**6712-01**

**FEDERAL COMMUNICATIONS COMMISSION**

**47 CFR Part 11**

**[PS Docket No. 15-94, PS Docket No. 15-91; FCC 16-5**

Rules Regarding the Emergency Alert System and Wireless Emergency Alerts

**AGENCY:** Federal Communications Commission.

**ACTION:** Notice of proposed rulemaking

**SUMMARY:** This document proposes taking the next step towards strengthening the nation's public alert and warning systems, the Emergency Alert System (EAS) and Wireless Emergency Alerts (WEA), as community-driven public safety tools capable of ensuring that the public is able to receive and properly respond to alerts issued by alerting authorities in emergency situations. This document seeks comment on proposed rule changes in four areas: improving alerting organization at the state and local levels; building effective community-based public safety exercises; ensuring that alerting mechanisms are able to leverage advancements in technology, including IP-based technologies; and securing the EAS against accidental misuse and malicious intrusion. By this action, the Commission affords interested parties an opportunity to submit comments on these proposed rule changes. Through this action, the Commission hopes to empower state and local alert originators to participate more fully in WEA, and to enhance the utility of EAS and WEA as an alerting tool.

**DATES:** Comments are due on or before [**INSERT DATE 45 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]** and reply comments are due on or before [**INSERT DATE 75 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**. Written Paperwork Reduction Act (PRA) comments on the proposed information collection requirements contained herein must be submitted by the public, Office of Management

and Budget (OMB), and other interested parties on or before **[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

**ADDRESSES:** You may submit comments, identified by PS Docket No. 15-94 and PS Docket No. 15-91, by any of the following methods:

• Federal eRulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.

• Federal Communications Commission's Web site: http://fjallfoss.fcc.gov/ecfs2/. Follow the instructions for submitting comments.

• People with Disabilities: Contact the FCC to request reasonable accommodations (accessible format documents, sign language interpreters, CART, etc.) by email: FCC504@fcc.gov or phone: 202-418-0530 or TTY: 202-418-0432.

For detailed instructions for submitting comments and additional information on the rulemaking process, see the SUPPLEMENTARY INFORMATION section of this document. In addition to filing comments with the Secretary, a copy of any PRA comments on the proposed information collection requirements contained herein should be submitted to the Federal Communications Commission via email to PRA@fcc.gov and to Nicholas A. Fraser, Office of Management and Budget, via email to Nicholas_A._Fraser@omb.eop.gov or via fax at 202-395-5167.

**FOR FURTHER INFORMATION CONTACT:** Lisa Fowlkes, Deputy Bureau Chief, Public Safety and Homeland Security Bureau, at (202) 418-7452, or by email at Lisa.Fowlkes@fcc.gov. For additional information concerning the information collection requirements contained in this document, send an email to PRA@fcc.gov or contact Nicole Ongele, Office of Managing Director, Performance Evaluation and Records Management, 202-418-2991, or by email at Nicole.Ongele@fcc.gov.

**SUPPLEMENTARY INFORMATION:**

This is a summary of the Commission's Notice of Proposed Rulemaking in PS Docket Nos. 15-94 and 15-91, FCC 16-5, released on January 29, 2015. The documents are available for download at http://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db0129/FCC-16-5A1.pdf. The complete text of this document is also available for inspection and copying during normal business hours in the FCC Reference Information Center, Portals II, 445 12th Street SW., Room CY-A257, Washington, DC 20554. To request materials in accessible formats for people with disabilities (Braille, large print, electronic files, audio format), send an email to FCC504@fcc.gov or call the Consumer & Governmental Affairs Bureau at 202-418-0530 (voice), 202-418-0432 (TTY).

This document contains proposed information collection requirements. The Commission, as part of its continuing effort to reduce paperwork burdens, invites the general public and OMB to comment on the information collection requirements contained in this document, as required by the Paperwork Reduction Act of 1995, Public Law 104-13. Public and agency comments on the PRA proposed information collection requirements are due **[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**. Comments should address: (a) Whether the proposed collection of information is necessary for the proper performance of the functions of the Commission, including whether the information shall have practical utility; (b) the accuracy of the Commission's burden estimates; (c) ways to enhance the quality, utility, and clarity of the information collected; (d) ways to minimize the burden of the collection of information on the respondents, including the use of automated collection techniques or other forms of information technology and (e) ways to further reduce the information collection burden on small business concerns with fewer than 25 employees. 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.

To view or obtain a copy of this information collection request (ICR) submitted to OMB: (1) Go to this OMB/GSA web page: http://www.reginfo.gov/public/do/PRAMain, (2) look for the section of the web page called "Currently Under Review," (3) click on the downward-pointing arrow in the "Select Agency" box below the "Currently Under Review" heading, (4) select "Federal Communications Commission" from the list of agencies presented in the "Select Agency" box, (5) click the "Submit" button to the right of the "Select Agency" box, and (6) when the list of FCC ICRs currently under review appears, look for the Title of this ICR and then click on the ICR Reference Number. A copy of the FCC submission to OMB will be displayed.

**OMB Control Number:** 3060-0207.

**Title:** Part 11 – Emergency Alert System (EAS), NPRM, FCC 16-5.

**Form Number:** Not applicable.

**Type of Review:** Revision of a currently approved collection.

**Respondents:** Business or other for-profit entities, not-for-profit institutions, and state, local, or tribal government.

**Number of Respondents and Responses:** 63,080 respondents; 3,597,086 responses.

**Estimated Time per Response:** 51 hours.

**Frequency of Response:** On occasion reporting requirement and recordkeeping requirement.

**Obligation to Respond:** Obligatory for all entities required to participate in EAS. Statutory authority for this collection of information is contained in 47 U.S.C. sections 154(i) and 606 of the Communications Act of 1934, as amended.

**Total Annual Burden:** 116,933 hours.

**Total Annual Cost: None.**

**Privacy Impact Assessment:** No impact(s).

**Nature and Extent of Confidentiality:** The Commission seeks comment on whether any aspects of State EAS Plans submitted via the State EAS Plan Filing Interface (SEPFI) should be made confidential and, further, whether it would be sufficient to provide such data with the same level of confidentiality as test data submitted to the Commission via the Electronic Test Reporting System (ETRS). The Commission has stated that it will allow such data to be shared on a confidential basis with other Federal agencies and state government emergency management agencies that have confidentiality protection at least equal to that provided by the Freedom of Information Act (FOIA, 5 U.S.C. 552 (2006), amended by OPEN Government Act of 2007, Pub. L. No. 110-175, 121 Stat. 2524). The Commission also seeks comment on the degree of confidentiality that should be provided for the security certifications and false alert and lockout notifications submitted to the Commission via ETRS. Specifically, the Commission seeks comment on its tentative conclusion that the act of filing an annual certification and the responses on the face of such certification forms should not be treated as presumptively confidential but that the act of filing addenda to the certification describing alternative approaches or corrective action with respect to performance of required security measures, as well as the contents of such addenda, should be treated as presumptively confidential. The Commission also seeks comment on its tentative conclusion that the mere fact of filing or not filing a false alert report or lockout notification should not be treated as presumptively confidential, while the information submitted in the report should be treated as presumptively confidential.

**Initial Regulatory Flexibility Analysis**

1. As required by the Regulatory Flexibility Act of 1980, as amended (RFA), the Commission has prepared this present Initial Regulatory Flexibility Analysis (IRFA) of the

possible significant economic impact on a substantial number of small entities by the policies and rules proposed in this Notice of Proposed Rulemaking (NPRM). Written public comments are requested on this IRFA. Comments must be identified as responses to the IRFA and must be filed by the deadlines for comments on the NPRM provided in section III of the NPRM. The Commission will send a copy of the NPRM, including this IRFA, to the Chief Counsel for Advocacy of the Small Business Administration (SBA).

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

2. With this NPRM, the Commission takes another step towards strengthening the Emergency Alert System (EAS) and Wireless Emergency Alerts (WEA) as community-driven public safety tools by proposing revisions to the EAS and WEA rules to ensure the public is able to receive and properly respond to alerts issued by alerting authorities in emergency situations. The Commission's proposals fall into four categories, improving alerting organization at the state and local levels, building effective community-based public safety exercises, ensuring that alerting mechanisms are able to leverage advancements in technology (including IP-based technologies), and securing the EAS against accidental misuse and malicious intrusion. With respect to improving alerting organization at the state and local levels, the Commission proposes to adopt EAS designations that more accurately reflect the current roles and responsibilities of key EAS Participants; streamline and update the State EAS Plan filing process by requiring State Emergency Communications Committees (SECCs) to file their plans electronically in an online State EAS Plan filing system; and adopt a standard online template for State EAS Plan content to allow the SECCs to file plans that fully detail their strategy for delivering Presidential and other life-saving alerts in an evolving technological landscape. With respect to building effective community-based alerting exercise programs, the Commission proposes to expand the EAS testing regime to include "live" code tests as community public safety exercises and to allow the

use of EAS header codes and emergency alerting Attention Signal in Public Service Announcements (PSAs) by entities aiming to raise public awareness of, and alert initiator proficiency with EAS. The Commission seeks comment on how to best ensure that community based exercises address the needs of individuals with limited English proficiency and individuals with disabilities. The Commission seeks comment on several issues that reflect the extent to which evolving technologies are changing the alerting landscape. Specifically, the Commission seeks comment on whether to retain the current forced tuning and selective override provisions in light of stakeholder feedback and advances in technology. Further, the Commission seeks comment on whether an EAS Participant cable or Internet Protocol Television (IPTV) provider should be required to deliver EAS alerts and tests over any channel, whether "programmed" or not, if it is controlled by the EAS Participant and viewable by the consumer. Finally, the Commission seeks comment on potential technological advancements to improve alert accessibility.

3. This NPRM represents another step towards achieving one of the Commission's highest priorities – "to ensure that all Americans have the capability to receive timely and accurate alerts, warnings and critical information regarding disasters and other emergencies." This NPRM also is consistent with the Commission's obligation under Executive Order 13407 to "adopt rules to ensure that communications systems have the capacity to transmit alerts and warnings to the public as part of the public alert and warning system," and the Commission's mandate under the Communications Act to promote the safety of life and property through the use of wire and radio communication. The Commission takes these steps as part of an overarching strategy to advance the nation's alerting capability, which includes both WEA and EAS, to keep pace with evolving technologies and to empower communities to initiate life-saving alerts.

### B. Legal Basis

4. Authority for the actions proposed in the NPRM may be found in 47 U.S.C. 151, 152, 154(i), 154(o), 301, 303(b), (g) and (r), 303(v), 307, 309, 335, 403, 544(g), 606, 613, 615 and 1302; Sections 602(a), (b), (c), (d), (f), 603, 604, and 606 of the Warning, Alert and Response Network (WARN) Act, Title VI of the Security and Accountability For Every Port Act of 2006, Pub. L. No. 109-347, 120 Stat. 1884 (2006); Twenty-First Century Communications and Video Accessibility Act of 2010, Pub. L. No. 111-260 and Pub. L. No. 111-265.

