EAS devices that are currently permitted under our rules? In what ways is the authorization process for EAS software that we propose above different? Commenters on this issue should quantify the costs associated with each of those differences. How many vendors are expected to seek authorization for EAS software? Because the use of EAS software is voluntary, and the vendors would only seek Commission authorization for their EAS software when their assessed economic gains outweigh the costs of such authorization, we tentatively conclude this proposal would result in net gains despite any certification costs that may arise from the use of EAS software. We seek further comment on our preliminary conclusion.

133. *EAS-related Hardware Replacement.* While we believe most of the issues we seek comment on will be implemented through software modifications, others, such as legacy EAS authentication and implementation of a universal alert identifier for legacy EAS would likely involve the changes to the EAS header codes. As a result, these changes may ultimately require replacement of EAS equipment, National Weather Radio receivers, or other types of equipment involved in the generation and reading of the existing EAS header codes. We seek comment on whether these changes would require the replacement of certain types of equipment, as well as the associated replacement costs. We believe these costs would be minimized if our associated compliance timeframes allowed EAS Participants to naturally replace their EAS equipment with its normal business lifecycle rather than require the equipment to be removed from service early to satisfy a compliance deadline. We seek comment on this belief. If we were to set a compliance deadline that was aligned with natural equipment replacement cycles, what is the normal lifespan for the types of equipment that would need to be replaced to effectuate these requirements?

134. *WEA Standards and Testing.* For WEA, we estimate that Participating CMS Providers would incur a maximum $39.5 million industry-wide,[405] one-time compliance costs to update the standards and software necessary to comply with the WEA-related proposals we put forth today. We also note that participation in WEA is voluntary, so CMS Providers would only incur these costs if they choose to participate. Consistent with the Commission's assessment in the *2023 WEA Third Report & Order*,[406] we estimate that that Participating CMS Providers would incur a maximum $318,427 cost to develop new standards to prevent duplicate alerts through a universal alert message identifier and eliminate outdated exceptions to WEA geotargeting. If we were to adopt rules requiring amplification of WEA earthquake alerts and retirement of 90-character WEA messages, necessary updates to the standards to comply with those rules would also be included in the same standards development process. We quantify the $318,427 cost of modifying standards as the annual compensation for 30 network engineers compensated at the national average wage for their field ($65.33/hour),[407] plus a 46% mark-up for

[405] The total one-time cost of $39.5 million includes: $318,427 in standards development and modifications + $11,500,614 in software modification + $27,601,474 in software testing + $66,337 in WEA configuration changes = $39,486,852, rounded to $39.5 million.

[406] *Wireless Emergency Alerts; Amendments to Part 11 of the Commission's Rules Regarding the Emergency Alert System*, PS Docket Nos. 15-91, 15-94, Third Report and Order, 38 FCC Rcd 10116, 10150-52, paras. 64-65 (2023) (*2023 WEA Third R&O*).

benefits ($30.05/hour),[408] and a 7% inflation adjustment between 2024 and 2026,[409] working for 26 hours a year for a maximum of four distinct standards.[410]

135. In addition to standards development and modifications, we further estimate a one-time cost of $36.5 million for WEA software updates, including $11.5 million for software modifications and $25.8 million for software testing. The Commission has previously quantified the cost of modifying WEA software as the compensation of a software developer compensated at the national average for their field ($135,910/year), plus annual benefits ($62,519/year), working for the amount of time it takes to develop software (10 months) at each of the 65 CMS Providers that participate in WEA.[411] The Commission has also quantified the cost of testing these modifications (including integration testing, unit testing and failure testing) to require 12 software developers compensated at the national average for their field working for two months at each of the 65 CMS Providers that participate in WEA.[412] We have used the same framework since 2016 for changes to software, ranging from enhanced geotargeting to alert

(Continued from previous page)

[407] *See* Bureau of Labor Statistics, *Occupational Employment and Wage Statistics, Occupational Employment and Wages, May 2022*, *15-1241 Computer Network Architects*, https://www.bls.gov/oes/current/oes151241.htm (last visited Apr. 17, 2026) (stating that the mean hourly wage for a computer network architect is $65.33/hour).

[408] According to the Bureau of Labor Statistics, as of December 2025, civilian wages and salaries averaged $33.45/hour and benefits averaged $15.33/hour. Total compensation therefore averaged $33.45 + $15.33 = $48.78. Bureau of Labor Statistics, *Employer Costs for Employee Compensation – December 2025* (Mar. 20, 2026), https://www.bls.gov/news.release/pdf/ecec.pdf. Using these figures, benefits constitute a markup of $15.33/$33.45 = 46%. We therefore markup wages by 46% to account for benefits.

[409] *See* Federal Reserve Bank of St. Louis, *Average Hourly Earnings of All Employees, Total Private (CES0500000003)*, https://fred.stlouisfed.org/series/CES0500000003 (last visited Mar. 27, 2026) (*Inflation Adjustment*) (showing that, according to Bureau of Labor Statistics data, the average hourly private wage increased by 7% between May 2024 and February 2026).

[410] The four standards that likely would need to be revised include J-STD-101 (Joint ATIS/TIA CMAS Federal Alert Gateway to CMSP Gateway Interface Specification), ATIS-0700008 (Cell Broadcast Entity (CBE) to Cell Broadcast Center (CBC) Interface Specification); ATIS-0700010 (CMAS via EPS Public Warning System Specification); and J-STD-100 (WEA Mobile Device Behavior Specification). After adjusting the 7% inflation, the hourly compensation is $102.06 (= ($65.33 + $30.05) × 107%). Multiplying it by the number of engineers, hours worked, and the number of standards, the one-time cost is calculated as follows: 30 network engineers × $102.06 per hour per network engineer × 26 hours per standard × 4 standards = $318,427. *See* Letter from Thomas Goode, General Counsel, ATIS, to Marlene Dortch, Secretary, FCC, PS Docket No. 15-91, at 1 (filed Sept. 6, 2016) (stating that, when standards need to be modified for WEA, it would be common practice for groups of approximately 30 individuals with relevant technical expertise meet approximately bi-weekly for an hour to discuss the modifications).

[411] This is calculated as follows: ($135,910 + $62,519) annually per Participating CMS Provider × 107% inflation adjustment × 10 months / 12 months per year × 65 Participating CMS Providers = $11,500,614. *See* Bureau of Labor Statistics, *Table 1. National employment and wage data from the Occupational Employment and Wage Statistics survey by occupation, May 2025* (May 15, 2026), https://www.bls.gov/news.release/ocwage.t01.htm; Verizon Comments, PS Docket No. 15-91, at 5 (rec. Jan. 13 2016) (stating that it takes manufacturers and vendors 12 months to incorporate new WEA standards into their products and test them); FCC, Master WEA Registry, https://www.fcc.gov/sites/default/files/WEA-MasterRegistry11212023.xlsx (last visited Apr. 1, 2026) (reflecting that 65 CMS Providers participate in WEA either in whole or in part); *see also 2023 WEA Third R&O*, 38 FCC Rcd at 10150-52, paras. 64-65 (using the same cost estimation methodology).

[412] This is calculated as follows: 12 software developers × ($135,910 + $62,519) annually per Participating CMS Provider × 107% inflation adjustment × 2 months / 12 months per year × 65 Participating CMS Providers = $27,601,474. *See 2023 WEA Third R&O*, 38 FCC Rcd at 10150-51, para. 65 (using the same cost estimation methodology).

preservation.[413] We seek comment on whether this remains an appropriate framework and on these cost estimates and the underlying methodology in general.

136. *WEA Configuration Changes.* If we were to require Participating CMS Providers to rebroadcast WEA messages at least once every sixty seconds throughout an alert's active period and cease retransmission of WEA messages with a 24-hour active period five minutes before the end of that period, we do not anticipate that compliance would require the development of new standards or more than *de minimis* software development. We estimate that the necessary changes to configurations and settings of WEA-related systems would require no more than 10 hours per Participating CMS Provider, amounting to an estimated maximum cost of approximately $66,000.[414] We seek comment on this estimate.

G. Compliance Timeframes

137. Below, we propose compliance timeframes for the amendments to the rules discussed in this *Further Notice*. We aim to strike an appropriate balance between the urgent public safety need to improve our nation's alerting systems and alerting participants' need to develop software, practices, and procedures to effectively comply. Where possible, we have grouped compliance timeframes together to reduce implementation burdens. We seek comment on the compliance framework proposed below. Given the importance of EAS and WEA to our nation's safety, we seek comment on the proposed timelines, which we believe are the shortest practicable amount of time within which these measures could be implemented. To the extent an alternative timeframe would be more appropriate, we ask commenters to provide a detailed explanation.

138. *Effective Date for Retiring 90-character WEA Messages.* We propose that the rules to retire 90-character WEA messages should become effective 30 days after publication of the rule in the *Federal Register*.[415] Because we are proposing to eliminate the requirement that Participating CMS Providers support these messages, but are not proposing to outright prohibit their use, we believe that this change can go into effect quickly. Retiring 90-character WEA messages may lead to standards development and technical changes to relevant networks and systems, but we believe it would be appropriate to allow stakeholders to deploy these changes as they become ready rather than set a distant effective date for requiring those changes to occur. We seek comment on this approach. Alternatively, would it promote regulatory clarity and stakeholder coordination to set a target date for the retirement of 90-character messages by all stakeholders after relevant necessary standards and software revisions are prepared? If so, what should that date be?

139. *Effective Date for WEA Message Retransmission and EAS-related Requirements.* We propose that the rules to ensure consistent retransmission of WEA messages, implement EAS location codes as adopted by the Bureau on delegated authority, and authenticate all CAP EAS messages become effective twelve months after publication of the rules in the *Federal Register*.[416] We also propose that rules allowing the use of EAS software become effective either twelve months after publication of the rules in the *Federal Register* or 30 days after the Bureau publishes a notice in the *Federal Register* that Paperwork Reduction Act (PRA) review of rules by the Office of Management and Budget (OMB) is complete, whichever is later. We seek comment on this proposal. We expect that twelve months provides sufficient time for CMS Providers to implement consistent retransmission of WEA messages

[413] *See 2016 WEA R&O*, 31 FCC Rcd at 11168-81, paras. 96-103; *2018 Second WEA R&O*, 33 FCC Rcd at 1344-45, para. 33 ("We received no objections to this approach in the record.").

[414] ($65.33 + $30.05) per hour for a network engineer per Participating CMS Provider × 107% × 10 hours × 65 Participating CMS Providers = $66,337.

[415] *See infra* Appx. B (47 CFR §§ 10.430, 11.2(e), 11.32, 11.33).

[416] *See infra* Appx. B (47 CFR §§ 10.460, 11.55, 11.56).

configuration and settings changes to their systems and for EAS Participants to replace, patch, or reconfigure its EAS equipment to support the EAS-related requirements. We also expect that 12 months would allow the Commission to make sufficient preparations for accepting authorization applications for EAS software, and we anticipate that some vendors may begin developing EAS software in parallel with these efforts. We seek comment on our proposal and expectations. Would any of these requirements require more or less than 12 months to implement, and if so, why? Would authentication of EAS CAP messages require equipment replacement? If we were to set a compliance deadline for EAS CAP authentication that was aligned with natural equipment replacement cycles, what is the normal lifespan for the types of equipment that would need to be replaced to effectuate these requirements? How long would it take for the EAS geotargeting functionality described above to become available to EAS Participants?

