FEDERAL COMMUNICATIONS COMMISSION

47 CFR Parts 0, 10, 11

[PS Docket Nos. 15-91, 15-94, 25-224; FCC-26-38; FR ID 359294]

Wireless Emergency Alerts; The Emergency Alert System; Modernization of the Nation's Alerting Systems

AGENCY: Federal Communications Commission.

ACTION: Proposed rule.

SUMMARY: In this document, the Federal Communications Commission ("FCC" or "Commission") adopted a Further Notice of Proposed Rulemaking that seeks comment on proposed rules intended to make the Emergency Alert System (EAS) and Wireless Emergency Alerts (WEA) more resilient, flexible, and useful.

DATES: Comments are due on or before **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN FEDERAL REGISTER]**, and reply comments are due on or before **[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN FEDERAL REGISTER]**.

ADDRESSES: You may submit comments, identified by PS Docket Nos. 15-91, 15-94, and 25-224, by the following method:

- *Electronic Filers*: Comments may be filed electronically using the Commission's website by accessing the Electronic Comment Filing System (ECFS): *https://apps.fcc.gov/ecfs/*. Follow the instructions for submitting comments
- *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.

- *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).

FOR FURTHER INFORMATION CONTACT: For further information concerning the information contained in this document, please contact David Kirschner, Attorney Advisor, Cybersecurity and Communications Reliability Division, Public Safety and Homeland Security Bureau, at 202-418-0695, or by email to David.Kirschner@fcc.gov, or George Donato, Associate Division Chief, Cybersecurity and Communications Reliability Division, Public Safety and Homeland Security Bureau at 202-418-0729, or by email to George.Donato@fcc.gov.

SUPPLEMENTARY INFORMATION: This is a summary of the Commission's Further Notice of Proposed Rulemaking (*NPRM*) in PS Docket Nos. 15-91, 15-94, and 25-224, FCC 26-38, adopted on June 25, 2026, and released on June 29, 2026. A summary of the accompanying Report and Order adopted in PS Docket Nos. 22-329 and 25-224, FCC 26-38, adopted on June 25, 2026 and released on June 29, 2026 is published elsewhere in this issue of the *Federal Register*. The full text of this document is available at https://docs.fcc.gov/public/attachments/FCC-26-38A1.pdf.

Ex Parte Rules – Permit-But-Disclose. The proceeding this Notice initiates shall be treated as a "permit-but-disclose" proceeding in accordance with the Commission's *ex parte* rules. 47 CFR 1.1200 *et seq*. Persons making *ex parte* presentations must file a copy of any written presentation or a memorandum summarizing any oral presentation within two business days after the presentation (unless a different deadline applicable to the Sunshine period applies). Persons making oral *ex parte* presentations are reminded that memoranda summarizing the presentation must (1) list all persons attending or otherwise participating in the meeting at which the *ex parte* presentation was made, and (2) summarize all data presented and arguments made during the presentation. If the presentation consisted in whole or in part of the presentation of data or arguments already reflected in the presenter's written comments, memoranda or other filings in the proceeding, the presenter may provide citations to such data or arguments in his or her prior comments, memoranda, or other filings (specifying the relevant page and/or paragraph numbers where such data or arguments can be found) in lieu of summarizing them in the memorandum. Documents shown or given to Commission staff during *ex parte* meetings are deemed to be written *ex parte* presentations and must be filed consistent with rule 1.1206(b). In proceedings governed by rule 1.49(f) or for which the Commission has made available a method of electronic filing, written *ex parte* presentations and memoranda summarizing oral *ex parte* presentations, and all attachments thereto, must be filed through the electronic comment filing system available for that proceeding, and must be filed in their native format (*e.g.*, .doc, .xml, .ppt, searchable .pdf). Participants in this proceeding should familiarize themselves with the Commission's *ex parte* rules.

Providing Accountability Through Transparency Act. The Providing Accountability Through Transparency Act, Public Law 118–9, requires each agency, in providing notice of a rulemaking, to post online a brief plain language summary of the proposed rule. The required summary of the *NPRM* is available at *https://www.fcc.gov/proposed-rulemakings*.