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

5. The RFA directs agencies to provide a description of, and, where feasible, an estimate of the number of small entities that may be affected by the proposed rules, if adopted. 5 U.S.C. 603(b)(3). The RFA generally defines the term "small entity" as having the same meaning as the terms "small business," "small organization," and "small governmental jurisdiction." In addition, the term "small business" has the same meaning as the term "small business concern" under the Small Business Act. A "small business concern" is one which: (1) is independently owned and operated; (2) is not dominant in its field of operation; and (3) satisfies any additional criteria established by the SBA. Below, the Commission describes and estimates the number of small entity licensees that may be affected by the proposed rules.

6. Small Businesses, Small Organizations, and Small Governmental Jurisdictions. Nationwide, there are a total of approximately 28.2 million small businesses, according to the SBA. In addition, a "small organization" is generally "any not-for-profit enterprise which is independently owned and operated and is not dominant in its field." Nationwide, as of 2007, there were approximately 1,621,315 small organizations. Finally, the term "small governmental jurisdiction" is defined generally as "governments of cities, towns, townships, villages, school

districts, or special districts, with a population of less than fifty thousand." Census Bureau data for 2007 indicate that there were 89,476 local governmental jurisdictions in the United States. The Commission estimates that, of this total, as many as 88,761 entities may qualify as "small governmental jurisdictions." Thus, the Commission estimates that most governmental jurisdictions are small.

7. Radio Stations. This Economic Census category comprises establishments primarily engaged in broadcasting aural programs by radio to the public. Programming may originate in the station's own studio, from an affiliated network, or from an external source. The SBA defines a radio broadcasting entity that has $38.5 million or less in annual receipts as a small business. According to Commission staff review of the BIA Kelsey Inc. Media Access Radio Analyzer Database as of June 5, 2013, about 90 percent of the 11,340 of commercial radio stations in the United States have revenues of $38.5 million or less. Therefore, the majority of such entities are small entities. The Commission has estimated the number of licensed noncommercial radio stations to be 3,917. The Commission does not have revenue data or revenue estimates for these stations. These stations rely primarily on grants and contributions for their operations, so the Commission will assume that all of these entities qualify as small businesses. The Commission notes that in assessing whether a business entity qualifies as small under the above definition, business control affiliations must be included. In addition, to be determined to be a "small business," the entity may not be dominant in its field of operation. The Commission notes that it is difficult at times to assess these criteria in the context of media entities, and the Commission's estimate of small businesses may therefore be over-inclusive.

8. Low-Power FM Stations. The same SBA definition that applies to radio broadcast licensees would apply to low-power FM ("LPFM") stations. The SBA defines a radio broadcast station as a small business if such station has no more than $38.5 million in annual receipts.

Currently, there are approximately 864 licensed LPFM stations. Given the nature of these services, the Commission will presume that all of these licensees qualify as small entities under the SBA definition.

9. Television Broadcasting. The SBA defines a television broadcasting station as a small business if such station has no more than $38.5 million in annual receipts. Business concerns included in this industry are those "primarily engaged in broadcasting images together with sound." These establishments operate television broadcasting studios and facilities for the programming and transmission of programs to the public. These establishments also produce or transmit visual programming to affiliated broadcast television stations, which in turn broadcast the programs to the public on a predetermined schedule. Programming may originate in the station's own studio, from an affiliated network, or from an external source.

10. According to Commission staff review of the BIA Financial Network, Inc. Media Access Pro Television Database as of March 31, 2013, about 90 percent of an estimated 1,385 commercial television stations in the United States have revenues of $38.5 million or less. Based on this data and the associated size standard, the Commission concludes that the majority of such establishments are small. The Commission has estimated the number of licensed noncommercial educational ("NCE") stations to be 396. The Commission does not have revenue estimates for NCE stations. These stations rely primarily on grants and contributions for their operations, so the Commission will assume that all of these entities qualify as small businesses. In addition, there are approximately 567 licensed Class A stations, 2,227 licensed low-power television ("LPTV") stations, and 4,518 licensed TV translators. Given the nature of these services, the Commission will presume that all LPTV licensees qualify as small entities under the above SBA small business size standard.

11. The Commission notes that in assessing whether a business entity qualifies as small

under the above definition, business control affiliations must be included. The Commission's estimate, therefore, likely overstates the number of small entities affected by the proposed rules, because the revenue figures on which this estimate is based do not include or aggregate revenues from affiliated companies.

12. In addition, an element of the definition of "small business" is that the entity not be dominant in its field of operation. The Commission is unable at this time and in this context to define or quantify the criteria that would establish whether a specific television station is dominant in its market of operation. Accordingly, the foregoing estimate of small businesses to which the rules may apply does not exclude any television stations from the definition of a small business on this basis and is therefore over-inclusive to that extent. An additional element of the definition of "small business" is that the entity must be independently owned and operated. It is difficult at times to assess these criteria in the context of media entities, and the Commission's estimates of small businesses to which they apply may be over-inclusive to this extent.

13. Wired Telecommunications Carriers. This industry comprises establishments "primarily engaged in operating and/or providing access to transmission facilities and infrastructure that they own and/or lease for the transmission of voice, data, text, sound, and video using wired telecommunications networks." Transmission facilities "may be based on a single technology or a combination of technologies." Establishments in this industry use the wired telecommunications network facilities that they operate to provide a variety of services, such as wired telephony services, including VoIP services; wired (cable) audio and video programming distribution; and wired broadband Internet services. By exception, "establishments providing satellite television distribution services using facilities and infrastructure that they operate are included in this industry." In this category, the SBA deems a wired telecommunications carrier to be small if it has 1,500 or fewer employees. Census data for 2007

shows 3,188 firms in this category. Of these, 3,144 had fewer than 1,000 employees. On this basis, the Commission estimates that a substantial majority of the providers of wired telecommunications carriers are small.

14. Cable and Other Subscription Programming. This industry comprises establishments primarily engaged in operating studios and facilities for the broadcasting of programs on a subscription or fee basis. The broadcast programming is typically narrowcast in nature (e.g., limited format, such as news, sports, education, or youth-oriented). These establishments produce programming in their own facilities or acquire programming from external sources. The programming material is usually delivered to a third party, such as cable systems or direct-to-home satellite systems, for transmission to viewers. The SBA size standard for this industry establishes as small any company in this category which receives annual receipts of $38.5 million or less. U.S. Census data for 2007 show that 396 firms operated for the entire year. Of these, 349 operated with annual receipts of less than $25 million a year. Based on this data, the Commission estimates that the majority of firms operating in this industry is small.

15. Cable System Operators (Rate Regulation Standard). The Commission has developed its own small business size standard for cable system operators, for purposes of rate regulation. Under the Commission's Rules, a "small cable company" is one serving 400,000 or fewer subscribers nationwide. Industry data indicate that there are currently 4,600 active cable systems in the United States. Of this total, all but nine cable operators nationwide are small under the 400,000-subscriber size standard. In addition, under the Commission's rate regulation rules, a "small system" is a cable system serving 15,000 or fewer subscribers. Current Commission records show 4,600 cable systems nationwide. Of this total, 3,900 cable systems have fewer than 15,000 subscribers, and 700 systems have 15,000 or more subscribers, based on the same records. Thus, under this standard, the Commission estimates that most cable systems are small.

16. Cable System Operators (Telecom Act Standard). The Communications Act of 1934, as amended, also contains a size standard for small cable system operators, which is "a cable operator that, directly or through an affiliate, serves in the aggregate fewer than 1 percent of all subscribers in the United States and is not affiliated with any entity or entities whose gross annual revenues in the aggregate exceed $250,000,000." There are approximately 52,403,705 cable video subscribers in the United States today. Accordingly, an operator serving fewer than 524,037 subscribers shall be deemed a small operator if its annual revenues, when combined with the total annual revenues of all its affiliates, do not exceed $250 million in the aggregate. Based on available data, the Commission finds that all but nine incumbent cable operators are small entities under this size standard. The Commission notes that it neither requests nor collects information on whether cable system operators are affiliated with entities whose gross annual revenues exceed $250 million. Although it seems certain that some of these cable system operators are affiliated with entities whose gross annual revenues exceed $250,000,000, the Commission is unable at this time to estimate with greater precision the number of cable system operators that would qualify as small cable operators under the definition in the Communications Act.

17. Satellite Telecommunications. This category comprises firms "primarily engaged in providing telecommunications services to other establishments in the telecommunications and broadcasting industries by forwarding and receiving communications signals via a system of satellites or reselling satellite telecommunications." This category has a small business size standard of $32.5 million or less in average annual receipts, under SBA rules. For this category, Census Bureau data for 2007 show that there were a total of 512 satellite communications firms that operated for the entire year. Of this total, 482 firms had annual receipts of less than $25 million. Consequently, the Commission estimates that the majority of Satellite

Telecommunications firms are small entities that might be affected by the Commission's action.

18. Other Telecommunications. This category includes "establishments primarily engaged in . . . providing satellite terminal stations and associated facilities operationally connected with one or more terrestrial communications systems and capable of transmitting telecommunications to or receiving telecommunications from satellite systems." The SBA definition of Other Telecommunications entities comprises those that have $32.5 million or less in average annual receipts. For this category, Census Bureau data for 2007 show that there were a total of 2,383 firms that operated for the entire year. Of this total, 2,346 firms had annual receipts of under $25 million and 37 firms had annual receipts of $25 million to $49,999,999. Consequently, the Commission estimates that the majority of Other Telecommunications firms are small entities that might be affected by the Commission's action.

19. The Educational Broadcasting Services. In addition, the SBA's placement of Cable Television Distribution Services in the category of Wired Telecommunications Carriers is applicable to cable-based Educational Broadcasting Services. Since 2007, these services have been defined within the broad economic census category of Wired Telecommunications Carriers, which was developed for small wireline businesses. This category is defined as follows: "This industry comprises establishments primarily engaged in operating and/or providing access to transmission facilities and infrastructure that they own and/or lease for the transmission of voice, data, text, sound, and video using wired telecommunications networks. Transmission facilities may be based on a single technology or a combination of technologies. Establishments in this industry use the wired telecommunications network facilities that they operate to provide a variety of services, such as wired telephony services, including VoIP services; wired (cable) audio and video programming distribution; and wired broadband Internet services." The SBA has developed a small business size standard for this category, which is: all such businesses

having 1,500 or fewer employees. Census data for 2007 shows that there were 31,996 establishments that operated that year. Of this total, 30,178 establishments had fewer than 100 employees, and 1,818 establishments had 100 or more employees. Therefore, under this size standard, the Commission estimates that the majority of businesses can be considered small entities. In addition to Census data, the Commission's internal records indicate that as of September 2014, there are 2,207 active EBS licenses. The Commission estimates that of these 2,207 licenses, the majority are held by non-profit educational institutions and school districts, which are by statute defined as small businesses.