140. *Effective Date for Remaining WEA Requirements.* We propose that rules to strengthen WEA geotargeting, prevent duplicate alerts by requiring use of a universal alert message identifier, promote a common symbology for alerts, and amplify WEA earthquake alerts become effective thirty-six months after publication of the rules in the *Federal Register*.[417] We believe these rules, if adopted, will require a longer time period to implement as they may require updates to standards, firmware, infrastructure, and mobile devices. For updates to WEA standards and firmware, the Commission has previously reasoned that it requires industry 30 months to complete—i.e., 12 months to work through appropriate industry bodies to publish relevant standards; another 12 months for Participating CMS Providers and mobile device manufacturers to develop, test, and integrate firmware upgrades consistent with those standards; and six more months to deploy the new technology to the field during normal technology refresh cycles.[418] We also believe that providing an additional six months (for a total of three years) will help reduce costs for Participating CMS Providers in light of number of requirements that we are contemplating would need to be implemented in parallel. We seek comment on this approach. Would requiring the use of a universal alert message identifier require equipment replacement? If we were to set a compliance deadline for use of a universal alert message identifier that was aligned with natural equipment replacement cycles, what is the normal lifespan for the types of equipment that would need to be replaced to effectuate these requirements?

141. Are there benefits that may arise from further aligning these compliance timeframes? We seek comment on alternatives to the tiered timeframes we propose above and on any additional actions that we can take to promote efficient implementation.

V. PROCEDURAL MATTERS

142. *Ex Parte Rules – Permit-But-Disclose*. The proceeding shall be treated as a "permit-but-disclose" proceeding in accordance with the Commission's *ex parte* rules.[419] 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

[417] *See infra* Appx. B (47 CFR § 10.450).

[418] *See 2016 WEA R&O*, 31 FCC Rcd at 11161-62, para. 79.

[419] 47 CFR § 1.1200 *et seq.*

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.

143. *Filing Requirements—Comments and Replies.* 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).

- *Electronic Filers*: Comments may be filed electronically using the Internet by accessing the ECFS: https://www.fcc.gov/ecfs/.
- *Paper Filers*: Parties who choose to file by paper must file an original and one copy of each filing.
    - Filings can be sent by hand or messenger delivery, by commercial courier, or by the U.S. Postal Service. **All filings must be addressed to the Secretary, Federal Communications Commission.**
    - Hand-delivered or messenger-delivered paper filings for the Commission's Secretary are accepted between 8:00 a.m. and 4:00 p.m. by the Commission's mailing contractor at 9050 Junction Drive, Annapolis Junction, MD 20701. All hand deliveries must be held together with rubber bands or fasteners. Any envelopes and boxes must be disposed of before entering the building.
    - Commercial courier deliveries (any deliveries not by the U.S. Postal Service) must be sent to 9050 Junction Drive, Annapolis Junction, MD 20701.
    - Filings sent by U.S. Postal Service First-Class Mail, Priority Mail, and Priority Mail Express must be sent to 45 L Street NE, Washington, DC 20554.

144. *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 (voice).

145. *Paperwork Reduction Act Analysis*. This *Report and Order* does not contain proposed information collections subject to the Paperwork Reduction Act of 1995 (PRA), 44 U.S.C. §§ 3501-3521. In addition, therefore, it does not contain any new or modified information collection burden for small business concerns with fewer than 25 employees, pursuant to the Small Business Paperwork Relief Act of 2002, 44 U.S.C. § 3506(c)(4).

146. The *Further Notice* may contain proposed new or modified information collection requirements. The Commission, as part of its continuing effort to reduce paperwork burdens, invites the general public and the OMB to comment on the information collection requirements contained in this document, as required by PRA. 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.

147. *Congressional Review Act*. The Commission has determined, and the Administrator of the Office of Information and Regulatory Affairs, Office of Management and Budget, concurs, that this rule is non-major under the Congressional Review Act, 5 U.S.C. § 804(2). The Commission will send a

copy of this *Report and Order* to Congress and the Government Accountability Office pursuant to 5 U.S.C. § 801(a)(1)(A).

148. *OPEN Government Data Act*. The OPEN Government Data Act,[420] requires agencies to make "public data assets" available under an open license and as "open Government data assets," i.e., in machine-readable, open format, unencumbered by use restrictions other than intellectual property rights, and based on an open standard that is maintained by a standards organization.[421] This requirement is to be implemented "in accordance with guidance by the Director" of the OMB.[422] The term "public data asset" means "a data asset, or part thereof, maintained by the Federal Government that has been, or may be, released to the public, including any data asset, or part thereof, subject to disclosure under [the Freedom of Information Act (FOIA)]."[423] A "data asset" is "a collection of data elements or data sets that may be grouped together,"[424] and "data" is "recorded information, regardless of form or the media on which the data is recorded."[425]

149. *Regulatory Flexibility Act*. The Regulatory Flexibility Act of 1980, as amended (RFA),[426] requires that an agency prepare a regulatory flexibility analysis for notice-and-comment rulemakings , unless the agency certifies that "the rule will not, if promulgated, have a significant economic impact on a substantial number of small entities."[427] Accordingly, the Commission has prepared a Final Regulatory Flexibility Analysis (FRFA) concerning the possible impact of the rule changes contained in this *Report and Order* on small entities. The FRFA is set forth in Appendix C.

150. The Commission has also prepared an Initial Regulatory Flexibility Analysis (IRFA) concerning the potential impact of rule and policy change proposals on small entities in the *Further Notice*. The IRFA is set forth in Appendix D. The Commission invites the general public, in particular small businesses, to comment on the IRFA. Comments must be filed by the deadlines for comments on the *Further Notice* indicated on the first page of this document and must have a separate and distinct heading designating them as responses to the IRFA.

151. *Providing Accountability Through Transparency* Act. Consistent with the Providing Accountability Through Transparency Act, Public Law 118-9, a summary of this document will be available on https://www.fcc.gov/proposed-rulemakings.

152. *Additional Information*. For further information, please contact George Donato, Associate Division Chief, Cybersecurity and Communications Reliability Division, Public Safety and Homeland Security Bureau, (202) 418-0729, or by email to George.Donato@fcc.gov; or David Kirschner, Attorney-Advisor, Cybersecurity and Communications Reliability Division, Public Safety and Homeland Security Bureau, at (202) 418-0695, or by email David.Kirschner@fcc.gov.

---

[420] Congress enacted the OPEN Government Data Act as Title II of the Foundations for Evidence-Based Policymaking Act of 2018, Pub. L. No. 115-435 (2019), §§ 201-202.

[421] 44 U.S.C. § 3502(20), (22) (definitions of "open Government data asset" and "public data asset"); *id.* § 3506(b)(6)(B) (public availability).

[422] OMB has not yet issued final guidance.

[423] 44 U.S.C. § 3502(22).

[424] *Id.* § 3502(17).

[425] *Id*. § 3502(16).

[426] 5 U.S.C. § 601 et seq., as amended by the Small Business Regulatory Enforcement and Fairness Act (SBREFA), Pub. L. No. 104-121, 110 Stat. 847 (1996).

[427] *Id*. § 605(b).

VI. ORDERING CLAUSES

153. Accordingly, IT IS ORDERED, pursuant to Sections 1, 2, 4(i), 4(n), 301, 303(b), 303(e), 303(g), 303(j), 303(r), 303(v), 307, 309, 316, 335, 403, 624(g), 706, and 713 of the Communications Act of 1934, as amended, 47 U.S.C §§ 151, 152, 154(i), 154(n), 301, 303(b), 303(e), 303(g), 303(j), 303(r), 303(v), 307, 309, 316, 335, 403, 544(g), 606, and 613, as well as by sections 602(a), (b), (c), (f), 603, 604, and 606 of the WARN Act, 47 U.S.C. §§ 1201 (a), (b), (c), (f), 1203, 1204 and 1206, and the National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283, 134 Stat. 3388, § 9201, 47 U.S.C. §§ 1201, 1206, that this *Report and Order and Further Notice of Proposed Rulemaking* IS ADOPTED.[428]

154. IT IS FURTHER ORDERED that the Commission's rules ARE HEREBY AMENDED as set forth in Appendix A and such amendments shall become effective 90 days after publication in the Federal Register.

155. IT IS FURTHER ORDERED that, pursuant to applicable procedures set forth in sections 1.415 and 1.419 of the Commission's rules, 47 CFR §§ 1.415, 1.419, interested parties may file comments on the *Further Notice of Proposed Rulemaking* on or before 30 days after publication in the Federal Register, and reply comments on or before 60 days after publication in the Federal Register.

156. IT IS FURTHER ORDERED that, should no petitions for reconsideration or petitions for judicial review be timely filed, PS Docket No. 22-329 SHALL BE TERMINATED, and the docket will be closed.

157. IT IS FURTHER ORDERED that, pursuant to 47 CFR § 1.407, the Petition for Rulemaking of the National Association of Broadcasters, filed on March 31, 2025, IS GRANTED.

158. IT IS FURTHER ORDERED that the Commission's Office of the Secretary, SHALL SEND a copy of this *Report and Order and Further Notice of Proposed Rulemaking*, including the Final and Initial Regulatory Flexibility Analyses, to the Chief Counsel for the Small Business Administration (SBA) Office of Advocacy.

159. IT IS FURTHER ORDERED that the Office of Managing Director, Performance Program Management, SHALL SEND a copy of this *Report and Order* in a report to be sent to Congress and the Government Accountability Office pursuant to the Congressional Review Act, 5 U.S.C. § 801(a)(1)(A).

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

[428] Pursuant to Executive Order 14215, 90 Fed. Reg. 10447 (Feb. 24, 2025), this regulatory action has been determined to be not significant under Executive Order 12866, 58 Fed. Reg. 51735 (Oct. 4, 1993).

APPENDIX A

FINAL RULES

For the reasons set forth above, the Federal Communications Commission amends 47 CFR part 11 as follows:

Part 11 – EMERGENCY ALERT SYSTEM (EAS)

1. The authority citation for part 11 continues to read as follows:

Authority: 47 U.S.C. 151, 154 (i) and (n), 303(r), 544(g), 606, 1201, and 1206.

2. Amend § 11.35 by adding paragraph (d) to read as follows:

§ 11.35 Equipment operational readiness.

* * * * *

(d) EAS Participants shall employ the following security controls with respect to EAS equipment, studio transmitter link equipment, and any remotely managed equipment that routes, processes, or inserts content into the transmission of the EAS Participant's programming:

(1) Prior to any use to broadcast to the public, EAS Participants shall change any default password, use strong passwords, and change any password if the EAS Participant has reason to believe that the password has been compromised.