Paperwork Reduction Act Analysis. The NPRM 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 Office of Management and Budget (OMB) to comment on the information collection requirements contained in the *NPRM*, as required by the Paperwork Reduction Act of 1995, Public Law 104–13. In addition, pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107–198, *see* 44 U.S.C. 3506(c)(4), the Commission seeks specific comment on how it might further reduce the information collection burden for small business concerns with fewer than 25 employees.

SYNOPSIS

Securing EAS Through Message Authentication

While the security measures that we require radio and television stations, cable television systems, satellite radio and video services, and other entities required to participate in the EAS (collectively, "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 Common Alerting Protocol (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. 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 the Integrated Public Alert and Warning System (IPAWS), IPAWS maintains the public keys for all alert originators including itself. 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. 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.

Digital Alert Systems, Inc. (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." Washington State Emergency Management 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." 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. 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.

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. 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. 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.

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. 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. Is there any reason to expect that there would be 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?

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. 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. 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. 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. 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. Adding the data necessary for a digital signature would delay alert message transmission and, in turn, delay the public's receipt of emergency alerts. According to CSRIC VI, 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 strings. 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. According to CSRIC VI, "[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[, which] could include many EAS Participants themselves." CSRIC VI adds 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."

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. 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. We seek comment on how to address these challenges, including the non-conformity of legacy equipment that is no longer supported by software updates. Would the National Weather Service (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?

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?

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

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?

Bolstering the Reliability of Emergency Alerts

In the 2025 Notice of Proposed Rulemaking (*Alerting Modernization NPRM*) that commenced a ground-up review of the nation's alerting systems, the Commission 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. 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. 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." 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.

Preventing Duplicate Alerts Through a Universal Identifier. When we sought comment on alert originators' expectations for delivery of alerts, 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. As the Washington State Emergency Management Division writes, "[a]lerts must be . . . non-duplicative to avoid fatigue and maintain public trust." 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.

To reduce confusion and alert fatigue, we propose to require Participating Commercial Mobile Service (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 § 10.500(g) of the Commission's rules already requires WEA-capable mobile devices to detect and suppress duplicate WEA messages, the Commission still frequently receives complaints that members 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. 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?

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. 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. 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.

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 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 the Federal Emergency Management Agency (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.

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? The Alliance for Telecommunications Industry Solutions (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." 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?

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. 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. 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?

Ensuring the Consistent Transmission of WEA Messages. 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. Among major 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. 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. 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?

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. 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. 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?

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. In these circumstances, differences between how the CMS network and mobile devices determine the age of 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.

Improving the Accuracy of Alert Geotargeting

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. Commenters widely recognize that accurate geotargeting is "critical" to accomplishing alerting systems' goals, and they overwhelmingly support improving those capabilities. King County comments that "[w]e strongly agree that geographic targeting is a necessity for a modern alerting system." Sonoma County Department of Emergency Management comments: "Geographic targeting is also critical. Alerts should be as precise as possible to reach only those at risk." 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."

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." 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," Alaska resident Shawn Williams observes that geotargeting overshoot can be equally pernicious in rural areas. 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. Consequently, people may ignore EAS and WEA messages that are intended for them or disable WEA warnings altogether. APCO International states that "alert originators are less likely to use alerting systems" because of the negative consequences of poor geotargeting. 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." 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." 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.

Strengthening WEA Geotargeting by Eliminating Outdated Exceptions. Commenters offer several suggestions on ways to improve WEA geotargeting. 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. 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," our rules allow for exceptions for "network infrastructure [that] is technically incapable of matching the specified target area." The Commission has provided a non-exhaustive list of circumstances in which a Participating CMS Provider's network 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. 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."

Even though technically incapable networks are nonetheless required to deliver WEA messages to their best approximation of the target area, the Commission and its federal partners frequently receive complaints that WEA messages are being received outside of the target area. 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.

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. We understand that many Participating CMS Providers either have already retired or are actively retiring their 2G and 3G networks. Which, if any, currently deployed networks cannot support geotargeting as currently described in our rules? 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 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?

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. Participating CMS Providers use device-based geofencing to comply with the geographic targeting requirements of

§ 10.450(a), which limits overshoot to 0.1 miles on technically capable infrastructure and devices. 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. When the Public Safety and Homeland Security Bureau (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. The Bureau also found that at least some of these failures likely occurred because devices had location services disabled. 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?

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." 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?

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." 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." According to King County Office of Emergency Management (King County), however, "[i]f those location services data are not shared off the device, there would be no privacy concerns." We believe King County is correct that mobile device location data is never shared outside of the device for the purpose of WEA geofencing. 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?