20. Direct Broadcast Satellite ("DBS") Service. DBS service is a nationally distributed subscription service that delivers video and audio programming via satellite to a small parabolic "dish" antenna at the subscriber's location. DBS is now included in SBA's economic census category "Wired Telecommunications Carriers." This category is defined as follows: "This industry comprises establishments primarily engaged in operating and/or providing access to transmission facilities and infrastructure that they own and/or lease for the transmission of voice, data, text, sound, and video using wired telecommunications networks. Transmission facilities may be based on a single technology or a combination of technologies. Establishments in this industry use the wired telecommunications network facilities that they operate to provide a variety of services, such as wired telephony services, including VoIP services; wired (cable) audio and video programming distribution; and wired broadband Internet services. The SBA has developed a small business size standard for this category, which is: all such businesses having 1,500 or fewer employees. Census data for 2007 shows 3,188 firms in this category. Of these, 3,144 had fewer than 1,000 employees. Based on that data, the Commission concludes that the majority of wireline firms are small under the applicable standard. However, based on more recent data developed internally by the Commission, currently only two entities provide DBS

service, which requires a great deal of capital for operation: DIRECTV and DISH Network. Accordingly, the Commission must conclude that internally developed Commission data are persuasive that in general DBS service is provided only by large firms.

21. Wireless Telecommunications Carriers (except satellite). This industry comprises establishments engaged in operating and maintaining switching and transmission facilities to provide communications via the airwaves. Establishments in this industry have spectrum licenses and provide services using that spectrum, such as cellular phone services, paging services, wireless Internet access, and wireless video services. The appropriate size standard under SBA rules for the category Wireless Telecommunications Carriers (except satellite) is that a business is small if it has 1,500 or fewer employees. Census data for 2007 show that there were 1,383 firms that operated for the entire year. Of this total, 1,368 firms had employment of fewer than 1000 employees. Thus under this category and the associated small business size standard, the Commission estimates that the majority of wireless telecommunications carriers (except satellite) are small.

22. Broadband Personal Communications Service. The broadband personal communications services (PCS) spectrum is divided into six frequency blocks designated A through F, and the Commission has held auctions for each block. The Commission initially defined a "small business" for C- and F-Block licenses as an entity that has average gross revenues of $40 million or less in the three previous calendar years. For F-Block licenses, an additional small business size standard for "very small business" was added and is defined as an entity that, together with its affiliates, has average gross revenues of not more than $15 million for the preceding three calendar years. These small business size standards, in the context of broadband PCS auctions, have been approved by the SBA. No small businesses within the SBA-approved small business size standards bid successfully for licenses in Blocks A and B. There

were 90 winning bidders that claimed small business status in the first two C-Block auctions. A total of 93 bidders that claimed small business status won approximately 40 percent of the 1,479 licenses in the first auction for the D, E, and F Blocks. On April 15, 1999, the Commission completed the reauction of 347 C-, D-, E-, and F-Block licenses in Auction No. 22. Of the 57 winning bidders in that auction, 48 claimed small business status and won 277 licenses.

23. On January 26, 2001, the Commission completed the auction of 422 C and F Block Broadband PCS licenses in Auction No. 35. Of the 35 winning bidders in that auction, 29 claimed small business status. Subsequent events concerning Auction 35, including judicial and agency determinations, resulted in a total of 163 C and F Block licenses being available for grant. On February 15, 2005, the Commission completed an auction of 242 C-, D-, E-, and F-Block licenses in Auction No. 58. Of the 24 winning bidders in that auction, 16 claimed small business status and won 156 licenses. On May 21, 2007, the Commission completed an auction of 33 licenses in the A, C, and F Blocks in Auction No. 71. Of the 12 winning bidders in that auction, five claimed small business status and won 18 licenses. On August 20, 2008, the Commission completed the auction of 20 C-, D-, E-, and F-Block Broadband PCS licenses in Auction No. 78. Of the eight winning bidders for Broadband PCS licenses in that auction, six claimed small business status and won 14 licenses.

24. Narrowband Personal Communications Service. To date, two auctions of narrowband personal communications services (PCS) licenses have been conducted. For purposes of the two auctions that have already been held, "small businesses" were entities with average gross revenues for the prior three calendar years of $40 million or less. Through these auctions, the Commission has awarded a total of 41 licenses, out of which 11 were obtained by small businesses. To ensure meaningful participation of small business entities in future auctions, the Commission has adopted a two-tiered small business size standard in the Narrowband PCS

Second Report and Order. A "small business" is an entity that, together with affiliates and controlling interests, has average gross revenues for the three preceding years of not more than $40 million. A "very small business" is an entity that, together with affiliates and controlling interests, has average gross revenues for the three preceding years of not more than $15 million. The SBA has approved these small business size standards.

25. Wireless Communications Services. This service can be used for fixed, mobile, radiolocation, and digital audio broadcasting satellite uses. The Commission defined "small business" for the wireless communications services (WCS) auction as an entity with average gross revenues of $40 million for each of the three preceding years, and a "very small business" as an entity with average gross revenues of $15 million for each of the three preceding years. The SBA has approved these definitions.

26. 700 MHz Guard Band Licensees. In 2000, in the 700 MHz Guard Band Order, the Commission adopted size standards for "small businesses" and "very small businesses" for purposes of determining their eligibility for special provisions such as bidding credits and installment payments. A small business in this service is an entity that, together with its affiliates and controlling principals, has average gross revenues not exceeding $40 million for the preceding three years. Additionally, a very small business is an entity that, together with its affiliates and controlling principals, has average gross revenues that are not more than $15 million for the preceding three years. SBA approval of these definitions is not required. An auction of 52 Major Economic Area licenses commenced on September 6, 2000, and closed on September 21, 2000. Of the 104 licenses auctioned, 96 licenses were sold to nine bidders. Five of these bidders were small businesses that won a total of 26 licenses. A second auction of 700 MHz Guard Band licenses commenced on February 13, 2001, and closed on February 21, 2001. All eight of the licenses auctioned were sold to three bidders. One of these bidders was a small

business that won a total of two licenses.

27. Lower 700 MHz Band Licenses. The Commission previously adopted criteria for defining three groups of small businesses for purposes of determining their eligibility for special provisions such as bidding credits. The Commission defined a "small business" as an entity that, together with its affiliates and controlling principals, has average gross revenues not exceeding $40 million for the preceding three years. A "very small business" is defined as an entity that, together with its affiliates and controlling principals, has average gross revenues that are not more than $15 million for the preceding three years. Additionally, the lower 700 MHz Service had a third category of small business status for Metropolitan/Rural Service Area (MSA/RSA) licenses—"entrepreneur"—which is defined as an entity that, together with its affiliates and controlling principals, has average gross revenues that are not more than $3 million for the preceding three years. The SBA approved these small size standards. An auction of 740 licenses (one license in each of the 734 MSAs/RSAs and one license in each of the six Economic Area Groupings (EAGs)) commenced on August 27, 2002, and closed on September 18, 2002. Of the 740 licenses available for auction, 484 licenses were won by 102 winning bidders. Seventy-two of the winning bidders claimed small business, very small business or entrepreneur status and won a total of 329 licenses. A second auction commenced on May 28, 2003, closed on June 13, 2003, and included 256 licenses: 5 EAG licenses and 476 Cellular Market Area licenses. Seventeen winning bidders claimed small or very small business status and won 60 licenses, and nine winning bidders claimed entrepreneur status and won 154 licenses. On July 26, 2005, the Commission completed an auction of 5 licenses in the Lower 700 MHz band (Auction No. 60). There were three winning bidders for five licenses. All three winning bidders claimed small business status.

28. In 2007, the Commission reexamined its rules governing the 700 MHz band in the

700 MHz Second Report and Order. An auction of 700 MHz licenses commenced January 24, 2008 and closed on March 18, 2008, which included, 176 Economic Area licenses in the A Block, 734 Cellular Market Area licenses in the B Block, and 176 EA licenses in the E Block. Twenty winning bidders, claiming small business status (those with attributable average annual gross revenues that exceed $15 million and do not exceed $40 million for the preceding three years) won 49 licenses. Thirty three winning bidders claiming very small business status (those with attributable average annual gross revenues that do not exceed $15 million for the preceding three years) won 325 licenses.

29. Upper 700 MHz Band Licenses. In the 700 MHz Second Report and Order, the Commission revised its rules regarding Upper 700 MHz licenses. On January 24, 2008, the Commission commenced Auction 73 in which several licenses in the Upper 700 MHz band were available for licensing: 12 Regional Economic Area Grouping licenses in the C Block, and one nationwide license in the D Block. The auction concluded on March 18, 2008, with 3 winning bidders claiming very small business status (those with attributable average annual gross revenues that do not exceed $15 million for the preceding three years) and winning five licenses.

30. Advanced Wireless Services. AWS Services (1710–1755 MHz and 2110–2155 MHz bands (AWS-1); 1915–1920 MHz, 1995–2000 MHz, 2020–2025 MHz and 2175–2180 MHz bands (AWS-2); 2155–2175 MHz band (AWS-3)). For the AWS-1 bands, the Commission has defined a "small business" as an entity with average annual gross revenues for the preceding three years not exceeding $40 million, and a "very small business" as an entity with average annual gross revenues for the preceding three years not exceeding $15 million. For AWS-2 and AWS-3, although the Commission does not know for certain which entities are likely to apply for these frequencies, the Commission notes that the AWS-1 bands are comparable to those used for cellular service and personal communications service. The Commission has not yet adopted

size standards for the AWS-2 or AWS-3 bands but proposes to treat both AWS-2 and AWS-3 similarly to broadband PCS service and AWS-1 service due to the comparable capital requirements and other factors, such as issues involved in relocating incumbents and developing markets, technologies, and services.

31. Broadband Radio Service and Educational Broadband Service. Broadband Radio Service systems, previously referred to as Multipoint Distribution Service (MDS) and Multichannel Multipoint Distribution Service (MMDS) systems, and "wireless cable," transmit video programming to subscribers and provide two-way high speed data operations using the microwave frequencies of the Broadband Radio Service (BRS) and Educational Broadband Service (EBS) (previously referred to as the Instructional Television Fixed Service (ITFS)). In connection with the 1996 BRS auction, the Commission established a small business size standard as an entity that had annual average gross revenues of no more than $40 million in the previous three calendar years. The BRS auctions resulted in 67 successful bidders obtaining licensing opportunities for 493 Basic Trading Areas (BTAs). Of the 67 auction winners, 61 met the definition of a small business. BRS also includes licensees of stations authorized prior to the auction. At this time, the Commission estimates that of the 61 small business BRS auction winners, 48 remain small business licensees. In addition to the 48 small businesses that hold BTA authorizations, there are approximately 392 incumbent BRS licensees that are considered small entities. After adding the number of small business auction licensees to the number of incumbent licensees not already counted, the Commission finds that there are currently approximately 440 BRS licensees that are defined as small businesses under either the SBA or the Commission's rules.