(i) A strong password is any password that has a minimum of 15 characters and does not use dictionary words. Instead of using a strong password, EAS Participants may use alternative authentication measures, such as look-up secrets, out-of-band devices, single- or multi-factor one-time password devices, or single- or multi-factor cryptographic authentication, that are reasonably sufficient to mitigate the risk of unauthorized access.

(ii) Passwords employed to comply with this requirement shall not be reused for the EAS Participant's other accounts, equipment, applications, or services.

(2) Install security patches and security-related software and firmware updates issued by equipment manufacturers promptly after those patches or upgrades become available. Security patches and security-related software and firmware updates issued by equipment manufacturers may be tested before they are installed, provided that the testing begins promptly and is completed in a timeframe that is consistent with industry best practices; and

(3) Use a network firewall or comparable network segmentation practice that limits remote management access to authorized devices and authorized users.

APPENDIX B

PROPOSED RULES

For the reasons discussed in this document, the Federal Communications Commission proposes to amend 47 CFR parts 0, 10 and 11 as follows:

Part 0 – COMMISSION ORGANIZATION

The authority citation for part 0 continues to read as follows:

Authority: 47 U.S.C. 151, 154(i), 154(j), 155, 225, 409, and 1754, unless otherwise noted.

1. Amend § 0.392 by redesignating paragraph (l) as paragraph (m) and adding new paragraph (l) to read as follows:

§ 0.392 Authority delegated.

* * * * *

(l) The Chief of the Public Safety and Homeland Security Bureau is delegated authority to revise the Code of Federal Regulations to adopt Emergency Alert System (EAS) location codes for inclusion in § 11.31(f) in response to a request from an alerting authority or State Emergency Communications Committee responsible for emergency alerting in that location.

Part 10 – WIRELESS EMERGENCY ALERTS

2. The authority citation for part 10 continues to read as follows:

Authority: 47 U.S.C. 151, 152, 154(i), 154(n), 201, 301, 303(b), 303(e), 303(g), 303(j), 303(r), 307, 309, 316, 403, 544(g), 606, 1201, 1202, 1203, 1204, and 1206.

3. Revise and republish § 10.430 to read as follows:

§ 10.430 Character limit.

A Participating CMS Provider must support transmission of an Alert Message that contains a maximum of 360 characters of alphanumeric text.

4. Amend § 10.450 by revising paragraph (a) to read as follows:

§ 10.450 Geographic targeting.

* * * * *

(a) A Participating CMS Provider must deliver any Alert Message that is specified by a geocode, circle, or polygon to an area that matches the specified geocode, circle, or polygon.

(1) A Participating CMS Provider is considered to have matched the target area when it:

(i) delivers and displays each Alert Message on 100 percent of opted-in WEA-capable mobile devices that are connected to its network and located in the Alert Message's target area; and

(ii) does not display an Alert Message on WEA-capable mobile devices located more than 0.1 of a mile outside of the Alert Message's target area.

(2) Notwithstanding any other legal or regulatory requirements, any and all location data collected solely for the purpose of conducting WEA geographic targeting shall be:

(i) prohibited from being used for any purpose other than WEA geographic targeting, except as required by statute or law;

(ii) prohibited from being used by the mobile device, software on the mobile device, firmware on the mobile device, and/or any applications on the mobile device, except to conduct WEA geographic targeting and as otherwise required by statute or law;

(iii) prohibited from being transmitted off of the mobile device, including over the airwaves or network of the Participating CMS Provider, except as required by statute or law; and

(iv) deleted immediately after the geotargeting is performed, regardless of whether the geotargeting is successful or unsuccessful, except as required by statute or law.

(3) If a mobile device automatically enables location services upon receipt of a WEA message, location services must be disabled immediately after the device collects or attempts to collect the location data necessary for compliance with the requirements of this section.

* * * * *

5. Revise § 10.460 to read as follows:

§ 10.460 Retransmission frequency.

Participating CMS Providers shall rebroadcast an Alert Message once per minute until the Alert Message expires. For Alert Messages that expire at 24 hours, Participating CMS Providers shall cease rebroadcasting the Alert Message five minutes before the Alert Message's scheduled expiration.

6. Amend § 10.500 by revising paragraph (g) to read as follows:

§ 10.500 General Requirements.

* * * * *

(g) Detection and suppression of presentation of duplicate alerts across Participating CMS Provider networks, including through the use of a universal Alert Message identifier.

* * * * *

Part 11 – EMERGENCY ALERT SYSTEM (EAS)

7. The authority citation for part 11 is revised to read as follows:

Authority: 47 U.S.C. 151, 152, 154 (i) and (n), 301, 303, 307, 309, 316, 335, 403, 544(g), 606, 613, 1201, and 1206.

8. Amend § 11.2 by adding paragraph (e) to read as follows:

§ 11.2 Definitions.

* * * * *

(e) **EAS Software.** Software physically integrated within an EAS Participant's audio and video processing system that performs and/or manages the requirements specified in § 11.32, § 11.33, and §11.56. EAS Software may be installed in a single device (such as a server, personal computer, or custom-manufactured system component), or across multiple components within an EAS Participant's signal processing system, but must be located at the EAS Participant's local facility used to provide service, such as a broadcaster's studio or transmitter site associated with its licensed service area, or cable service provider's headend facility. EAS functions and alerts produced within cloud-based systems, and cloud-based third-party EAS services, are excluded from this definition.

9. Amend § 11.32 by revising paragraphs (a)(2) and (3), (a)(7), (a)(9)(iv) through (vi) to read as follows:

§ 11.32 EAS Encoder.

(a) * * *

(2) ***Inputs.*** The encoder shall have at least one virtual or physical input port used for audio messages and at least one input port used for data messages.

(3) ***Outputs.*** The encoder shall have at least one virtual or physical audio output port and at least one virtual or physical data output port.

* * * * *

(7) ***Indicator.*** An aural or visible means that is activated when the Preamble is sent and deactivated at the End of Message code.

* * * * *

(9) * * *

(iv) ***Time Period for Transmission of Tones***. The encoder shall accurately generate the two tones simultaneously for a time period of 8 seconds.

(v) ***Inadvertent activation.*** The controls used for initiating the automatic generation of the simultaneous tones shall be protected to prevent accidental operation.

(vi) ***Indicator Display***. The encoder shall provide a visual and/or aural indicator which clearly shows that the Attention Signal is activated.

* * * * *

10. Amend § 11.33 by revising paragraphs (a)(4) and (a)(7) to read as follows:

§ 11.33 EAS Decoder.

(a) * * *

(4) ***Display and logging***. For received alert messages formatted in both the EAS Protocol and Common Alerting Protocol, a visual message shall be developed from any valid header codes for tests, national activations, and any preselected header codes received. The message shall at a minimum include the Originator, Event, Location, the valid time period of the message and the local time the message was transmitted. The message shall be in the primary language of the EAS Participant and be fully displayed on the decoder, decoder user interface, or other display available to participant operators and readable in normal light and darkness. The visual message developed from received alert messages formatted in the Common Alerting Protocol must conform to the requirements in §§ 11.51(d), (g)(3), (h)(3), and (j)(2) of this part. EAS decoders must provide a means to permit the selective display and logging of EAS messages containing header codes for state and local EAS events.

* * * * *

(7) ***Outputs***. Decoders shall provide at least one data output port where received valid EAS header codes and received preselected header codes are available, at least one audio output port that is capable of monitoring each decoder audio input, and an internal speaker to enable personnel to hear audio from each

input. EAS Software can comply with the internal speaker requirement by providing an additional audio output capable of driving external speakers.

* * * * *

11. Amend § 11.34 by revising paragraphs (a) through (f) to read as follows:

§ 11.34 Acceptability of the equipment.

(a) An EAS Encoder used for generating the EAS codes and the Attention Signal must be Certified in accordance with the procedures in part 2, subpart J, of this chapter. The data and information submitted must show the capability of the equipment to meet the requirements of this part as well as the requirements contained in part 15 of this chapter for digital devices, with the exception that the requirement to demonstrate compliance with part 15 shall not apply to EAS Software.

(b) Decoders used for the detection of the EAS codes and receiving the Attention Signal must be Certified in accordance with the procedures in part 2, subpart J, of this chapter. The data and information submitted must show the capability of the equipment to meet the requirements of this part as well as the requirements contained in part 15 of this chapter for digital devices, with the exception that the requirement to demonstrate compliance with part 15 shall not apply to EAS Software.

(c) The functions of the EAS decoder, Attention Signal generator and receiver, and the EAS encoder specified in §§ 11.31, 11.32 and 11.33 may be combined and Certified as a single unit or as EAS Software defined in § 11.2(e) provided that the unit or EAS Software complies with all specifications in this rule section.

(d) Manufacturers must include instructions and information on how to install, operate and program an EAS Encoder, EAS Decoder, combined unit, or EAS Software as defined in § 11.2(e) and a list of all State and county ANSI numbers with each unit sold or marketed in the U.S..

(e) Waiver requests of the Certification requirements for EAS Encoders, EAS Decoders, or EAS Software which are constructed for use by an EAS Participant but are not offered for sale will be considered on an individual basis in accordance with part 1, subpart G, of this chapter.

(f) Modifications to existing authorized EAS decoders, encoders combined units, or EAS Software as defined in § 11.2(e) necessary to implement EAS codes specified in § 11.31 will be considered Class I permissive changes that do not require a new application for and grant of equipment certification under part 2, subpart J of this chapter.

* * * * *

12. Revise and republish § 11.35 to read as follows:

§ 11.35 Equipment operational readiness.

(a) EAS Participants are responsible for ensuring that EAS Encoders, EAS Decoders, Attention Signal generating and receiving equipment, Intermediate Devices, and EAS Software used as part of the EAS to decode and/or encode messages formatted in the EAS Protocol and/or the Common Alerting Protocol are installed so that the monitoring and transmitting functions are available during the times the stations and systems are in operation. Additionally, EAS Participants must determine the cause of any failure to receive the required tests or activations specified in § 11.61(a)(1) and (2). Appropriate entries indicating reasons why any tests were not received must be made in the broadcast station log as specified in §§ 73.1820 and 73.1840 of this chapter for all broadcast streams and cable system records as specified in §§ 76.1700, 76.1708, and 76.1711 of this chapter. All other EAS Participants must also keep records

indicating reasons why any tests were not received and these records must be retained for two years, maintained at the EAS Participant's headquarters, and made available for public inspection upon reasonable request.

(b) If an EAS Encoder, EAS Decoder or Intermediary Device used as part of the EAS to decode and/or encode messages formatted in the EAS Protocol and/or the Common Alerting Protocol becomes defective, the EAS Participant may operate without the defective equipment pending its repair or replacement for 60 days without further FCC authority. If EAS Software used as part of the EAS to decode and/or encode messages formatted in the EAS Protocol and/or the Common Alerting Protocol becomes defective, the EAS Participant may operate without the defective equipment pending its repair or replacement for 72 hours without further FCC authority. Entries shall be made in the broadcast station log, cable system records, and records of other EAS Participants, as specified in paragraph (a) of this section, showing the date and time the equipment was removed and restored to service. For personnel training purposes, the required monthly test script must still be transmitted even though the equipment for generating the EAS message codes, Attention Signal and EOM code is not functioning.