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." 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 emergency involves power outages, a consumer might reasonably choose to conserve device battery life over the ability to receive more targeted alerts." 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.

Exemption for Geocodes. We propose to require WEA messages that geotarget alerts by using Federal Information Processing System, Codes for States and Counties (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. As a result, according to CTIA, "the alert will not contain the geographic coordinates necessary to activate [device-based geofencing]. . . ." 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. 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.

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. Since then, the U.S. Census Bureau has published a mapping of county codes to polygon coordinates. 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, 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? 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?

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?

Incentivizing EAS Geofencing. 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, 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. As DAS comments, "[b]y design, once an EAS alert is issued, everyone watching that channel receives it." As REC Networks states, "since EAS was originally intended for national messages, more localized messages are just an afterthought." Alerting authorities and EAS

equipment manufacturers take the view that EAS is being underutilized because of these limited geotargeting capabilities. For example, during the January 2025 Los Angeles County wildfires alerting 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." DAS states that improvements to EAS geotargeting "could reduce alert fatigue and make alerts more relevant." Because many CAP EAS messages include WEA-supported circles or polygons in addition to county codes (legacy EAS messages do not contain geo-targeting information more accurate than the county codes), 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.

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?

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. The Advanced Warning and Response Network (AWARN) Alliance, ATSC: The Broadcast Standards Association, Sinclair, Inc., the National Association of Broadcasters (NAB), and the Oregon Department of Emergency Management advocate for increased use of ATSC 3.0 as a way to transmit geotargeted emergency alerts. Would our proposal 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?

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. NWS has expressed concerns that existing location names can be potentially confusing or misleading to the public. For example, in Monroe County, Florida the "southwest" subcounty code might be used for alerts relevant to Key West. 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. For example, the American National Standards Institute (ANSI) standard for FIPS codes and the Commission's EAS rules establish that the code for Monroe County, Florida is "12087." The code "12088," on the other hand, is currently unused and could potentially be assigned to "Key West" for EAS purposes.

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?

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 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.

Enhancing Alert Effectiveness

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. 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." 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. The Snohomish County Department of Emergency Management cautions that creating and transmitting multimedia content could delay alert delivery.

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 U.S. Geological Survey's (USGS) recommendation that the receipt of a WEA earthquake alert should trigger an announcement of the alert message text using text-to-speech. 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.

Promoting the Use of Symbols for Alerts. 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. For example, Notify NYC & Cornell Tech have previously found that the use of incident-specific symbols doubled participant comprehension and literacy. 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. 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." 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." FEMA has previously argued that the use of graphical symbols could improve alert message interpretation by individuals with limited English proficiency.

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. 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? 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 . . ." 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?

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, which is publicly available at no cost and is supported by FEMA? 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," the presence of

NAPSG symbology did not improve the participants' understanding of either the event or the recommended protective action. 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.

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 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.

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?

Amplifying WEA Earthquake Alerts. The faster the public understands an alert, the faster they can react. This is particularly important during events that occur without prior notice or predication. 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. While WEA's attention signal and vibration cadence are intended to quickly grab subscribers' attention, 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. 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. 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 automatically

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

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." 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). 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. 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?

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?

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. 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, and significant public education would be required 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?

Removing Unnecessary Alerting Requirements

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. 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, The Competitive Carriers Association (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." CCA asks that this proceeding build upon the Commission's

Delete, Delete, Delete proceeding. Similarly, with respect to EAS, NTCA–The Rural Broadband Association (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." 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. 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. We also respond to the March 31, 2025, Petition for Rulemaking filed by the National Association of Broadcasters (NAB) 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.

Approving the Use of EAS Software. We grant NAB's Petition for Rulemaking 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, and we find that it discloses sufficient reasons in support of the action requested to justify the institution of a rulemaking proceeding. 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, and "encourag[ing] the provision of new technologies and services to the public." 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.

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." 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." 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."

We also agree with commenters like CMG Media Corporation (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 equipment." 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)." NCTA 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," 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." 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." 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.

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. 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," adding that there is no "FCC process for certifying software-only EAS solutions." 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." We observe that the need to develop equipment certification or approval requirements appears to be anticipated in the NAB Petition, and by its supporters. As Sage puts it, "[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." 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.