32. In 2009, the Commission conducted Auction 86, the sale of 78 licenses in the BRS areas. The Commission offered three levels of bidding credits: (i) a bidder with attributed

average annual gross revenues that exceed $15 million and do not exceed $40 million for the preceding three years (small business) received a 15 percent discount on its winning bid; (ii) a bidder with attributed average annual gross revenues that exceed $3 million and do not exceed $15 million for the preceding three years (very small business) received a 25 percent discount on its winning bid; and (iii) a bidder with attributed average annual gross revenues that do not exceed $3 million for the preceding three years (entrepreneur) received a 35 percent discount on its winning bid. Auction 86 concluded in 2009 with the sale of 61 licenses. Of the ten winning bidders, two bidders that claimed small business status won 4 licenses; one bidder that claimed very small business status won three licenses; and two bidders that claimed entrepreneur status won six licenses.

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

34. Radio and Television Broadcasting and Wireless Communications Equipment Manufacturing. The Census Bureau defines this category as follows: "This industry comprises establishments primarily engaged in manufacturing radio and television broadcast and wireless communications equipment. Examples of products made by these establishments are: transmitting and receiving antennas, cable television equipment, GPS equipment, pagers, cellular

phones, mobile communications equipment, and radio and television studio and broadcasting equipment." The SBA has developed a small business size standard for firms in this category, which is: all such firms having 750 or fewer employees. According to Census Bureau data for 2010, there were a total of 810 establishments in this category that operated for the entire year. Of this total, 787 had employment of fewer than 500, and an additional 23 had employment of 500 to 999. Thus, under this size standard, the majority of firms can be considered small.

35. Software Publishers. Since 2007 these services have been defined within the broad economic census category of Custom Computer Programming Services; that category is defined as establishments primarily engaged in writing, modifying, testing, and supporting software to meet the needs of a particular customer. The SBA has developed a small business size standard for this category, which is annual gross receipts of $25 million or less. According to data from the 2007 U.S. Census, there were 41,571 establishments engaged in this business in 2007. Of these, 40,149 had annual gross receipts of less than $10,000,000. Another 1,422 establishments had gross receipts of $10,000,000 or more. Based on this data, the Commission concludes that the majority of the businesses engaged in this industry are small.

36. NCE and Public Broadcast Stations. The Census Bureau defines this category as follows: "This industry comprises establishments primarily engaged in broadcasting images together with sound. These establishments operate television broadcasting studios and facilities for the programming and transmission of programs to the public." The SBA has created a small business size standard for Television Broadcasting entities, which is: such firms having $38.5 million or less in annual receipts. According to Commission staff review of the BIA Publications, Inc., Master Access Television Analyzer Database as of May 16, 2003, about 814 of the 1,220 commercial television stations in the United States had revenues of $12 (twelve) million or less. The Commission notes, however, that in assessing whether a business concern

qualifies as small under the above definition, business (control) affiliations must be included. The Commission's estimate, therefore, likely overstates the number of small entities that might be affected by the Commission's action, because the revenue figure on which it is based does not include or aggregate revenues from affiliated companies.

37. In addition, an element of the definition of "small business" is that the entity not be dominant in its field of operation. The Commission is unable at this time to define or quantify the criteria that would establish whether a specific television station is dominant in its field of operation. Accordingly, the estimate of small businesses to which rules may apply do not exclude any television station from the definition of a small business on this basis and are therefore over-inclusive to that extent. Also as noted, an additional element of the definition of "small business" is that the entity must be independently owned and operated. The Commission notes that it is difficult at times to assess these criteria in the context of media entities and the Commission's estimates of small businesses to which they apply may be over-inclusive to this extent. There are also 2,117 low power television stations (LPTV). Given the nature of this service, the Commission will presume that all LPTV licensees qualify as small entities under the above SBA small business size standard.

38. The Commission has estimated the number of licensed NCE television stations to be 380. The Commission notes, however, that, in assessing whether a business concern qualifies as small under the above definition, business (control) affiliations must be included. The Commission's estimate, therefore, likely overstates the number of small entities that might be affected by the Commission's action, because the revenue figure on which it is based does not include or aggregate revenues from affiliated companies. The Commission does not compile and otherwise does not have access to information on the revenue of NCE stations that would permit it to determine how many such stations would qualify as small entities.

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

39. This Notice of Proposed Rulemaking proposes to expand the scope of State EAS Plans to include additional information necessary to reflect advances in technology, and to ensure the successful transmission of a Presidential Alert, such as uniform EAS designations, a description of SECC governance structure, expanded descriptions of emergency alerting procedures, a more accurate statement of monitoring requirements, a statement of the extent to which states leverage one-to-many/many-to-one communications, expanded testing procedures and security elements. It proposes that such Plans be submitted via an online State EAS Plan Filing Interface (SEPFI) designed to minimize filing burdens attendant to the Commission's State EAS Plan requirements, and to offset any additional burden that the Commission's expanded requirements may impose.

40. This Notice of Proposed Rulemaking also proposes adding an annual certification to the existing Form 1 of the mandatory electronic reporting system, Electronic Test Reporting System (ETRS), that EAS Participants have done the following: (1) kept their systems updated with the latest firmware and software patches, (2) put a program in place to control access to EAS devices that includes changing default passwords, requiring password complexity, and removing or disabling expired accounts, (3) ensured that all EAS devices are not directly accessible from the Internet, and that, if required, any remote access is properly secured and logged, and (4) configured EAS devices to validate digital signatures on CAP messages if the source of the CAP message requires this feature. Depending on whether the employee checking for performance of required security measures is also the certifying official, including a certification on Form 1 could take between five minutes and an hour for the many EAS Participants that already have performed all required security measures. The Commission estimates that additional time, and legal and managerial resources may be needed for some EAS

Participants to complete this certification in the first instance only. For those who are not using best practices, the Commission estimates it should take no more than four hours per device to perform the necessary changes. Given the importance of maintaining basic security hygiene, the Commission proposes that the impact on small entities of this annual certification would not impose an undue burden.

41. The Commission also proposes extending ETRS to include a false alert and lockout reporting requirement. An initial report including only the EAS header codes and time discovered of the false message may be required within fifteen to thirty minutes of identification of a false EAS message transmission, and a final report may be required within seventy-two hours including the root cause of the improper transmission. Because EAS security incidents have occurred at a rate of one or two per year and EAS Participants must already investigate unauthorized EAS alert matters as they occur, a reporting requirement for false alerts and lockouts would likely have a very minimal impact on small entities.

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

42. The RFA requires an agency to describe any significant, specifically small business alternatives that it has considered in reaching its conclusions, which may include the following four alternatives (among others): "(1) the establishment of differing compliance or reporting requirements or timetables that take into account the resources available to small entities; (2) the clarification, consolidation, or simplification of compliance or reporting requirements under the rule for small entities; (3) the use of performance, rather than design, standards; and (4) an exemption from coverage of the rule, or any part thereof, for small entities." 5 U.S.C. 603(c)(1)-(c)(4).

43. With respect to the State EAS Plan filing process, converting the paper-based filing process into an online process is intended to reduce reporting costs and associated burdens for

SECCs. With respect to State EAS Plan contents, the Commission seeks comment on whether the same EAS designations and plan components can be applied universally to all states, and have taken steps to allow states flexibility to stipulate EAS Plans that fit their individual needs. With respect to live code tests, the Commission seeks comment on whether removing the need for SECCs to request a waiver of the Commission's rules to conduct live code tests will reduce costs and remove regulatory burdens. With respect to forced tuning and selective override provisions, the Commission seeks comment on whether small entities should be subject to different requirements than their larger counterparts.

44. With respect to security, smaller entities often face particular challenges in maintaining awareness of current security measures, due to limited human, financial or technical resources; however, the Commission is merely proposing performance of required security measures to which many EAS Participants, including smaller entities, already adhere. Because proper patching and updating and basic account management are common best practices accepted across the sector, the assumption is that there would be no additional impact on small entities to keep EAS systems current. An annual certification allows small entities to comply even if they choose to update patches semi-annually rather than quarterly, and small entities may alternatively explain why they are unable to certify. Digital signature authentication has more of an impact on states, which must modify EAS plans, and smaller entities often have the advantage of simpler setups than those of large entities.

45. The Commission seeks comment on whether the Presidential Alert warrants additional/heightened security measures whose costs may exceed the benefits when applied to alerts that are issued more commonly, and that have a less immediate impact on national security. The Commission seeks comment on whether to except EAS Participants currently designated as PN stations from some or all of the security requirements the Commission

proposes. The Commission also seeks comment on whether and how it should consider excepting EAS Participants that qualify as "small businesses" under the Small Business Association (SBA) standard their respective industries from some or all of the security requirements it proposes. Finally, the Commission proposes implementation timeframes for each of its rules that are intended to allow EAS Participants to come into compliance with its rules in a manner that balances the need for improving EAS organization and effectiveness as soon as possible, with any potential burdens that may be imposed by adoption of its proposals.

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

46. None

**Synopsis of the Notice of Proposed Rulemaking**

47. Technological advancements continue to change the landscape of alerting for emergency managers. Alerting tools such as EAS and WEA that had previously occupied fundamentally different infrastructures now share common platforms and a common language. Social media such as Google and Twitter provide emergency managers with entirely new ways of informing the public of dangers to life and property, and new ways of assessing the public's response. The interactivity enabled by IP-based systems may provide emergency managers with the opportunity to receive rapid feedback from the public on the effectiveness of alerts and warnings.

48. The Commission is obligated to ensure that the President can reach the public in times of national emergency. In light of continuous technological advancements, the Commission has taken significant steps to ensure that the nation's public alert and warning systems perform this function in an effective and accessible manner. At the same time, the Commission must continue to review its rules to ensure that the EAS and WEA perform this important function in a manner that minimizes burdens for stakeholders and safeguards these alerting systems against inherent vulnerabilities and attacks. Accordingly, this NPRM proposes rules and seeks comment on alerting issues in an evolving technological climate in order to continue to provide emergency managers with effective tools to assess

and coordinate available alerting systems to securely deliver an alert from the President during a national crisis, and to improve the ability of emergency managers to alert and train those communities to take protective action in response to national, regional and local emergencies.