(c) If repair or replacement of defective equipment is not completed within 60 days, or 72 hours in the case of EAS Software, an informal request shall be submitted to the Public Safety and Homeland Security Bureau for additional time to repair the defective equipment. This request must explain what steps have been taken to repair or replace the defective equipment, the alternative procedures being used while the defective equipment is out of service, and when the defective equipment will be repaired or replaced.

13. Amend § 11.55 by revising the introductory text of paragraph (d) to read as follows:

§ 11.55 EAS operation during a State or Local Area emergency.

* * * * *

(d) An EAS Participant that participates in the State or Local Area EAS, upon receipt of a State or Local Area EAS message that has been formatted in the Common Alerting Protocol and that has an event code and CAP area segment (using SAME geocodes or polygon/circle coordinates) indicating that it is a type of message that the EAS Participant normally relays, must do the following:

* * * * *

14. Amend § 11.56 by revising paragraph (c) to read as follows:

§ 11.56 Obligation to process CAP-formatted EAS messages.

* * * * *

(c) EAS Participants shall configure their systems to reject all CAP-formatted EAS messages that do not include a valid digital signature.

* * * * *

APPENDIX C

Final Regulatory Flexibility Analysis

1. As required by the Regulatory Flexibility Act of 1980, as amended (RFA),[1] the Federal Communications Commission (Commission) incorporated an Initial Regulatory Flexibility Analysis (IRFA) in the *Modernization of the Nation's Alerting Systems Notice of Proposed Rulemaking* (*Alerting Modernization NPRM*), released in August 2025, and the *Amendment of Part 11 of the Commission's Rules Regarding the Emergency Alert System; Wireless Emergency Alerts; Protecting the Nation's Communications Systems from Cybersecurity Threats* (*Alerting Security NPRM*), released October 2022.[2] The Commission sought written public comment on the proposals in the NPRMs, including comment on the IRFA. The comments received are addressed below. This Final Regulatory Flexibility Analysis (FRFA) conforms to the RFA and it (or summaries thereof) will be published in the Federal Register.[3]

A. Need for, and Objectives of, the Rules

2. The *Report and Order* adopts targeted measures to enhance Emergency Alert System (EAS) security that address the public safety risks arising from breaches of EAS equipment that can result in false alerts or hijacked broadcasts. The Commission requires EAS Participants to do the following with respect to EAS equipment, studio transmitter link equipment, and any remotely managed equipment that routes, processes, or inserts content into the EAS Participant's programming: (1) prior to operation, change any default password, use strong passwords, and change any password if the EAS Participant has reason to believe that the password has been compromised; (2) test and install security patches, security-related software and firmware upgrades issued by equipment manufacturers promptly after those patches or upgrades become available; and (3) use a network firewall or comparable network segmentation practice to limit remote management access to authorized devices and authorized users. These rules support the Commission's goals of strengthening the security of alerting systems to ensure these systems are designed to be secure from attacks by foreign adversaries and other malicious actors. When criminals can gain access to these systems, they can cause alarm by sending out false alerts that cause public panic or deliver false information about crises and disasters. This unauthorized access can also prevent real alerts from being transmitted. The Commission has observed attacks in recent months where threat actors exploited improperly secured, remotely accessible equipment in broadcasters' signal processing systems to gain control of station transmissions and insert unauthorized audio that included EAS tones, offensive language, and promotional content.[4]

---

[1] 5 U.S.C. § 601 *et seq*., as amended by the Small Business Regulatory Enforcement and Fairness Act (SBREFA), Pub. L. No. 104-121, 110 Stat. 847 (1996).

[2] *Modernization of the Nation's Alerting Systems*, PS Docket No. 25-224, Notice of Proposed Rulemaking, 40 FCC Rcd 6695 (2025) (*Alerting Modernization NPRM*); *Amendment of Part 11 of the Commission's Rules Regarding the Emergency Alert System; Wireless Emergency Alerts; Protecting the Nation's Communications Systems from Cybersecurity Threats*, PS Docket Nos. 15-94, 15-91, and 22-329, Notice of Proposed Rulemaking, 37 FCC Rcd 12932 (2022) (*Alerting Security NPRM*).

[3] 5 U.S.C. § 604.

[4] *See Public Safety and Homeland Security Bureau Reminds Broadcasters to Ensure They Comply With Best Practices to Prevent Cyberattacks*, Public Notice, DA 25-996 (PSHSB 2025), https://docs.fcc.gov/public/attachments/DA-25-996A1.pdf; *see also*, *e.g.*, Lance Venta, *ESPN 97.5 Houston Victim of Barix Hack* (Nov. 23, 2025), https://radioinsight.com/headlines/321936/espn-97-5-houston-victim-of-barix-hack/; Katelyn Harlow, *NPR affiliate's backup audio signal hacked, 'offensive material' broadcast in Richmond* (Nov. 21, 2025), https://www.wric.com/news/local-news/npr-affiliates-backup-audio-signal-hacked-offensive-material-broadcast-in-richmond-area/; *Apparent Barix Hacks Highlight Gaps in Cybersecurity, This is not the first time hijackers have attacked Barix boxes to stream explicit content*, Elle Kehres (Sept. 10, 2025), https://www.radioworld.com/news-and-business/apparent-barix-hacks-highlight-poor-cybersecurity-practices.

B. Summary of Significant Issues Raised by Public Comments in Response to the IRFA

3. In 2022, the Commission released a *Notice of Proposed Rulemaking* (*Alerting Security NPRM*) seeking comment on ways to strengthen the operational readiness of EAS equipment.[5] The *Alerting Security NPRM* proposed requiring EAS Participants to report compromises of their EAS equipment, communications systems, and services to the Commission, and also proposed requiring EAS Participants and Commercial Mobile Service providers that participate in Wireless Emergency Alerts (WEA) (Participating CMS Providers) to annually certify that they have a cybersecurity risk management plan in place, and to employ sufficient security measures to ensure the confidentiality, integrity, and availability of their respective alerting systems.[6] The proposal would have required an annual certification attesting that the EAS Participant has created, updated, and implemented a cybersecurity risk management plan that includes security controls sufficient to ensure the confidentiality, integrity and availability of the EAS through the following best practices: 1) changing default passwords prior to operation; 2) installing security updates in a timely manner; 3) securing equipment behind properly configured firewalls or using other segmentation practices; 4) requiring multifactor authentication where applicable; 5) addressing the replacement of end-of-life equipment; and 6) wiping, clearing, or encrypting user information before disposing of old devices.[7] It also proposed requiring Participating CMS Providers take steps to ensure that only valid alerts are being displayed on consumer devices.[8]

4. Several commenters raise concerns about the burdens associated with these specific proposals. In the record of this proceeding, Prometheus Radio Project (Prometheus), NPR, and REC Networks comment on the impact of the proposed rules on small entities.[9] Prometheus comments that it supports cybersecurity best practices for all broadcasters, but notes that compliance will be "onerous for small, rural and LPFM broadcasters, most of whom lack in-house technical expertise and will have to shoulder significant additional financial burden."[10] Prometheus also states that the Commission "must take a more nuanced approach to ensuring the security of EAS equipment, by providing cybersecurity assistance to EAS Participants directly and by placing compliance burden on EAS equipment manufacturers when technically feasible."[11] Prometheus agrees, however, with the Commission's "initiative to strengthen security practices and EAS and supports the implementation of cybersecurity practices for all broadcasters, big and small."[12] NPR agrees that there should be "secure, reliable communications during emergencies without relying on the Internet, which may be offline or become unreliable, particularly during power outages" but raises concerns "that some of the proposed rules would create costly obligations for stations without clear public benefits [and] [s]ome of the proposed rules would be especially burdensome for noncommercial public radio stations—stations that already provide consistent and trusted emergency alerting service despite significant staffing and monetary constraints."[13]

---

[5] *Alerting Security NPRM*, 37 FCC Rcd at 12938-39, paras. 9-12.

[6] *Id.* at 12939-49, paras. 13-36.

[7] *Id.* at 12944-45, para. 25.

[8] *Id*. at 12949-51, paras. 37-40.

[9] Prometheus Radio Project Comments, PS Docket Nos. 15-94, 15-91, and 22-329, at 2 (rec. Dec. 26, 2022) (Prometheus Alerting Security NPRM Comments); National Public Radio, Inc. Reply, PS Docket Nos. 15-94, 15-91, and 22-329, at 2-3 (rec. Jan. 23, 2023) (NPR Alerting Security NPRM Reply); REC Networks Comments, PS Docket Nos. 15-94, 15-91, and 22-329, at 2 (rec. Dec. 22, 2022) (REC Networks Alerting Security NPRM Comments).

[10] Prometheus Alerting Security NPRM Comments at 2.

[11] *Id*.

[12] *Id*.

[13] NPR Alerting Security NPRM Reply at 2-3.

REC Networks similarly states "that security of EAS equipment is of paramount importance" but emphasizes the limited resources of "'small stations' [] normally operated by small nonprofit organizations, minority groups, 'mom and pop' and individual owners with limited budgets and very limited information technology resources."[14] REC Networks states that they "will oppose the 'one size fits all' approach to information security as proposed by the Commission including any requirements that involve the immediate reporting of any security breaches . . . as well as the requirements to develop, update and maintain complex extensive cyber-security risk management policies as they would be applied to small stations."[15] Finally, DAS notes in its reply comments that while sometimes equipment manufacturers provide firmware and software updates "sometimes at no cost or sometimes with a charge," others in the record accurately note that "(e)ven small operators should consider these [firmware and software] updates to be the normal cost of doing business."[16]

5. In response to the *Alerting Modernization NPRM*, DAS expresses concerns that "large operators may move ahead quickly, but small-market and rural licensees might find it hard to keep up" and urges a "comprehensive cost-benefit and small-entity impact assessment before final rule adoption."[17] The Competitive Carriers Association comments that there needs to be "relief and/or reduction of the cadence of imposition of new regulatory requirements related to public safety" and that small providers are at risk of a disadvantage in sales because "smaller carriers would likely lose customers to larger providers that offer [alerting] but with potentially less coverage and quality of service in rural and remote areas."[18]

6. We are persuaded by these views. We agree that the practices proposed in the *Alerting Security NPRM* are overly burdensome, especially for smaller providers. As such, we adopt a very narrowly tailored subset of these proposals. These requirements have been streamlined with smaller providers in mind and are adaptable for various providers, regardless of size.

C. Response to Comments by the Chief Counsel for the Small Business Administration Office of Advocacy

7. Pursuant to the Small Business Jobs Act of 2010, which amended the RFA,[19] the Commission is required to respond to any comments filed by the Chief Counsel for the Small Business Administration (SBA) Office of Advocacy, and provide a detailed statement of any change made to the proposed rules as a result of those comments.[20] The Chief Counsel did not file any comments in response to the proposed rules in this proceeding.

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

8. 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 adopted rules.[21] The RFA generally defines the term "small entity" as having the same meaning as the terms "small business," "small organization," and "small governmental jurisdiction."[22] In addition, the term "small business" has the same meaning as the

[14] REC Networks Alerting Security NPRM Comments at 2.