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." 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.

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," 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." 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." We observe that, as stated above, the NAB Petition has made the showing required for Petitions for Rulemaking, and discloses sufficient reasons to justify the institution of a rulemaking proceeding. Moreover, as the NAB Petition described it, software-performed EAS might enable "an immediate fail-over of functionality" to backup EAS software operating on systems in other locations. 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." These functions strike us as potentially enhancing the reliability, availability and, potentially in times of outages, the reach of the EAS.

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. 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. 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." 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. These 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." We seek comment on these expectations.

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? 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?

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." 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. We seek comment on this proposal and our 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*?

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. 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." 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."

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. (By "studio," we mean the local physical facility wherein programming is generated and/or compiled and processed for transmission.) 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," 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." DAS and NCTA also express concern that remote hosting and EAS software processing may diminish the Commission's capacity for oversight and enforcement.

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?

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. 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." 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." 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."

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

We seek comment on these views. 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?

DAS also argues that "[EAS software] developers must now account for potential IP landmines that could stall or complicate product viability." 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." To that end, DAS asserts that "[u]ndisclosed intellectual property may introduce significant concerns related to policy and competition in the marketplace." 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?

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. 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." We seek comment on what certification or other approval framework should apply to EAS software.

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. While § 11.34(a) and (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. 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) 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.

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." DAS raises concerns that EAS software certification is necessary, but that "there is no [], widely accepted FCC process for certifying software-only EAS solutions." 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 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?

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 §§ 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. 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. 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." 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?

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. 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." Sage further observes, "[a]s a practical matter, this requires a separate box for certification." 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? 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). 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. We seek comment on the sufficiency of these proposed revisions.

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. More specifically, the EAS software certification would be a component of and subsumed under the custom-designed product's certification. EAS software that is installed and integrated across multiple system components would have 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.

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, § 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. 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. 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." 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. 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?

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." DAS further observes that "[u]nlike physical devices, software platforms have large attack surfaces, including APIs, databases, and remote access points." 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." 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 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. 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." We seek comment on these views.

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? (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.) 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. 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? Would cybersecurity certification of EAS software alone be sufficient to ensure the 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?

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." 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?

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. Under the current rules, EAS Participants may operate without defective equipment pending its repair or replacement for 60 days without further FCC authority. 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. 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." 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 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?

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? 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.

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. 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?

Finally, we observe that § 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. 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.

Retiring 90-character WEA Messages. 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." This requirement is in addition to the 360-character maximum version. As a 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. 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." 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." 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. 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?

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." 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. We understand that many Participating CMS Providers either have already retired or are actively retiring their 2G and 3G networks. According to 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. 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?

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. 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?

Analysis of Costs and Benefits

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

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.

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. Likewise, the local radio and television broadcasting sector

a subset of EAS Participants, supported $1.19 trillion of the nation's GDP in 2025, so preventing a disruption of even 0.0011% in a single year would offset the one-time EAS software update costs. Are there other ways to quantify the benefits to EAS security that message authentication would deliver?

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.

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. 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. 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. 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. 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. This is calculated as follows: 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. 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. 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. This is calculated as follows: $48,000,000 ~ 3 years × 456,250 deployments per year × $3,500 per deployment. 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?

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 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.

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. 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? 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.

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.

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

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. 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. We also note that incremental EAS software update costs could be avoided by implementing the relevant changes in conjunction with previously scheduled software updates. 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, we estimate that implementation costs for one-time necessary EAS software updates would not exceed $13 million, adjusted for inflation. 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. 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. 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%). We seek comment on this analysis and on the cost to EAS equipment manufacturers to create these updates.

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 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?

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.

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?

WEA Standards and Testing. For WEA, we estimate that Participating CMS Providers would incur a maximum $39.5 million industry-wide, one-time compliance costs to update the standards and software necessary to comply with the WEA-related proposals we put forth today. 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. 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, 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), plus a 46% mark-up for benefits ($30.05/hour), and a 7% inflation adjustment between 2024 and 2026, working for 26 hours a year for a maximum of four distinct standards. 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.

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. 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. 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. 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. We have used the same framework since 2016 for changes to software, ranging from enhanced geotargeting to alert preservation. We seek comment on whether this remains an appropriate framework and on these cost estimates and the underlying methodology in general.