49. As discussed in greater detail below, the Commission estimates that the cost of the proposed changes would be more than offset by the public benefit of lives saved, together with the reduction in human suffering and property loss. One measure against which the Commission can balance costs associated with complying with its proposed rules is the Department of Transportation (DOT) model, which estimates the value of risk reduction, measured in terms of an expected life saved, to be $9.1 million. Using the Value of a Statistical Life (VSL) as a benchmark, even one life saved could more than offset the one-time costs potentially imposed by the Commission's proposals. The Commission anticipates that its proposed rules represent an incremental improvement to the nation's alerting capability that could readily save multiple lives per year in the foreseeable future. The Commission seeks comment on this analysis, and on whether the DOT statistic is the most appropriate yardstick to measure the benefits our proposals. The Commission seeks comment on whether there is a better measure for quantifying the benefits of establishing a new alerting paradigm. If so, commenters should specify what specific measure should be used. The Commission encourages commenters to include with their comments any data relevant to its analysis of the costs and timing involved with the implementation of today's proposals.

## II. NOTICE OF PROPOSED RULEMAKING

### A. Improving Alert Organization at the State and Local Levels

#### 1. EAS Designations

50. The Commission created EAS designations to "use succinct terminology to more clearly define EAS functions." The current EAS designations are:

- **Primary Entry Point (PEP) System**. Defined in Section 11.2, 47 CFR 11.2, as "a nationwide network of broadcast stations and other entities connected with government activation points . . . used to distribute EAS messages . . . formatted in the EAS Protocol .

. . , including the [Emergency Action Notification (EAN)] and EAS national test messages" that includes "some of the nation's largest radio broadcast stations," as approved by FEMA, and is "designated to receive the Presidential alert from FEMA and distribute it to local stations."

- **National Primary (NP) stations**. Defined in Section 11.2 as "the primary entry point for Presidential messages delivered by FEMA . . . responsible for broadcasting a Presidential alert to the public and to State Primary stations within their broadcast range," and by Section 11.18 simply as "a source of EAS Presidential messages."
- **State Primary (SP) stations**. Defined in Section 11.2 as "the entry point for State messages, which can originate from the Governor or a designated representative." Section 11.18 defines SP stations as "a source of EAS State messages" and adds that such messages originate from the "State Emergency Operating Center (EOC) or State Capital," and that such messages "are sent via the State Relay Network."
- **State Relay Network**. Defined in Section 11.20 as a network composed of "State Relay (SR) sources, leased common carrier communications facilities or any other available communication facilities. The network distributes State EAS messages originated by the Governor or designated official."
- **State Relay (SR)**. Defined in Section 11.18 as "a source of EAS State messages" that is "part of the State Relay Network and relays National and State common emergency messages into Local Areas."
- **Local Primary (LP) stations**. Defined in Section 11.2 as radio or TV stations that act as key EAS monitoring sources, stating that each LP station "must monitor its regional PEP station and a back-up source for Presidential messages." LPs are further defined in Section 11.18 as "a source of EAS Local Area messages . . . responsible for coordinating

the carriage of common emergency messages from sources such as the National Weather Service or local emergency management offices as specified in its EAS Local Area Plan." According to Section 11.18, if an LP "is unable to carry out this function, other LP sources in the Local Area may be assigned the responsibility as indicated in State and Local Area Plans" and "LP sources are assigned numbers (LP-1, 2, 3, *etc*.) in the sequence they are to be monitored by other broadcast stations in the Local Area."

- **Participating National (PN) sources**. Defined in Section 11.18 as sources that "transmit EAS National, State or Local Area messages . . . for direct public reception," as defined in Section 11.18.
- NP, SP, LP and SR stations are defined collectively in Section 11.21 as "key EAS sources."

51. Since the Commission defined these EAS designations, SECCs have taken disparate approaches to their implementation, leading to the inconsistent use of these terms among State EAS Plans. For example, not all State EAS Plans contain an NP-designated station, and it is unclear whether, in some states, the designations PEP and NP are used interchangeably. Further, while some State EAS Plans refer to primary sources of state and local alerts as SPs, others identify primary sources as SRs. A number of State EAS Plans term the system of transmitting state alerts from SR to LP stations and from LP stations to PN stations and the public as the State Relay Network, but many State EAS Plans do not include SR or State Relay Network designations at all. As the Nationwide EAS Test Report indicated, such disparate use of what should be common terminology makes it difficult for Commission staff to determine how the distribution systems described in various state plans can be aggregated into a single comprehensive nationwide alerting architecture.

52. In order to ensure that the Commission can meaningfully review and confirm states'

preparedness to deliver Presidential Alerts the Commission proposes to revise its EAS designation scheme to more accurately and consistently describes key EAS sources. Specifically, the Commission proposes to continue to designate the primary entry point for a Presidential Alert as a PEP, as that is a designation determined by FEMA. For each State EAS Plan, however, the Commission proposes that the entity tasked with primary responsibility for delivering the Presidential Alert to that state's EAS Participants will be designated as the National Primary (NP). Thus, for a state that has a FEMA-designated PEP, that station would also be designated as that state's NP. For a state that does not have a PEP, another station would have to be identified to act as the state's NP. The Commission further proposes that an entity tasked with initiating the delivery of a state EAS alert will be designated as a State Primary (SP). An SP may be a broadcaster, a state emergency management office, or other authorized entity capable of initiating a state-based EAS alert. The Commission proposes that the same entity may be designated as an SP and as an NP. In that case, each designation for that station would have to be separately listed in the State EAS Plan. The Commission would retain the current definition of Participating National (PN) and Local Primary (LP). In cases where geography or other reasons necessitate another layer of monitoring and retransmission between the LP and PN levels, the Commission proposes that such stations be designated in State EAS Plans as "Relay Stations." The Commission anticipates that this proposed terminology scheme would more clearly define key EAS functions in a manner that could be used consistently across all State EAS Plans. As discussed in further detail below, the standard SEPFI template provides an opportunity to ensure that, going forward, these terms are used pursuant to a common understanding of their meaning.

53. The Commission seeks comment on the designations it has identified, based on its analysis of State EAS Plans, as necessary for the successful distribution of Presidential, state and

local EAS alerts. The Commission also seeks comment on whether additional EAS designations may be needed, for example to encompass new roles EAS Participants may play in an evolving technological environment, non-traditional monitoring sources, CAP-formatted alerts, and a more accurate way to account for the significant number of viewers served by cable service providers. The Commission seeks comment on whether its proposed designations could be used as a uniform vernacular to clarify the roles of EAS Participants, including key EAS sources, in each state and territory.

54. Roles and Designations. Do the current EAS designations limit SECCs ability to adequately assign roles and responsibilities to EAS Participants in their respective states? Or, on the other hand, does the Commission currently maintain more EAS designations than are necessary for this task? The Commission seeks comment on how SECCs currently distinguish between PEPs and NP stations. Can one station have both designations? Do the meanings of these terms overlap, as they are used in State EAS Plans? If not every state contains a PEP station, do states designate as NP the station or stations in their state responsible for monitoring the nearest PEP? If so, how does this designation differ from that of an SP station? Are some SPs also denominated as NPs where they act as the primary entry point for both the presidential and some or all state and local alerts? If the definitions of the terms PEP, NP, and SP significantly overlap, is it appropriate that the Commission simplifies its EAS denominations by eliminating extraneous terms?

55. Do all state and local alerts originate at the same source? If not, should the Commission provide SECCs with terms that allow them to distinguish among the primary initiation points for the various types of state and local alerts that are initiated in their respective states? What would be an appropriate title for such designations? For example, would it be appropriate to designate the source responsible for originating an AMBER Alert as a State

AMBER Alert Primary? Conversely, are some state or local alerts likely to initiate from more than one source, frustrating the use of a single designation? Is it appropriate that the Commission continues to use LP as the denomination for those stations that are monitored by PN stations? Is it appropriate that the Commission continues to use the term PN for stations that are not monitored, in light of the fact that the Non-Participating National (NN) designation was deleted from the rules when the Commission required all EAS Participants to carry the Presidential Alert? If not, what designation would be preferable?

56. Uniform Vernacular. Can the designations the Commission proposes be used as a uniform vernacular for referring to the roles of EAS Participants in State EAS Plans? CSRIC IV notes that there is "no one-size-fits-all framework" that can be applied to every SECC because SECCs have limited resources to write State EAS Plans. Although each SECC must create a State EAS Plan that addresses the needs of their respective states, fundamental components of EAS are uniformly implemented nationwide. In the Commission's analysis, these commonalities are sufficient to support successful implementation of a uniform set of EAS designations, and the uniform designations that the Commission proposes to adopt are sufficient to describe states' varied approaches to EAS. The Commission seeks comment on this analysis, and on any idiosyncrasies in states' approaches to EAS that may merit special consideration. The Commission also seeks comment on whether the same EAS designations can be used both for EAS Participants' role in transmitting the Presidential Alert, as well as for state and local EAS alerts. Finally, the Commission also seeks comment on CSRIC IV's conclusion that limitations on state resources frustrate the use of uniform designations. What additional resources, if any, would be necessary to utilize the EAS designations that the Commission proposes to adopt?

57. Additional Designations. Are additional EAS designations necessary to reflect

changes in the alerting landscape? Should EAS designations reflect the service provided by the designated entity in light of the fact that EAS Participants are no longer only broadcasters, and that many EAS Participants monitor non-broadcast sources, such as satellite? For example, would it be appropriate for State EAS Plans to designate a "satellite NP?" Are EAS designations useful for CAP monitoring, or does the fact that most EAS Participants receive an EAS alert by monitoring a CAP feed preclude the need for designations? Further, the Commission seeks comment on whether any EAS Participants other than broadcasters (*e.g.*, analog and digital cable systems, wireline video systems, wireless cable systems and direct broadcast satellite) are currently designated as key EAS sources. Should they be? The Commission notes, for example, that an individual cable headend can be responsible for delivering an EAS alert to as many as 803,000 subscribers. In light of these facts, the Commission believes that the ability of cable providers, DBS providers and wireline video providers to effectively transmit an EAS alert would be crucial to the American public's ability to receive a Presidential Alert. Should the Commission update EAS designations to add a category for cable and other Multichannel Video Programming Distributors (MVPDs) that monitor LPs but serve a significant number of people? What about any other EAS Participant that serves a significant portion of the public? Should the EAS Participants with the most extensive coverage or subscribership in a state be given a specific EAS designation? Should they be considered key EAS sources, notwithstanding the fact that they are not monitored by other EAS Participants? Should entities other than broadcasters be monitored by EAS Participants? The Commission also seeks comment on the extent to which non-broadcaster EAS Participants are members of or otherwise involved in the operations of their SECCs. What steps can the Commission take to facilitate increased participation by representatives of these entities in the SECC and State EAS Plan process?