[15] *Id.*

[16] Digital Alert Systems, Inc. Reply, PS Docket Nos. 15-94, 15-91, and 22-329, at 2 (rec. Jan. 23, 2023).

[17] Digital Alert Systems, Inc. Reply, PS Docket No. 25-224, at 2 (Nov. 13, 2025).

[18] Competitive Carriers Association Comments, PS Docket No. 25-224, at 8 (rec. Sept. 25, 2025).

[19] Small Business Jobs Act of 2010, Pub. L. No. 111-240, 124 Stat. 2504 (2010).

[20] 5 U.S.C. § 604(a)(3).

[21] *Id.*§ 604(a)(4).

term "small business concern" under the Small Business Act (SBA).[23] 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.[24] The SBA establishes small business size standards that agencies are required to use when promulgating regulations relating to small businesses; agencies may establish alternative size standards for use in such programs, but must consult and obtain approval from SBA before doing so.[25]

9. Our actions, over time, may affect small entities that are not easily categorized at present. We therefore describe three broad groups of small entities that could be directly affected by our actions.[26] In general, a small business is an independent business having fewer than 500 employees.[27] These types of small businesses represent 99.9% of all businesses in the United States, which translates to 34.75 million businesses.[28] Next, "small organizations" are not-for-profit enterprises that are independently owned and operated and are not dominant their field.[29] While we do not have data regarding the number of non-profits that meet that criteria, over 99 percent of nonprofits have fewer than 500 employees.[30] Finally, "small governmental jurisdictions" are defined as cities, counties, towns, townships, villages, school districts, or special districts with populations of less than fifty thousand.[31] Based on the 2022 U.S. Census of Governments data, we estimate that at least 48,724 out of 90,835 local government jurisdictions have a population of less than 50,000.[32]

10. The rules we adopt in the *Report and Order* will apply to small entities in the industries identified in the chart below by their six-digit North American Industry Classification System (NAICS)[33]

(Continued from previous page)

[22] *Id*. § 601(6).

[23] *Id*. § 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."

[24] 15 U.S.C. § 632.

[25] 13 CFR § 121.903.

[26] 5 U.S.C. § 601(3)-(6).

[27] *See* SBA, Office of Advocacy, *Frequently Asked Questions About Small Business* (July 23, 2024), https://advocacy.sba.gov/wp-content/uploads/2024/12/Frequently-Asked-Questions-About-Small-Business_2024-508.pdf.

[28] *Id*.

[29] 5 U.S.C. § 601(4).

[30] *See* SBA, Office of Advocacy, *Small Business Facts, Spotlight on Nonprofits* (July 2019), https://advocacy.sba.gov/2019/07/25/small-business-facts-spotlight-on-nonprofits/.

[31] 5 U.S.C. § 601(5).

[32] *See* U.S. Census Bureau, 2022 Census of Governments –Organization, https://www.census.gov/data/tables/2022/econ/gus/2022-governments.html, tables 1-11.

[33] The North American Industry Classification System (NAICS) is the standard used by Federal statistical agencies in classifying business establishments for the purpose of collecting, analyzing, and publishing statistical data related to the U.S. business economy. *See* www.census.gov/NAICS for further details regarding the NAICS codes identified in this chart.

codes and corresponding SBA size standard.[34] Where available, we also provide additional information regarding the number of potentially affected entities in the identified industries below.

Table 1. 2022 U.S. Census Bureau Data by NAICS Code

Regulated Industry (Footnotes specify potentially affected entities within a regulated industry where applicable)	NAICS Code	SBA Size Standard	Total Firms[35]	Total Small Firms[36]	% Small Firms
Radio and Television Broadcasting and Wireless Communications Equip Manufacturing[37]	334220	1,250 employees	155	136	87.74%
Communications Equipment Manufacturing[38]	334290	800 employees	310	294	94.84%
Audio and Video Equipment Manufacturing	334310	750 employees	506	492	97.23%
Radio Broadcasting Stations[39]	516110	$47 million	2,616	2,136	81.65%
Television Broadcasting Stations[40]	516120	$47 million	413	316	76.51%
Media Streaming Distribution Services, Social Networks, and Other Media Networks and Content Providers[41]	516210	$47 million	5,217	3,673	70.40%
Wired Telecommunications	517111	1,500	3,403	3,027	88.95%

[34] The size standards in this chart are set forth in 13 CFR § 121.201, by six digit NAICS code.

[35] *U.S. Census Bureau*, "*Selected Sectors: Employment Size of Firms for the U.S.: 2022*." Economic Census, ECN Core Statistics Economic Census: Establishment and Firm Size Statistics for the U.S., Table EC2200SIZEEMPFIRM, 2025, "*Selected Sectors: Sales, Value of Shipments, or Revenue Size of Firms for the U.S.: 2022*." Economic Census, ECN Core Statistics Economic Census: Establishment and Firm Size Statistics for the U.S., Table EC2200SIZEREVFIRM, 2025.

[36] *Id*.

[37] Affected Entities in this industry include Broadcast Auxiliary Services (BAS), Radio Frequency Equipment Manufacturers.

[38] Affected Entities in this industry include Radio Frequency Equipment Manufacturers (Non-standard specialized equipment).

[39] Affected Entities in this industry include Auxiliary, Special Broadcast and Other Program Distribution Services FM Translator Stations and Low Power FM Stations, Low Power FM Stations, NCE and Public Broadcast Stations (Radio).

[40] Affected Entities in this industry include Auxiliary, Special Broadcast and Other Program Distribution Services, Broadcast Auxiliary Services (BAS) Remote Pickup (RPU) Licensees (TV Stations), NCE and Public Broadcast Stations (TV).

[41] Affected Entities in this industry include Cable Broadcasting Networks, Cable Television Networks, Satellite Television Networks, and Subscription Television Networks.

Regulated Industry (Footnotes specify potentially affected entities within a regulated industry where applicable)	NAICS Code	SBA Size Standard	Total Firms[35]	Total Small Firms[36]	% Small Firms
Carriers[42]		employees			
Wireless Telecommunications Carriers (except Satellite)[43]	517112	1,500 employees	1,184	1,081	91.30%
Satellite Telecommunications[44]	517410	$44 million	332	195	58.73%

Table 2. Telecommunications Service Provider Data

2024 Universal Service Monitoring Report Telecommunications Service Provider Data [45] (Data as of December 2023)	SBA Size Standard (1500 Employees)		
Affected Entity	**Total # FCC Form 499A Filers**	**Small Firms**	**% Small Entities**
Wired Telecommunications Carriers[46]	4,682	4,276	91.33
Wireless Telecommunications Carriers (except Satellite)[47]	585	498	85.13

Table 3. Broadcast Entity Data

Broadcast Station Owners (as of August 8, 2025)[48]	SBA Size Standard ($47 Million)

[42] Affected Entities in this industry include Cable Companies and Systems (Rate Regulation), Cable System Operators (Telecom Act Standard), Direct Broadcast Satellite (DBS).

[43] Affected Entities in this industry Broadband Radio Service and Educational Broadband Service, Low Power Auxiliary Station (LPAS) Licensees.

[44] Affected Entities in this industry include Fixed Satellite Small Transmit/Receive Earth Stations, Fixed Satellite Very Small Aperture Terminal (VSAT) Systems, Mobile Satellite Earth Stations.

[45] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2024), https://docs.fcc.gov/public/attachments/DOC-408848A1.pdf.

[46] Local Resellers fall into another U.S. Census Bureau industry (Telecommunications Resellers) and therefore data for these providers is not included in this industry.

[47] Affected Entities in this industry include all reporting wireless carriers and service providers.

[48] Data as of 2024, according to Commission staff review of the BIA Kelsey Inc. Media Access Pro Television Database (BIA) on August 8, 2025.

Affected Entity	# Commercial Licensed[49] [50]	Small Firms	% Small Entities
Radio Stations (AM & FM) Groups	2,881	2,863	99.38
Television Stations	171	142	83.04

Table 4. Cable Entities Data

Cable Entities	Size Standard	Total Firms	Small Firms	% Small Firms in Industry
Cable System Operators (Telecom Act Standard) Small Cable Operator	Serves fewer than 498,000 subscribers, either directly or through affiliates[51] [52]	530[53]	524[54]	98.87%
Cable Companies and Systems (Rate Regulation) Small Cable Company	Serves 400,000 or fewer subscribers nationwide[55] [56]	530[57]	523[58]	98.51%
Cable Companies and Systems	Serves 15,000 or			

[49] *Id.*

[50] As of December 31, 2025, there were 4,342 licensed commercial AM radio stations and 6,589 licensed commercial FM radio stations, for a combined total of 10,931 commercial radio stations. There were 4,755 licensed noncommercial (NCE) FM radio stations, 1,994 low power FM (LPFM) stations, and 8,867 FM translators and boosters. Additionally, there were 1,389 licensed commercial television stations, 388 licensed noncommercial educational (NCE) television stations, 397 Class A TV stations, 1,760 LPTV stations and 3,092 TV translator stations. *Broadcast Station Totals as of December 31, 2025*, Public Notice, DA 26-49 (rel. Jan. 13, 2026) (*January 2026 Broadcast Station Totals PN*), https://docs.fcc.gov/public/attachments/DA-26-49A1.pdf.

[51] Pursuant to 47 U.S.C. § 543(m)(2) of the Communications Act of 1934, as amended, the size standard for a "small cable operator," is a cable operator that, directly or through an affiliate, serves in the aggregate fewer than 1% of all U.S. subscribers and has no affiliation with entities with gross annual aggregate revenues exceed $250,000,000.

[52] *FCC Announces Updated Subscriber Threshold for the Definition of Small Cable Operator*, Public Notice, DA 23-906 (MB 2023) (*2023 Subscriber Threshold PN*). In the Public Notice, the Commission determined that there were approximately 49.8 million cable subscribers in the United States at that time using the most reliable source publicly available. This threshold will remain in effect until the Commission issues a superseding Public Notice. *See* 47 CFR § 76.901(e)(1).

[53] Based on Commission staff review of S&P Global Market Intelligence, S&P Capital IQ Pro, U.S., *Broadband & Video Subscribers by Geography Q3-2025(June 2025)* data. (last visited Sept. 15, 2025).

[54] *Id.*

[55] 47 CFR § 76.901(d).

[56] *Id.*

[57] Based on Commission staff review of S&P Global Market Intelligence, S&P Capital IQ Pro, U.S., *Broadband & Video Subscribers by Geography Q3-2025(June 2025)* data. (last visited Sept. 15, 2025).