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. This is calculated as follows: ($65.33 + $30.05) per hour for a network engineer per Participating CMS Provider × 107% × 10 hours × 65 Participating CMS Providers = $66,337. We seek comment on this estimate.

Compliance Timeframes

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.

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*. 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?

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*. 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 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?

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*. 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. 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?

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.

INITIAL REGULATORY FLEXIBILITY ANALYSIS

As required by the Regulatory Flexibility Act of 1980, as amended (RFA), 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 in the item.

Need for, and Objectives of, the Proposed Rules. 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: (i) enhancing EAS security against false messages by using digital signature-based authentication; (ii) 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; (iii) 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; (iv) 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 (v) 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.

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

Description and Estimate of the Number of Small Entities to Which the Proposed Rules Will Apply. 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) codes and corresponding SBA size standard. 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	Total Small Firms	% Small Firms
Electronic Computer Manufacturing	334111	1,250 employees	148	128	86.49%
Radio and Television Broadcasting and Wireless Communications Equip Manufacturing	334220	1,250 employees	155	136	87.74%
Communications Equipment Manufacturing	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	516110	$47 million	2,616	2,136	81.65%
Television Broadcasting Stations	516120	$47 million	413	316	76.51%
Media Streaming Distribution Services, Social Networks, and	516210	$47 million	5,217	3,673	70.40%

Regulated Industry (Footnotes specify potentially affected entities within a regulated industry where applicable)	NAICS Code	SBA Size Standard	Total Firms	Total Small Firms	% Small Firms
Other Media Networks and Content Providers					
Wired Telecommunications Carriers	517111	1,500 employees	3,403	3,027	88.95%
Wireless Telecommunications Carriers (except Satellite)	517112	1,500 employees	1,184	1,081	91.30%
Satellite Telecommunications	517410	$44 million	332	195	58.73%
All Other Telecommunications	517810	$40 million	1,673	1,007	60.19%

Table 2. Telecommunications Service Provider Data

2024 Universal Service Monitoring Report Telecommunications Service Provider Data (Data as of December 2023)	SBA Size Standard (1500 Employees)		
Affected Entity	**Total # FCC Form 499A Filers**	**Small Firms**	**% Small Entities**
Wired Telecommunications Carriers	4,682	4,276	91.33
Wireless Telecommunications Carriers (except Satellite)	585	498	85.13
Wireless Telephony	326	247	75.77

Table 3. Broadcast Entity Data

Broadcast Station Owners (as of August 8, 2025)	SBA Size Standard ($47 Million)		
Affected Entity	**# Commercial Licensed**	**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	530	524	98.87%
Cable Companies and Systems (Rate Regulation) Small Cable Company	Serves 400,000 or fewer subscribers nationwide	530	523	98.51%
Cable Companies and Systems (Rate Regulation) Small Cable System (headends)	Serves 15,000 or fewer subscribers	4,545	3,965	87.24%

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

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. 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.

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, a $170,000 average cost for software modifications, and a $10,600 cost to participate in a standards development process, 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. 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 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.

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.

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.

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

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.

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.

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.

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.

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.

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.

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

None.

Legal Authority.

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, sec. 9201, 47 U.S.C. 1201, 1206.

List of Subjects

47 CFR Part 0

Authority delegations (Government agencies), Classified information, Communications, Communications common carriers, Equal access to justice, Freedom of information, Government publications, Infants and children, Investigations, Organization and functions (Government agencies), Penalties, Postal Service, Privacy, Reporting and recordkeeping requirements, Sunshine Act, Telecommunications.

47 CFR Part 10

Communications, Communications common carriers, Communications equipment, Electronic products, Individuals with disabilities, Radio, Telecommunications.

47 CFR Part 11

Radio, Television.

Federal Communications Commission.

Marlene Dortch,
Secretary, Office of the Secretary.

Proposed Rules

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

PART 0 – COMMISSION ORGANIZATION

1. 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.

2. 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

3. 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.

4. 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.

5. 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.

* * * * *

6. 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.

7. 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)

8. 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.

9. 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.

10. 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.

* * * * *

11. 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.

* * * * *

12. 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.

* * * * *

13. 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.

14. 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:

* * * * *

15. 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.

* * * * *

[FR Doc. 2026-15600 Filed: 7/30/2026 8:45 am; Publication Date: 7/31/2026]