### 2. State EAS Plan Filing Interface (SEPFI)

58. The Commission adopted rules requiring states to file State EAS Plans that "contain guidelines which must be followed by EAS Participants' personnel, emergency officials, and National Weather Service (NWS) personnel to activate the EAS." These rules maintain the role of state and local committees in strategically organizing state and local EAS Participants into a network capable of ensuring the proper dissemination of, inter alia, the Presidential Alert. State EAS Plans are required to be submitted for review and approval by the Chief, Public Safety and Homeland Security Bureau (Bureau) prior to their implementation "to ensure that they are consistent with national plans, FCC regulations, and EAS operation." This requirement was adopted in light of commenters' assertions that the Commission must adopt safeguards to ensure that EAS is not abused, and that alerts are used only for genuine emergencies.

59. Following the first nationwide EAS test in 2011, the Bureau recommended that the Commission "consider whether to make the State EAS Plan filing process into an online, rather than a paper-based process" in light of inconsistencies identified in the structure of State EAS Plans. Subsequently, in the Sixth Report and Order, the Commission adopted the Electronic Test Reporting System (ETRS), which provides a standardized, online reporting mechanism for the submission and analysis of monitoring assignment data that can be cross-referenced with the EAS Participant designations and monitoring assignments contained in the State EAS Plans. Further, the Commission tasked CSRIC IV with recommending actions to improve the State EAS Plan filing process, and received a recommendation that State EAS Plans should be filed online. CSRIC IV also adopted recommendations regarding access to the recommended online platform, State EAS Plan template design, and identification mechanisms for facilities and geographic areas contained within State EAS Plans. The Commission seeks comment on these recommendations below.

60. The Commission proposes to convert the paper-based filing process for State EAS Plans into a secure, online process using a State EAS Plan Filing Interface (SEPFI) that would be designed to interoperate with the ETRS. The data collected in SEPFI would complement the monitoring assignment data already collected by ETRS. The data collected via ETRS and SEPFI would provide an end-to-end picture of the EAS distribution architecture for each state that could be used to populate an EAS Mapbook. The Commission proposes that the entry format for State EAS Plan data into SEPFI would be a pre-configured online template to be designed by the Bureau in collaboration with SECCs and other stakeholders, using a similar to process to the one the Commission directed the Bureau to use when designing the templates for ETRS. CSRIC IV observes that State EAS Plans are inconsistent in both structure and content, and that "[t]his lack of consistency makes it difficult for the FCC to determine if a proper distribution network exists for . . . distribution [of the Presidential Alert] in each state." The Commission seeks comment on this proposed online filing process below.

61. Costs. The Commission seeks comment on the cost savings likely to result from adopting SEPFI. The EAS collection approved by the Office of Management and Budget (OMB) estimates that each State EAS Plan takes twenty hours to complete, and that the average hourly wage of an individual who completes a State EAS Plan is $25 per/hour. Accordingly, OMB approves of the Commission's estimate that the production of State EAS Plans, nationwide, costs $25,000. How much reporting time and cost would be saved by bringing this process online if certain aspects of State EAS Plans could be automatically updated and populated by cross-referencing data already collected by the FCC, as recommended by CSRIC IV? For example, could SEPFI be pre-populated with data contained in the Consolidated Database System (CDBS), Licensing and Management System (LMS), or other relevant databases? The Commission seeks comment on CSRIC IV's recommendation. Would

additional time and cost be saved by offering users drop-down menus for each EAS designation that could include every licensed EAS Participant in the state? The Commission also seeks cost on any legal fees that SECCs may incur in order to ensure compliance with its proposed State EAS Plan requirements. In light of these potential improvements, the Commission seeks comment on whether any cost associated with requiring SECCs to reenter State EAS Plan data online would be significantly lower than those required to draft a new paper-based plan, and would be outweighed over time by the efficiency and/or other benefits (such as standardization of the information offered by the State EAS Plans, as described below) of an online, template-based process.

62. With respect to the potential administrative cost savings, the Commission anticipates that the proposed use of a template will facilitate the agency's review of the Plans. Because the State Plans currently are submitted in differing formats, with different levels of detail and using inconsistent terminology, it can be time-consuming and difficult to conduct a review that ensures that each Plan contains the elements required by the rules, or that the Plans, in concert, will function efficiently and effectively as a nationwide daisy chain that can pass along alerts in a seamless manner. The Commission believes that with the use of an on-line template, the Commission's ability to review the Plans for compliance with the required elements and to identify potential problems that might hinder achieving the basic goals of the EAS will be improved by enabling us to conduct such reviews in a quicker and more accurate fashion. Facilitating the review process in this manner may not only improve the effectiveness of the EAS, but it could yield significant administrative cost savings to the extent that FCC review and approval of the Plans could be automated, at least in part. The Commission seeks comment on the likelihood and weight of such potential benefits.

63. Standardization. Would adopting a standardized online template dramatically

increase the consistency and thoroughness of State EAS Plans? According to CSRIC IV, "SECCs need the resource of a federal government database to assure EAN dissemination." The Commission seeks comment on CSRIC IV's conclusion. On the other hand, CSRIC IV notes that there is "no one-size-fits-all framework" that can be applied to every SECC, because SECCs have limited resources to write State EAS Plans. The Commission seeks comment on the extent to which a standardized template for State EAS Plans would contribute to improving the efficacy and standardization of EAS, as well as streamline the development of State EAS Plans by identifying the appropriate informational parameters for State EAS Plans. What resource limitations do SECCs encounter that potentially challenge their ability to produce standardized State EAS Plans, and what measures could the Commission take to help address these constraints?

64. Structure. What is the optimal structure for the SEPFI template? CSRIC IV recommends that the Commission should follow the matrix-based model exemplified by the Washington State EAS Plan to quickly, clearly, and efficiently identify the dissemination path of the Presidential Alert through each state. The Commission seeks comment on whether the SEPFI template should be based on the matrix used by the Washington State EAS Plan. Could this matrix be adapted to also illustrate the dissemination path for alerts formatted in CAP, including state and local alerts? The Commission seeks comment on how the SEPFI template should identify EAS Participants. CSRIC IV recommends that EAS Participants be identified by FCC Facility ID as well as by a station's call letters in order "to reduce the need for frequent changes and updates to the database, and state plans due only to changes in call letters." The Commission seeks comment on CSRIC IV's recommendation, as well as on the optimal implementation of other structural elements of SEPFI.

65. Security. The Commission seeks comment on whether access to State EAS Plan data

should be limited and secured, as CSRIC IV recommends, and on the steps the Commission should take to safeguard against unauthorized access to SEPFI. Specifically, CSRIC IV recommends that the Commission should follow the Disaster Information Reporting System (DIRS) access model. The Commission observes that DIRS utilizes a two-layer access model and provides a secure methodology for multiple company employees to access the DIRS database, causing the Commission to believe that the model could be easily adaptable to the State EAS Plan context. The Commission seeks comment on whether access to SEPFI should be based on access provisions for DIRS. Similar to DIRS, should SEPFI utilize a two-layer security system, requiring both a SECC ID and an individual User ID to prevent any unauthorized person from establishing a fraudulent User ID under the company's name? The Commission seeks comment on the identifying information that SECCs should be required to provide for the individuals authorized to access the SEPFI. Should such information include a contact name, affiliated company name, office and cell phone numbers, and an e-mail address? Should additional information be required?

66. What is the most cost-effective way to protect potentially sensitive data contained in State EAS Plans? The Commission seeks comment on specific aspects of State EAS Plan data that may implicate national security or that otherwise could present security concerns when aggregated into a single database. Are there any particular aspects of State EAS Plans that should be made confidential in light of this sensitivity? Would it be sufficient to provide such data with the same level of confidentiality as test data submitted to the Commission via ETRS? If not, how should sensitive SEPFI data be protected? Even if data contained in an individual State EAS Plan may not be sensitive or present national security concerns, would State EAS Plan data become more sensitive when aggregated via SEPFI? If so, what additional protections should be afforded to aggregated data versus individual state data, and how could this be

implemented? What costs, if any, would those additional protections impose on reporting entities?

67. National Advisory Committee (NAC). The NAC succeeded the Emergency Broadcast System Advisory Committee (EBSAC) as the Federal Advisory Committee responsible for assisting the Commission with administration of the EAS. CSRIC IV recommends that the Commission should reestablish a NAC to facilitate communication with SECCs. The Commission seeks comment on CSRIC IV's recommendation. Is there a need for additional and routine communication with another organization that is not already taking place today between the Commission and the SECCs? Could a reestablished NAC be charged with initial approval of State EAS Plans? Could they be charged with performing outreach to SECCs to answer any questions about the Commission's new State EAS Plan filing process, and encouraging the timely completion of up-to-date State EAS Plans? With what other responsibilities should the NAC be charged? Should membership in the NAC continue to consist of SECCs Chairs, and representatives from the National Association of Broadcasters (NAB), the Society of Broadcast Engineers (SBE) and the NWS? If not, then how should the membership of the NAC be modified?

### 3. State EAS Plan Contents

68. The Commission's EAS rules currently state that State EAS Plans must contain the following elements:

1) A list of the EAS header codes and messages that will be transmitted by key EAS sources;
2) Procedures for state emergency management and other state officials, NWS, and EAS Participant personnel to transmit emergency information to the public during an emergency using EAS;

3) A data table, in computer-readable form, clearly showing monitoring assignments and the specific primary and backup path for the EAN formatted in the EAS Protocol from the PEP to each station in the plan;

4) A description of how CAP-formatted messages will be aggregated and distributed to EAS Participants within the state, including the monitoring requirements associated with distributing such messages;

5) A statement of any unique methods of EAS message distribution;

6) Instructions for state and local activations of EAS, including a list of all authorized entities participating in State or Local Area EAS; and

7) Procedures for conducting special EAS tests.

The EAS rules require that EAS operations must be conducted as specified in State EAS Plans in order to ensure that the Presidential Alert can be effectively delivered. The Commission adopted these requirements in the EAS Deployment Order, communicating expectations for the structure and administration of State EAS Plans and for the SECCs that create them. SECCs and State EAS Plans have fallen short of these expectations in some respects, including a lack of active cable service provider participation in SECCs, and the failure of some states to file State EAS Plans.

69. In 2013, the Commission evaluated the state of SECCs and State EAS Plans in the EAS Nationwide Test Report, summarizing the successes of the first nationwide EAS test, but observing specific shortcomings in EAS operations, including a lack of clarity in State EAS Plans. Specifically, the EAS Nationwide Test Report observed that the Commission's rules do not require SECCs Participants to provide monitoring assignment data below the LP level. The EAS Nationwide Test Report further observed that many State EAS Plans did not identify the

alternative monitoring sources that EAS Participants relied upon to receive the EAN during the first nationwide EAS test, or define SECCs' administration and governance practices. Accordingly, the Bureau recommended that the Commission "consider reviewing its State EAS Plan rules." CSRIC IV further recommends that the role of the SECC should be strengthened, and that "SECCs must be free to design and maintain their respective state's own robust and redundant EAS relay networks in the best and most practical ways possible." The Commission seeks to address the substantive shortcomings in State EAS Plans identified by CSRIC IV and the EAS Nationwide Test Report.