[58] *Id.*

Cable Entities	Size Standard	Total Firms	Small Firms	% Small Firms in Industry
(Rate Regulation) Small Cable System (headends)	fewer subscribers[59]	4,545[60]	3,965[61]	87.24%

E. Description of Economic Impact and Projected Reporting, Recordkeeping and Other Compliance Requirements for Small Entities

11. The RFA directs agencies to describe the economic impact of adopted rules on small entities, as well as projected reporting, recordkeeping and other compliance requirements, including an estimate of the classes of small entities which will be subject to the requirement and the type of professional skills necessary for preparation of the report or record.[62]

12. The rules we adopt in today's *Report and Order* affect small entities that are EAS Participants, but also reflect a preference for narrowly tailored, specific security controls that are less burdensome on small entities by adopting only a segment of the most crucial cybersecurity hygiene practices. Additionally, the requirements we adopt today provide sufficient flexibility for providers to adopt these rules, whether they are large or small. These rules focus on enhancing protections and securing systems against threats but are not one-size-fits-all. EAS Participants have the flexibility to satisfy these requirements in a manner tailored to their particular business needs, which will differ depending on business size, the geographic area served, etc. Further, the rules we adopt today follow Altice USA's recommendation that these "rules allow the greatest possible flexibility in cybersecurity policies and practices so that Participants can tailor them to the unique needs of their networks."[63] While these requirements share the common goal of protecting EAS systems from malicious actors, there are multiple avenues to do so for any variant of provider resources.

13. The rules do not contain any new reporting or recordkeeping requirements. While we cannot conclusively determine whether the rules we adopt in the *Report and Order* will require small entities to hire professionals to assist with compliance, we find that the requirements in the *Report and Order* will promote public safety and alerting system security without imposing substantial costs on small and other entities. We estimate that the costs per entity of changing and regular updating default passwords, installing security patches as available, and implementing firewalls or other network segmentation practices will not exceed $1,000 annually, based on 10 hours of labor per entity per year.[64]

---

[59] 47 CFR § 76.901(c).

[60] Based on Commission staff review of S&P Global Market Intelligence, S&P Capital IQ Pro, U.S. MediaCensusDW, *Operator Subscribers by Geography Q3-2025(June 2025)* data. (last visited Sept. 15, 2025).

[61] *Id.*

[62] 5 U.S.C. § 604(a)(5).

[63] Altice USA, Inc. Reply, PS Docket Nos. 15-94, 15-91, and 22-329, at 1 (rec. Jan. 23, 2023).

[64] We estimate the total cost of implementing the EAS security measures as follows: (10 hours per entity per year) × ($65 mean hourly wage) × (1 + 7% inflation adjustment) × (1 + 46% benefit mark-up) = $1,015.43 total cost per year, rounded to $1,000. *See* Press Release, Bureau of Labor Statistics, Economic News Release: Table 1. National employment and wage data from the Occupational Employment Statistics survey by occupation, May 2025 (May 15, 2026), https://www.bls.gov/news.release/ocwage.t01.htm; Federal Reserve Bank of St. Louis, *Average Hourly Earnings of All Employees, Total Private (CES0500000003)*, https://fred.stlouisfed.org/series/CES0500000003 (last visited Mar. 27, 2026) (showing that, according to Bureau of Labor Statistics data, the average hourly private wage increased by 7% between May 2024 and February 2026). According to the Bureau of Labor Statistics, as of

(continued….)

We expect this cost to be lower for those entities, including small entities, that already engage in password security and regular software update practices, for example, and small entities will have the flexibility to implement firewalls or other network segmentation practices to limit remote management access in the ways that best suit their particular business needs.

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

14. The RFA requires an agency to provide "a description of the steps the agency has taken to minimize the significant economic impact on small entities . . . including a statement of the factual, policy, and legal reasons for selecting the alternative adopted in the final rule and why each one of the other significant alternatives to the rule considered by the agency which affect the impact on small entities was rejected."[65]

15. Through its review of the record in the *Alerting Security NPRM* proceeding, the Commission has sought to minimize significant economic impact on small entities and, in doing so, has considered alternatives to the rules we adopt today. The rules we adopt are a limited set of those proposed in the *Alerting Security NPRM*. We have declined to adopt several expansive cybersecurity requirements, including the requirement that providers annually certify the creation, updating, and implementation of a cybersecurity risk management plan. Instead, the rules we adopt are narrowly tailored to address threats for which small entities are particularly at risk. The requirements we adopt in the *Report and Order* provide sufficient flexibility to account for diverse operational environments, regardless of provider size, capabilities, and resources. We mandate steps to better secure EAS Participant systems and defend against threats to cybersecurity without strict, specific requirements that box providers into particular price points, or rigid restrictions that force them to choose between safety and spending beyond their means. Compliance with these rules should be attainable for all entities, including small entities that may be financially or resource-constrained. Further, the scope of these rules has been narrowed from any EAS Participant systems and services that could potentially affect the provision of the EAS to more specific types of equipment that are most vulnerable. We have made it our focus to advance cybersecurity protections and minimize threats without forcing costly system redesigns or adopting overly complex compliance plan requirements.

G. Report to Congress

16. The Commission will send a copy of the *Report and Order*, including this Final Regulatory Flexibility Analysis, in a report to Congress pursuant to the Congressional Review Act.[66] In addition, the Commission will send a copy of the *Report and Order*, including this Final Regulatory Flexibility Analysis, to the Chief Counsel for the SBA Office of Advocacy and will publish a copy of the *Report and Order*, and this Final Regulatory Flexibility Analysis (or summaries thereof) in the Federal Register.[67]

(Continued from previous page)
December 2025, civilian wages and salaries averaged $33.45/hour and benefits averaged $15.33/hour. Total compensation therefore averaged $33.45 + $15.33 = $48.78. *See* Press Release, Bureau of Labor Statistics, *Employer Costs for Employee Compensation – December 2025* (Mar. 20, 2026), https://www.bls.gov/news.release/pdf/ecec.pdf. Using these figures, benefits constitute a markup of $15.33/$33.45 = 46%. We therefore mark up wages by 46% to account for benefits.

[65] 5 U.S.C. § 604(a)(6).

[66] 5 U.S.C. § 801(a)(1)(A).

[67] *Id.* § 604(b).

APPENDIX D

Initial Regulatory Flexibility Analysis

1. As required by the Regulatory Flexibility Act of 1980, as amended (RFA),[496] the Federal Communications Commission (Commission) has prepared this Initial Regulatory Flexibility Analysis (IRFA) of the policies and rules proposed in the *Further Notice of Proposed Rulemaking* (*Further Notice*) assessing the possible significant economic impact on a substantial number of small entities. The Commission requests written public comments on this IRFA. Comments must be identified as responses to the IRFA and must be filed by the deadlines for comments specified on the first page of this *Further Notice*. The Commission will send a copy of the *Further Notice*, including this IRFA, to the Chief Counsel for the Small Business Administration (SBA) Office of Advocacy.[497] In addition, the *Further Notice* and IRFA (or summaries thereof) will be published in the Federal Register.[498]

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

2. The *Further Notice* takes steps to modernize and improve the Emergency Alert System (EAS) and Wireless Emergency Alerts (WEA). In doing so, it advances the three core goals that alert and warning systems should serve: (1) alerting systems should provide authorities with the ability to rapidly notify the public of emergencies that may put the public at risk; (2) alerting systems should be capable of delivering instructions that facilitate the protection of life and property; and (3) alerting systems should provide a mechanism for government officials to provide additional authoritative communications with the public before, during, and after an emergency. Specifically, the *Further Notice* seeks comment on:

- enhancing EAS security against false messages by using digital signature-based authentication;
- bolstering the reliability of emergency alerts by establishing a universal alert identification number to improve the detection and blocking of duplicate alerts and ensuring that WEA messages are consistently sent to the public until the emergency ends;
- improving geographic accuracy by proposing to eliminate outdated WEA geotargeting exceptions that often cause alerts to be received in the wrong locations and expanding geotargeting options for EAS;
- making alerts more effective by seeking comment on requiring EAS and WEA to display symbols that match the type of emergency and improving the ability of earthquake alerts to grab the public's attention; and
- removing outdated and necessary alerting requirements by proposing to allow the implementation of EAS capabilities via software instead of hardware and retiring the 90-character-maximum versions of WEA messages.

B. Legal Basis

3. The proposed action is authorized pursuant to Sections 1, 2, 4(i), 4(n), 301, 303(b), 303(e), 303(g), 303(j), 303(r), 303(v), 307, 309, 316, 335, 403, 624(g), 706, and 713 of the Communications Act of 1934, as amended, 47 U.S.C §§ 151, 152, 154(i), 154(n), 301, 303(b), 303(e), 303(g), 303(j), 303(r), 303(v), 307, 309, 316, 335, 403, 544(g), 606, and 613, as well as by sections 602(a), (b), (c), (f), 603, 604, and 606 of the WARN Act, 47 U.S.C. §§ 1201 (a), (b), (c), (f), 1203, 1204

[496] 5 U.S.C. §§ 601 *et seq*., as amended by the Small Business Regulatory Enforcement and Fairness Act (SBREFA), Pub. L. No. 104-121, 110 Stat. 847 (1996).

[497] *Id.* § 603(a).

[498] *Id*.

and 1206, and the National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283, 134 Stat. 3388, § 9201, 47 U.S.C. §§ 1201, 1206.

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.[499] The RFA generally defines the term "small entity" as having the same meaning as the terms "small business," "small organization," and "small governmental jurisdiction."[500] In addition, the term "small business" has the same meaning as the term "small business concern" under the Small Business Act (SBA).[501] 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.[502] The SBA establishes small business size standards that agencies are required to use when promulgating regulations relating to small businesses; agencies may establish alternative size standards for use in such programs, but must consult and obtain approval from SBA before doing so.[503]

5. Our actions, over time, may affect small entities that are not easily categorized at present. We therefore describe three broad groups of small entities that could be directly affected by our actions.[504] In general, a small business is an independent business having fewer than 500 employees.[505] These types of small businesses represent 99.9% of all businesses in the United States, which translates to 34.75 million businesses.[506] Next, "small organizations" are not-for-profit enterprises that are independently owned and operated and not dominant in their field.[507] While we do not have data regarding the number of non-profits that meet that criteria, over 99 percent of nonprofits have fewer than 500 employees.[508] Finally, "small governmental jurisdictions" are defined as cities, counties, towns, townships, villages, school districts, or special districts with populations of less than fifty thousand.[509] Based on the 2022 U.S.

---

[499] 5 U.S.C. § 603(b)(3).

[500] *Id*. § 601(6).

[501] *Id*. § 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."

[502] 15 U.S.C. § 632.

[503] 13 CFR § 121.903.

[504] 5 U.S.C. § 601(3)-(6).

[505] *See* SBA, Office of Advocacy, *Frequently Asked Questions About Small Business* (July 23, 2024), https://advocacy.sba.gov/wp-content/uploads/2024/12/Frequently-Asked-Questions-About-Small-Business_2024-508.pdf.

[506] *Id*.

[507] 5 U.S.C. § 601(4).

[508] *See* SBA, Office of Advocacy, *Small Business Facts, Spotlight on Nonprofits* (July 2019), https://advocacy.sba.gov/2019/07/25/small-business-facts-spotlight-on-nonprofits/.

[509] 5 U.S.C. § 601(5).

Census of Governments data, we estimate that at least 48,724 out of 90,835 local government jurisdictions have a population of less than 50,000.[510]

6. The rules proposed in the *Further Notice* will apply to small entities in the industries identified in the chart below by their six-digit North American Industry Classification System (NAICS)[511] codes and corresponding SBA size standard.[512] Where available, we also provide additional information regarding the number of potentially affected entities in the industries identified below.

Table 1. 2022 U.S. Census Bureau Data by NAICS Code

Regulated Industry (Footnotes specify potentially affected entities within a regulated industry where applicable)	NAICS Code	SBA Size Standard	Total Firms[513]	Total Small Firms[514]	% Small Firms
Electronic Computer Manufacturing	334111	1,250 employees	148	128	86.49%
Radio and Television Broadcasting and Wireless Communications Equip Manufacturing[515]	334220	1,250 employees	155	136	87.74%
Communications Equipment Manufacturing[516]	334290	800 employees	310	294	94.84%
Audio and Video Equipment Manufacturing	334310	750 employees	506	492	97.23%
Software Publishers	513210	$47 million	16,824	12,148	72.21%
Radio Broadcasting Stations[517]	516110	$47 million	2,616	2,136	81.65%

[510] *See* U.S. Census Bureau, 2022 Census of Governments –Organization, https://www.census.gov/data/tables/2022/econ/gus/2022-governments.html, tables 1-11.

[511] The North American Industry Classification System (NAICS) is the standard used by Federal statistical agencies in classifying business establishments for the purpose of collecting, analyzing, and publishing statistical data related to the U.S. business economy. *See* www.census.gov/NAICS for further details regarding the NAICS codes identified in this chart.

[512] The size standards in this chart are set forth in 13 CFR § 121.201, by six digit NAICS code.

[513] *U.S. Census Bureau*, "*Selected Sectors: Employment Size of Firms for the U.S.: 2022*." Economic Census, ECN Core Statistics Economic Census: Establishment and Firm Size Statistics for the U.S., Table EC2200SIZEEMPFIRM, 2025, "*Selected Sectors: Sales, Value of Shipments, or Revenue Size of Firms for the U.S.: 2022*." Economic Census, ECN Core Statistics Economic Census: Establishment and Firm Size Statistics for the U.S., Table EC2200SIZEREVFIRM, 2025.

[514] *Id.*

[515] Affected Entities in this industry include Part 15 Handset Manufacturers, Radio Frequency Equipment Manufacturers.

[516] Affected Entities in this industry include Radio Frequency Equipment Manufacturers (Non-standard specialized equipment).

[517] Affected Entities in this industry include Broadcast Auxiliary Services (BAS), Auxiliary, Special Broadcast and Other Program Distribution Services FM Translator Stations and Low Power FM Stations, Educational Broadcasting Services (Radio), Low Power FM Stations, NCE and Public Broadcast Stations (Radio).

Regulated Industry (Footnotes specify potentially affected entities within a regulated industry where applicable)	NAICS Code	SBA Size Standard	Total Firms[513]	Total Small Firms[514]	% Small Firms
Television Broadcasting Stations[518]	516120	$47 million	413	316	76.51%
Media Streaming Distribution Services, Social Networks, and Other Media Networks and Content Providers[519]	516210	$47 million	5,217	3,673	70.40%
Wired Telecommunications Carriers[520]	517111	1,500 employees	3,403	3,027	88.95%
Wireless Telecommunications Carriers (except Satellite)[521]	517112	1,500 employees	1,184	1,081	91.30%
Satellite Telecommunications[522]	517410	$44 million	332	195	58.73%
All Other Telecommunications[523]	517810	$40 million	1,673	1,007	60.19%

Table 2. Telecommunications Service Provider Data

2024 Universal Service Monitoring Report Telecommunications Service Provider Data [524] (Data as of December 2023)	SBA Size Standard (1500 Employees)

[518] Affected Entities in this industry include Auxiliary, Special Broadcast and Other Program Distribution Services, Broadcast Auxiliary Services (BAS) Remote Pickup (RPU) Licensees (TV Stations), Educational Broadcasting Services (TV).

[519] Affected Entities in this industry include Cable Broadcasting Networks, Cable Television Networks, Satellite Television Networks, and Subscription Television Networks.

[520] Affected Entities in this industry include Cable Television Distribution Services, Cable System Operators (Telecom Act Standard), Direct Broadcast Satellite (DBS).

[521] Affected Entities in this industry include Advanced Wireless Services - AWS Services, Broadband Personal Communications Service, Broadband Radio Service and Educational Broadband Service, Low Power Auxiliary Station (LPAS) Licensees, Lower 700 MHz Band Licenses, Narrowband Personal Communications Services, , Specialized Mobile Radio Licenses, Upper 700 MHz Band Licenses Wireless Carriers and Service Providers, Wireless Communications Services, Wireless Telephony.

[522] Affected Entities in this industry include Fixed Satellite Small Transmit/Receive Earth Stations, Fixed Satellite Very Small Aperture Terminal (VSAT) Systems, Mobile Satellite Earth Stations.

[523] Affected Entities in this industry include Internet Service Providers (Non-Broadband), Non-Carrier RespOrgs, Non Licensee Owners of Towers and Other Infrastructure, and Telecommunications Relay Service (TRS) Providers.

[524] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2024), https://docs.fcc.gov/public/attachments/DOC-408848A1.pdf.

Affected Entity	Total # FCC Form 499A Filers	Small Firms	% Small Entities
Wired Telecommunications Carriers[525]	4,682	4,276	91.33
Wireless Telecommunications Carriers (except Satellite)[526]	585	498	85.13
Wireless Telephony[527]	326	247	75.77

Table 3. Broadcast Entity Data

Broadcast Station Owners (as of August 8, 2025)[528]	SBA Size Standard ($47 Million)		
Affected Entity	**# Commercial Licensed[529] [530]**	**Small Firms**	**% Small Entities**
Radio Stations (AM & FM) Groups	2,881	2,863	99.38
Television Stations	171	142	83.04

Table 4. Cable Entities Data

Cable Entities	Size Standard	Total Firms	Small Firms	% Small Firms in Industry
Cable System Operators (Telecom Act Standard)	Serves fewer than 498,000 subscribers, either	530[533]	524[534]	98.87%

[525] Local Resellers fall into another U.S. Census Bureau industry (Telecommunications Resellers) and therefore data for these providers is not included in this industry.

[526] Affected Entities in this industry include all reporting wireless carriers and service providers.

[527] Affected Entities in this industry include Cellular/PCS/SMR - Specialized Mobile Radio Licensees and SMR (Dispatch).

[528] Data as of 2024, according to Commission staff review of the BIA Kelsey Inc. Media Access Pro Television Database (BIA) on August 8, 2025.

[529] *Id.*

[530] As of December 31, 2025, there were 4,342 licensed commercial AM radio stations and 6,589 licensed commercial FM radio stations, for a combined total of 10,931 commercial radio stations. There were 4,755 licensed noncommercial (NCE) FM radio stations, 1,994 low power FM (LPFM) stations, and 8,867 FM translators and boosters. Additionally, there were 1,389 licensed commercial television stations, 388 licensed noncommercial educational (NCE) television stations, 397 Class A TV stations, 1,760 LPTV stations and 3,092 TV translator stations. *Broadcast Station Totals as of December 31, 2025*, Public Notice, DA 26-49 (rel. Jan. 13, 2026) (*January 2026 Broadcast Station Totals PN*), https://docs.fcc.gov/public/attachments/DA-26-49A1.pdf.

Cable Entities	Size Standard	Total Firms	Small Firms	% Small Firms in Industry
Small Cable Operator	directly or through affiliates[531] [532]			
Cable Companies and Systems (Rate Regulation) Small Cable Company	Serves 400,000 or fewer subscribers nationwide[535] [536]	530[537]	523[538]	98.51%
Cable Companies and Systems (Rate Regulation) Small Cable System (headends)	Serves 15,000 or fewer subscribers[539]	4,545 [540]	3,965[541]	87.24%

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

7. The RFA directs agencies to describe the economic impact of proposed rules on small entities, as well as projected reporting, recordkeeping and other compliance requirements, including an estimate of the classes of small entities which will be subject to the requirements and the type of professional skills necessary for preparation of the report or record.[542]

(Continued from previous page)

[533] Based on Commission staff review of S&P Global Market Intelligence, S&P Capital IQ Pro, U.S., *Broadband & Video Subscribers by Geography Q3-2025(June 2025)* data. (last visited Sept. 15, 2025).

[534] *Id.*

[531] Pursuant to 47 U.S.C. § 543(m)(2) of the Communications Act of 1934, as amended, the size standard for a "small cable operator," is a cable operator that, directly or through an affiliate, serves in the aggregate fewer than 1% of all U.S. subscribers and has no affiliation with entities with gross annual aggregate revenues exceed $250,000,000.

[532] *FCC Announces Updated Subscriber Threshold for the Definition of Small Cable Operator*, Public Notice, DA 23-906 (MB 2023) (*2023 Subscriber Threshold PN*). In the Public Notice, the Commission determined that there were approximately 49.8 million cable subscribers in the United States at that time using the most reliable source publicly available. This threshold will remain in effect until the Commission issues a superseding Public Notice. *See* 47 CFR § 76.901(e)(1).

[535] 47 CFR § 76.901(d).

[536] *Id*.

[537] Based on Commission staff review of S&P Global Market Intelligence, S&P Capital IQ Pro, U.S., *Broadband & Video Subscribers by Geography Q3-2025(June 2025)* data. (last visited Sept. 15, 2025).

[538] *Id.*

[539] 47 CFR § 76.901(c).

[540] Based on Commission staff review of S&P Global Market Intelligence, S&P Capital IQ Pro, U.S. MediaCensusDW, *Operator Subscribers by Geography Q3-2025(June 2025)* data. (last visited Sept. 15, 2025).

[541] *Id.*

[542] 5 U.S.C. § 603(b)(4).

8. The proposed requirements in the *Further Notice,* if adopted, will impose new or modified reporting, recordkeeping and/or other compliance obligations. Specifically, we propose and seek comment on requiring all vendors of EAS software that small business entities and other EAS participants may choose to purchase and use apply for certification of that software in accordance with our part 2 rules. Because costs of complying with that requirement are difficult to estimate given unknowns about the number of vendors that will seek to bring EAS software to market and differing burdens that vendors may face, the *Further Notice* seeks comment on several aspects of those potential burdens.

9. For EAS Participants, including small business entities, we estimate a one-time $500 cost per affected small entity to make the necessary software updates to comply with our proposed changes to Common Alerting Protocol (CAP) authentication and improvements to geotargeting via the addition of location codes. If we were to require adoption of a universal alert message identifier and common symbology for CAP-based EAS messages, we believe those costs would also be included in this estimate, insofar as those software updates could also be implemented at the same time. We believe these software updates would require a maximum of five hours of labor to implement, but we note that this is likely an overestimate, as incremental software update costs could be avoided for small and other EAS Participants by implementing the relevant changes in conjunction with previously scheduled software updates. Our estimate is based on an average hourly wage of $63.53 for software and web developers, programmers, and testers, and factors in a 46% markup of hourly wage for benefits, and a 7% inflation adjustment between 2024 and 2026, which amounts to a total hourly wage of $99.24/hour.[543] We seek comment on additional system modification costs that may arise from implementing EAS-related symbols on television screens. We also seek comment on whether it would be necessary for any small entities to replace equipment in the event that the Commission were to require legacy EAS to support authentication or universal alert identifiers, and if so, how those requirements could be implemented to minimize those costs.