70. Since the adoption of State EAS Plan rules in 1994, the alerting landscape has dramatically changed. Local alerts now originate from a wider array of sources, such as Public Safety Answering Points (PSAPs) and nuclear power plants. Local weather alerts continue to increase in frequency, and new alerting platforms such as WEA, SMS- and social media-based alerts are being rapidly added to the toolbox available to each community's alerting authority. For many alert initiators, WEA acts in concert with the EAS and other systems to transmit alerts to the public. Further, alert initiators may offer both EAS and WEA through IPAWS-OPEN, which serves as an interconnected CAP alert aggregator for previously siloed alerting platforms. In the EAS Nationwide Test Report, the Commission observed that many EAS Participants utilized the satellite-based National Public Radio (NPR) News Advisory Channel (Squawk Channel) to receive the Presidential Alert, as opposed to their regular monitoring assignment in the daisy chain. Even for state and local alerts, many EAS Participants use satellite-based distribution systems to supplement or replace the traditional alert distribution architecture. The Commission seeks comment on the extent to which these developments, as discussed in greater detail below, need to be included in State EAS Plans to provide the FCC with the information necessary for it to ensure that the EAS can allow the President to reach the entire American

public in time of national emergency.

71. The Commission proposes to amend Section 11.21 to integrate State EAS Plan requirements contained in other portions of Part 11, and to include new elements designed to enhance the value of State EAS Plans as community alerting tools, as well as to inform the Commission that the EAS remains an efficient and effective method to deliver a Presidential Alerts in an evolving technological landscape. The Commission proposes that State EAS Plans should include organizational, operational, testing/outreach, and security elements, as set forth below, and seeks comment on these proposals. While the Commission proposes to afford states considerable flexibility within these categories, to provide information they deem relevant to designing and maintaining their respective states' own robust and redundant EAS relay networks, the Commission believes these general categories will help establish a baseline level of information across states nationwide.

**a. Organizational Elements**

72. State EAS Plans and the SECCs that create them are designed to organize EAS Participants representing a variety of industries and regions into a cohesive whole capable of efficiently and reliably distributing emergency information to the public, including the Presidential Alert. In order to fulfill this purpose, SECCs and EAS Participants must be well organized. Accordingly, the Commission proposes that State EAS Plans filed with the Commission via SEPFI template include uniform designations for the roles of EAS Participants, a list of entities authorized to activate EAS, a description of SECC governance structure, and a clear role for Local Area EAS Plans, should they continue to be necessary.

73. Uniform Designations. The Commission proposes that SECCs input State EAS Plan monitoring assignment data into an online template using the uniform designations for key EAS sources that it proposes above. The Commission notes that in Section III(A)(1) it seeks comment on whether additional roles within the alert distribution hierarchy should be defined and given

designations in order to reflect their importance to the success of EAS. The Commission also seeks comment on whether any of these additional designations should be included in State EAS Plans.

74. A List of Entities Authorized to Activate EAS. The Commission proposes that State EAS Plans should contain a list of all entities authorized to activate EAS for state and local emergency messages (e.g., Public Safety Answering Points (PSAPs)) whose transmissions might be interrupted by a Presidential Alert. The Commission seeks comment on this proposal. The Commission notes that the Presidential Alert is required to take priority over all other alerts, and as such, might interrupt alerts initiated by any state-based entities. The Commission seeks comment on whether state and local alert originators would have reason to activate the EAS during a national crisis concurrent with a Presidential Alert. If so, is it reasonable to require that all entities authorized to activate the EAS should be included in State EAS Plans? Would such an inclusion ensure that SECCs are able to conduct outreach to these entities in order to organize and coordinate emergency managers' alert messaging should a Presidential Alert become likely, and to mitigate the potentially chaotic alerting situation that could result from a national crisis?

75. A Description of SECC Governance Structure. The Commission proposes that State EAS Plans should specify the SECC governance structure used to organize state and local resources to ensure the efficient and effective delivery of a Presidential Alert, including the duties of SECCs, the membership selection process utilized by the SECC, and the administrative structure of the SECCs. The Commission seeks comment on this proposal in light of the expectations expressed by the Commission in the EAS Deployment Order for the administration and governance of SECCs, and subsequent observations by the Bureau, CSRIC IV and EAS stakeholders that the Commission should provide further guidance on the issue. The Commission seeks comment on whether by soliciting information on SECC administration in State EAS

Plans, both in the form of comments in this docket and via the SEPFI, the Commission can develop a basis for analysis of SECC administration that it may leverage to produce best practices for SECC governance or otherwise offer guidance to these volunteer committees, as requested by CSRIC IV. Is there a need for a consistent, uniform governance structure for SECCs nationwide to ensure effective functioning of EAS? If so, what specific elements should such structure contain? Should the Bureau coordinate with SECCs to determine an optimal, uniform governance structure? The Commission acknowledges that CSRIC IV did not find that a "one size fits all" approach would work for SECC governance. Given the disparity of size and resources from state to state, is there guidance the Commission can issue that could clarify the roles and responsibilities of SECCs in a manner that would be useful in each state?

76. LECCs and Local Area EAS Plans. Finally, the Commission seeks comment on the role that LECCs continue to perform, and whether they serve a vital role in the delivery of EAS messages to local areas. The Commission seeks comment on whether LECCs perform a function that requires a separate Local Area EAS Plan to be filed with the Commission, or whether Local Area EAS Plans could be subsumed within State EAS Plans. CSRIC IV observes that "[a]ll federal emergency alert systems, of which EAS is an essential component, depend on local distribution" and recommends that policies be developed "that will encourage local communications distribution systems to participate in the emergency warning process." Consistent with that observation, the Commission seeks comment on whether SECCs currently have the expertise to describe and plan local alerting responsibilities. Do LECCs and Local Area EAS Plans provide an additional value not captured by SECCs and State EAS Plans? Does the size of some large states or the lack of SECC resources present challenges for comprehensive local planning? With SEPFI, information relevant to state and local plans will be filed in a single

system. Will there be a continued need for local plans, assuming the Commission moves forward with implementing SEPFI?

### b. Operational Elements

77. The primary purpose of EAS is to transmit a message from the President to the public during an emergency of national significance. In order to achieve that purpose, SECCs must maintain a detailed understanding of how multiple alerting platforms operate in concert with one another to create a seamless information distribution system within their respective states. Accordingly, the Commission proposes that State EAS Plans should include emergency alerting procedures for EAS alerts transmitted via all available alert distribution mechanisms that the state utilizes (e.g., EAS and WEA, as well as any alternative mechanisms the state may use, such as the NPR Squawk Channel, highway signs, and social media), up-to-date monitoring assignments for each key EAS source that reflect how those entities actually receive alerts, and a description of whether and to what extent these elements work in concert to create a cycle of information sharing through a "many-to-one/one-to-many" alerting dynamic.

78. Expanded Emergency Alerting Procedures. The Commission proposes that State EAS Plans should contain a comprehensive listing of procedures by which state emergency management officials, local NWS forecasting stations, and EAS Participant personnel transmit emergency information to the public during an emergency using regulated alerting tools (e.g., EAS and WEA) as well as any alternative alerting mechanisms (e.g., the NPR Squawk Channel, highway signs, and social media). The Commission proposes that this revised language would subsume the Section 11.21 language that State EAS Plans include a "statement of any unique methods of EAS message distribution such as the use of the Radio Broadcast Data System (RBDS)." The Commission seeks comment on this proposal. Would this proposed rule change allow SECCs to adequately capture the different alerting methods that EAS Participants may

leverage? Would it accurately reflect how emergency managers utilize the suite of alerting tools available to them?

79. In light of the monitoring assignments that EAS Participants used successfully during the first nationwide EAS test, and for the reasons provided below, the Commission proposes to encourage SECCs to specify a satellite-based source, such as the NPR Squawk Channel, in State EAS Plans as an alternate monitoring assignment for the Presidential Alert where it presents a reliable source of EAS messages. The Commission seeks comment on this approach. In the Second Report and Order, the Commission observed that "the vast coverage area of satellite signal footprints would allow immediate alerting of substantial portions of the country with appropriate equipment" and that satellite systems are "generally immune from natural disasters and therefore may provide critical redundancy in the event that terrestrial wireline or wireless infrastructure is compromised." CSRIC IV notes that many EAS Participants are currently unable to meet their requirement to monitor two sources for the Presidential Alert without recourse to such satellite-based communications technologies because of incomplete PEP coverage. NPR states that in instances where EAS Participants monitored both the Squawk Channel and their regular monitoring assignment, the Squawk Channel actually triggered EAS equipment ahead of the terrestrial relay network by 10-20 seconds in most cases. Does the NPR Squawk Channel provide a faster and equally reliable alternative to the daisy chain process? Do other satellite-based monitoring sources, such as EMnet? Are such technologies sufficiently reliable to serve as a primary or secondary EAS monitoring assignment for the Presidential Alert? If so, how should use of the Squawk Channel and other satellite-based communications resources approved by FEMA be codified in the Commission's EAS rules?

80. The Commission also seeks comment on whether and how alert originators use alternative alert distribution platforms, such as social media and highway signs, to supplement

their traditional alerting channels. What is the extent to which emergency managers at the federal, state, and local levels currently leverage targeted feedback during emergency situations to disseminate and gather information? The Commission seeks comment on the extent to which social media has served as a reliable and effective source of crowdsourced data about developing situations. To what extent have alert originators begun taking advantage of social media's crowdsourced communications functionality in order to establish a real-time conversation with individuals and communities in crisis? Is the information generated by social media platforms reliable enough to be trusted by emergency managers, and if not, what challenges are involved? The Commission seeks comment on the steps that emergency managers currently take to confirm the accuracy of crowdsourced reports of emergency situations in order to act on, correct or clarify, or otherwise respond to such reports. Are the platforms secure enough to be used in emergency situations? To what extent has the use of social media platforms supplemented alert accessibility, either by providing translations of alerts in languages other than English or by providing alerts in multiple formats? To what extent has the personalization of alerts facilitated and encouraged public engagement and participation with alerting platforms, and, in turn, instigated more rapid protective action taking? The Commission seeks comment on whether state and local use of social media alerting tools should be included in State EAS Plans. Further, the Commission seeks comment on the extent to which highway signs are used to retransmit EAS alerts formatted in CAP. If IPAWS-OPEN is capable of distributing CAP-formatted alerts to highway signs, do any barriers currently exist to such use? The Commission seeks comment on what, if any, other alternative alerting systems alert originators are relying upon to supplement their use of EAS and WEA, and seeks comment on its proposal that this information be specified in State EAS Plans.