10. For Participating Commercial Mobile Service (CMS) Providers, including small business entities, we estimate a maximum total one-time cost of $570,000 to cover the standards development processes, software modifications, and software testing required to comply with the relevant rule changes we propose in the *Further Notice*. This includes preventing duplicate alerts through a universal alert message identifier and eliminating outdated exceptions to WEA geotargeting. If we were to adopt rules requiring amplification of WEA earthquake alerts and retirement of 90-character WEA messages, necessary updates to the standards to comply with those rules would also be included in the same standards development process. Our estimate is based on approximately a $400,000 average cost for testing,[544] a $170,000 average cost for software modifications,[545] and a $10,600 cost to participate in a standards development process,[546] if applicable. However, we do not expect all Participating CMS Providers to engage in the standards development process, so small entities that do not participate would avoid this aspect of the cost.[547] Our estimates are based on the wages of a software developer compensated at the national average for their field ($139,850/year), plus a 46% markup for annual

[543] $99.24/hour x 5 hours = $496.20.

[544] 12 software developers × ($139,850 + $64,331) annually per Participating CMS Provider × 2 months / 12 months per year = $408,362 per provider.

[545] ($139,850 + $64,331) annually per Participating CMS Provider x 10 months / 12 months per year = $170,151 per standards process participant.

[546] ($65.33 + $30.05) per hour per network engineer × 107% × 26 hours per standard × 4 standards = $10,614.

[547] *See* Letter from Thomas Goode, General Counsel, ATIS, to Marlene Dortch, Secretary, FCC, PS Docket No. 15-91, at 1 (filed Sept. 6, 2016).

benefits ($64,331/year), working for the amount of time it takes to develop software (10 months) or test software (2 months) at each CMS Provider that participates in WEA.

11. If we were to require Participating CMS Providers, including small business entities, to rebroadcast WEA messages at least once every sixty seconds throughout an alert's active period and cease retransmission of WEA messages with a 24-hour active period five minutes before the end of that period, we do not anticipate that compliance would require the development of new standards or more than *de minimis* software development. We estimate that the necessary changes to configurations and settings of WEA-related systems would require no more than 10 hours per Participating CMS Provider, amounting to an estimated maximum cost of approximately $1,000 per provider.[548]

12. To help the Commission more fully evaluate the cost of compliance for small entities, we requested comments on the cost implications and cost estimates to implement these proposals and asked whether there are more efficient and less burdensome alternatives that might achieve the same results, including alternatives specific to smaller entities. The Commission expects the information we receive in comments to help us identify and evaluate impacts to small entities that may result if the changes to the nation's emergency alerting systems discussed in the *Further Notice* were adopted.

E. Discussion of Significant Alternatives Considered That Minimize the Significant Economic Impact on Small Entities

13. The RFA directs agencies to provide a description of any significant alternatives to the proposed rules that would accomplish the stated objectives of applicable statutes, and minimize any significant economic impact on small entities.[549] The discussion is required to include alternatives such as: "(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 and reporting requirements under the rule for such small entities; (3) the use of performance rather than design standards; and (4) an exemption from coverage of the rule, or any part thereof, for such small entities."[550]

14. In the *Further Notice*, the Commission's proposals and requests for comment are designed to minimize the economic impact on small entities where feasible, and the Commission seeks comment on the costs of alerting participants, including small entities. The Commission also seeks comment broadly on alternatives to the proposed compliance timeframes that might minimize economic burdens on small entities. We believe that the proposals in the *Further Notice* are the most efficient and least burdensome approaches.

15. Specifically, we believe our proposal to secure EAS through message authentication will protect small entities from costly cyberattacks that disrupt their business. We seek comment whether there might be potentially costly risks associated with adopting this requirement and if so, how to mitigate those risks. We also seek comment on additional ways to reduce burdens while maintaining expectations for EAS.

16. To improve the reliability of emergency alerts, the Commission also proposes to require a single, universal message identifier for WEA and EAS messages and sought comment on ways to reduce overhead for alerting participants, including small entities, including through hashing, and other, less burdensome alternatives.

---

[548] ($65.33 + $30.05) per hour for a network engineer per Participating CMS Provider × 107% × 10 hours = $1,021, which we round to $1,000.

[549] 5 U.S.C. § 603(c).

[550] *Id.* § 603(c)(1)-(4).

17. The Commission also proposes to improve the accuracy of WEA geotargeting by eliminating outdated regulatory exceptions, such as those related to legacy infrastructure and legacy devices, mobile devices with location services disabled, and alerts whose target areas are not specified by a polygon or circle. The Commission seeks comment on what types of Participating CMS Providers would be most impacted by these proposals, how costly the proposals might be, and whether there are less burdensome alternatives that should be considered. The Commission asks about small providers' timelines for sunsetting legacy networks, in order to inform future rules' effective dates that fit into planned business cycles for those entities.

18. For its proposal to promote rapid protective action in response to earthquake alerts, the Commission seeks comment on the technical implementation of text-to-speech for WEA, including ways to minimize implementation burdens on small entities. For both EAS and WEA, the Commission seeks comment on requiring alert messages to include standardized symbology that identifies the relevant threat type. The Commission asks whether, if adopted, such a requirement should be based on the National Alliance for Public Safety GIS (NAPSG) symbol library, which is publicly available at no cost, to minimize burdens on alerting participants, including small entities.

19. Finally, the Commission proposes to minimize burdens on all alerting participants, including small ones, by removing unnecessary alerting requirements. Namely, it proposes to permit, but not require, EAS Participants to meet their EAS obligations through the use of EAS software instead of dedicated hardware. This grants EAS Participants greater flexibility in how they design and configure their EAS systems. The Commission also seeks comment on alternative methods of implementing EAS software, including the software authentication and operational readiness requirements, that could further minimize burdens on EAS Participants. For Participating CMS providers, the Commission proposes to retire support for 90-character WEA messages. We believe this will minimize burdens on Participating CMS Providers, including small providers, and alert originators by eliminating the redundancy of having to send both a 90-character-maximum message and a 360-character-maximum message. We also believe that this will reduce burdens on Participating CMS Providers because their networks will no longer need to parse multiple versions of alerts for distribution among various generations of wireless technology.

20. Having data on the issues the Commission proposes and seeks comment on in the *Further Notice* regarding costs, benefits, and potential impacts of resulting rule changes will assist the Commission in evaluating the economic impact on small entities. It will also help the Commission determine how to minimize any significant economic impacts on small entities and less burdensome alternatives that were not yet considered. The Commission expects to more fully consider the economic impact and alternatives for small entities following the review of comments and reply comments filed in response to the *Further Notice*. The Commission's evaluation of the record will shape the alternatives it considers, final conclusions it reaches, and the actions it takes to minimize any significant economic impact on small entities.

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

21. None.

STATEMENT OF
CHAIRMAN BRENDAN CARR

Re: *Modernization of the Nation's Alerting Systems; Protecting the Nation's Communications Systems from Cybersecurity Threats; Wireless Emergency Alerts; Amendment of Part 11 of the Commission's Rules Regarding the Emergency Alert System*, Report and Order, PS Docket Nos. 25-224 and 22-329, Further Notice of Proposed Rulemaking, PS Docket Nos. 25-224, 15-94, 15-91, (June 25, 2026).

Some folks will remember more than a decade ago when television viewers in several states received what appeared to be a real emergency alert. The alert informed Americans that "the bodies of the dead are rising from their graves and attacking the living." Thankfully for those of us that aren't Daryl Dixon or Rick Grimes, it was not the beginning of a zombie apocalypse. But it was the result of a cyberattack that allowed bad actors to transmit a false warning over broadcast stations after gaining access to alerting equipment that was protected by default passwords and inadequate security measures.

While the FCC has worked to ensure that vulnerabilities in EAS and WEA are addressed, there have been additional instances of alerting and broadcast systems being compromised or manipulated, including recent attacks that used emergency alert tones and related broadcast equipment to transmit unauthorized content. These attacks are a stark reminder that threats continue to evolve and our work must continue.

Today's item builds on our prior work by taking commonsense steps to strengthen the cybersecurity of our emergency alert systems by addressing the very types of vulnerabilities that enabled the zombie-alert incident in the first place. Requiring stronger password practices, timely software updates, and improved security controls will help reduce opportunities for bad actors to exploit weaknesses in alerting equipment.

Today's item also tees up additional reforms that can improve the integrity, resilience, and effectiveness of emergency alerts, including improving geographic accuracy of alerts, improving the detection and blocking of duplicate alerts, and removing outdated and unnecessary alerting requirements to help encourage broader participation in alerting.

Thanks to Logan Bennett, Steven Carpenter, George Donato, Leon Kenworthy, David Kirschner, Zoe Li, David Munson, Zenji Nakazawa, Austin Randazzo, Tara Shostek, and James Wiley for their work on this item.

STATEMENT OF
COMMISSIONER OLIVIA TRUSTY

Re: *Modernization of the Nation's Alerting Systems; Protecting the Nation's Communications Systems from Cybersecurity Threats*; *Wireless Emergency Alerts; Amendment of Part 11 of the Commission's Rules Regarding the Emergency Alert System*, Report and Order, PS Docket Nos. 25-224 and 22-329, Further Notice of Proposed Rulemaking, PS Docket Nos. 25-224, 15-94, and 15-91(June 25, 2026).

In May, I had the opportunity to visit the Nebraska Emergency Management Agency at a time when Nebraska is experiencing the worst wildfire season in its history. Since February, more than 800,000 acres have burned, causing widespread destruction and millions of dollars in damage. Throughout these emergencies, NEMA has coordinated and initiated alerts that are then transmitted by broadcasters, cable operators, and other communications providers to people throughout the state.

This essential process is repeated every day across the country whenever disaster strikes. Whether the threat is a wildfire, tornado, hurricane, or other emergency, Americans rely on our alerting systems to deliver timely and accurate information when it matters most.

Any vulnerability in the Emergency Alert System can have serious consequences. That is why it has been appropriate for the Commission to conduct a comprehensive review of the EAS framework by focusing on the security of the system itself. As cybersecurity threats continue to evolve, EAS participants must take appropriate steps to safeguard the infrastructure that supports the delivery of life-saving alerts.

Today's Report and Order advances that goal by strengthening cybersecurity practices and helping secure this critical component of our nation's emergency communications infrastructure. The Further Notice charts a path toward modernizing the broader alerting framework by leveraging new technologies, streamlining outdated requirements, and improving the usability and effectiveness of the EAS system.

Protecting the nation's communications networks from malicious actors is among the Commission's most important responsibilities. And today's actions will help ensure that emergency alerts remain secure, reliable, and effective in keeping Americans out of harm's way and in saving lives.

I thank the Public Safety and Homeland Security Bureau for their work on this item.