81. Are there examples of best practices from the Commission's federal, state and local

government partners for using crowdsourced information in an emergency situation? The Commission observes that the Peta Jakarta initiative in Indonesia may provide an example of how a government alert initiator can leverage crowdsourced data to increase the overall effectiveness of alerts. The Peta Jakarta project piloted a program that monitored Twitter for posts mentioning the word for "flood" during flooding season. The system would automatically respond to such messages, asking whether the user saw flooding, at which point the user could confirm their report either by turning geo-location on in their device settings, or by responding, in turn, with the word for "flood." Peta Jakarta then incorporated the results of this information-gathering process into a live, public crisis map that depicted in real time areas in the city that were affected by flooding. To what extent would it be possible to leverage this model as a best practice for automated crowdsourcing of reliable emergency response data, using regulated alerting platforms in the United States? To what extent is a similar model to the one utilized by Peta Jakarta feasible using EAS and/or WEA, in order to provide an authoritative source of information? The Commission observes that emergency managers used Twitter in a 2013 flood in Boulder, Colorado to prioritize deployment of satellite- and drone-based imaging platforms to the most severely impacted areas. To what extent could community feedback via EAS or WEA be similarly used to prioritize emergency managers' information gathering efforts?

82. Monitoring Assignments. In this section, the Commission proposes rules and seeks comment on issues designed to optimize monitoring assignments in State EAS Plans. First, the Commission seeks comment on methods of improving and clarifying monitoring assignments as currently implemented in State EAS Plans. Specifically, the Commission seeks comment on how to define operational areas, on whether to include CAP-based monitoring assignments in State EAS Plans, and on how to remove single points of failure from EAS monitoring assignments. Next, the Commission proposes to expand the monitoring assignments section of

State EAS Plans to reflect more accurately the various methods that EAS Participants use to monitor sources for EAS. Specifically, the Commission proposes that State EAS Plans should include the extent to which monitoring assignments for state and local alerts differ from monitoring assignments for the Presidential Alert. Finally, the Commission proposes to clarify that EAS operations must be implemented in a manner consistent with guidelines established in a State EAS Plan submitted to the Commission.

83. The Commission proposes that State EAS Plans should continue to divide their respective states into geographically-based operational areas, specifying primary and backup monitoring assignments for EAS Participants to receive the Presidential Alert in each operational area. The Commission seeks comment on this proposal. The Commission seeks comment on whether dividing states into operational areas facilitates EAS administration by more clearly defining responsibilities for EAS alert distribution by geographic area for key EAS sources. CSRIC IV notes a lack of uniformity among State EAS Plan definitions of "operational areas," and recommends that such service areas should be uniformly identified. The Commission seeks comment on CSRIC IV's conclusion. Is it possible to standardize the definition of an operational area nationwide? If so, how should SEPFI define operational areas? Could the definition of an operational area have implications for President's ability to transmit a regional Presidential Alert?

84. The Commission proposes to remove the current restriction that State EAS Plans include monitoring assignments for Presidential Alerts formatted in the EAS Protocol only. The Commission seeks comment on this proposed change. As technologies evolve, the Presidential Alert may not necessarily be issued using the EAS Protocol, and the Commission seeks to remain technologically neutral so that its rules may evolve correspondingly. The Commission seeks comment on the extent to which EAS Participants are prepared to receive a Presidential

Alert formatted in CAP. The Commission observes that new alerting protocols may be developed in the future, and the Commission seeks comment on whether removing this technology-specific limitation from its rules better prepares the nation for receiving the Presidential Alert.

85. CSRIC IV observes that, as currently written, State EAS Plans reflect the requirement in the EAS rules that each EAS Participant monitor at least two sources for the Presidential Alert by including two monitoring assignments for the Presidential Alert, but also observes that merely listing two monitoring sources may not serve to remove single points of failure from EAS alert distribution where, for example, both monitored EAS sources, in turn, monitor the same source. The Commission agrees with CSRIC IV's observation and seeks comment on whether it should require that the two sources that EAS Participants are required to monitor for the Presidential Alert as specified in their State EAS Plan, cannot, in turn, monitor the same key EAS source. Are there further steps that the Commission can take to remove single points of failure within the EAS Protocol-based alert distribution architecture, and from EAS in general, and if so, what are they?

86. The Commission further proposes that State EAS Plans should include the extent to which monitoring assignments for state and local alerts differ from monitoring assignments for the Presidential Alert. To what extent do states' Presidential and local alerting strategies differ? The Commission seeks comment on whether the importance of transmitting state and local alerts to communities has had any impact on the ability of the community to deliver a Presidential Alert. Has the use of alternative alerting structures led to innovations that augment the ability of EAS Participants to efficiently and effectively receive and retransmit a Presidential Alert during a national crisis? Alternatively, has the use of such alternatives resulted in lack of use of the EAS and lack of proficiency in its use by local emergency managers and EAS Participants? In

either case, would including in State EAS Plans a description of the extent to which a state's alerting strategy for the Presidential Alert differs from their state and local alerting strategy serve to facilitate dialogue at the state and local level about the extent to which new and emerging technologies could be used to improve the ability of EAS Participants to receive and retransmit the Presidential Alert?

87. In order to address all State EAS Plan monitoring requirements in the same Section of Part 11, the Commission proposes to relocate State EAS Plan requirements currently contained in Sections 11.52 and 11.55 to Section 11.21. The Commission proposes to merge those requirements into one Section by amending Section 11.21 to state that EAS Participant monitoring assignments and EAS operations must be implemented in a manner consistent with guidelines established in a State EAS Plan submitted to the Commission, and by removing that language from Sections 11.52 and 11.55. The Commission seeks comment on whether this proposal is consistent with CSRIC IV's recommendation that the Commission amend Section 11.21 to state that "[s]tates that want to use the EAS shall submit a State EAS Plan." The Commission seeks comment on whether the data submitted in State EAS Plans must accurately reflect actual monitoring assignments for the EAS Mapbook to be a useful tool to analyze and address issues with EAS functionality. Would State EAS Plans be more up-to-date, inclusive, and effective given the improvements the Commission proposes in this NPRM? If so, does this militate for the use of State EAS Plan provisions other than monitoring assignments (e.g., expanded emergency alerting and testing procedures) as mandatory instructions for participation in EAS? The Commission seeks comment on whether, contrarily, failing to require EAS Participant monitoring assignments to be implemented pursuant to State EAS Plans would risk making the state EAS planning process a hollow exercise without bearing on the actual organization of EAS.

88. A Description of "One-to-Many, Many-to-One" Alerting Implementation. The Commission proposes that State EAS Plans should describe the extent to which alert originators coordinate alerts with community feedback mechanisms, such as 9-1-1, to make full use of public safety resources. The Commission seeks comment whether 9-1-1 call takers are well positioned as a nexus of communications between first responders and communities in crisis. The Commission seeks further comment on whether, notwithstanding that this has been true in the context of state and local emergencies, it would also be the case during a national crisis giving rise to a Presidential Alert. The Commission seeks comment on the extent to which alert originators are prepared to gather, analyze and act upon community feedback in crafting and initiating alert content. Relatedly, the Commission seeks comment on the extent to which first responder entities, such as PSAPs, are currently authorized as alert originators, and, if desirable, on the steps that the Commission can take to facilitate increased participation. Can PSAPs play an important role in ensuring that alerts are accessible or available in languages other than English if the 9-1-1 call(s) giving rise to the alert suggest that such measures could facilitate alert interpretation and impact? Finally, the Commission seeks comment on the impact that any potential next generation television capabilities may have on the ability to support two-way communications.

### c. Testing/Outreach Elements

89. In order to properly utilize EAS to fulfill its purpose to transmit a Presidential Alert, emergency managers must be assured that the alerting platforms available to them will function as intended when needed, and the public must be assured that those alerts will be made accessible to them, irrespective of disability or language preference. To this end, the Commission proposes that State EAS Plans include testing procedures and security elements.

90. Testing Procedures. The Commission proposes that State EAS Plans should continue

to contain procedures for special EAS tests, as required by Section 11.61, including the new "live code" tests that the Commission proposes to include as part of its Part 11 testing regime below. The Commission also proposes that State EAS Plans should be required to include procedures for Required Monthly Tests (RMTs), Required Weekly Tests (RWTs) and national tests designed to ensure that the system will function as designed when needed for a Presidential Alert. The Commission seeks comment on this proposal. The Commission seeks comment on whether specifying the schedule, origination source, and script are necessary components of the successful operation of RMTs, RWTs, and national tests, and on whether SECCs already communicate this information to EAS Participants in their state even where it is not included in State EAS Plans. Further, the Commission proposes that this section of State EAS Plans should include a description of the extent to which State/Local WEA Tests are utilized by alert originators as a complement to the Presidential Alert distribution system to verify that WEA is both capable of disseminating a Presidential Alert, and informing the public that a Presidential Alert is presently being delivered over EAS. The Commission seeks comment on these proposals.

91. The Commission seeks comment on whether State EAS Plans should include a listing of the manners in which a state or community conducts such live code tests. Should the Plan include the language of the notification to be provided during the test (e.g., audio voiceovers, video crawls) to make sure the public understands that the test is not, in fact, a warning about an actual emergency? The Commission also seeks comment on whether the notification requirement should incorporate the new accessibility component of Section 11.51 of the Commission's EAS rules, which establishes requirements for the visual message portion of an alert. Should the Plan contain pre-test outreach procedures to coordinate with EAS Participants, state and local emergency authorities, and first responder organizations and the public?

92. The Commission seeks comment on whether each of these testing procedures continues to play an important role in ensuring system readiness for a Presidential Alert. In particular, with respect to State/Local WEA Testing, the Commission seeks comment on whether the ubiquity of smartphone technology makes it likely that, in the event of a Presidential Alert, members of the public would likely have their smartphone closer at hand than any traditional EAS source. If so, the Commission seeks comment on whether it is likely that the first medium through which members of the public would receive notice that a Presidential Alert is occurring is through their smartphone, notwithstanding the fact that the actual alert may be aired over EAS. The Commission seeks comment on whether this makes State/Local WEA Testing procedures a necessary component of state-level preparedness to receive a Presidential Alert. If so, should the manner in which a state or community uses smartphone technology, through WEA or otherwise, to augment an EAS alert be included in State EAS Plans?

**d. Security Elements**

93. Security and reliability are critical components of an alerting system, especially one that may be used by the President. A public safety communications system that is vulnerable to mistaken use or malicious intrusion poses as much of a threat to public safety as an efficient, secure system offers a benefit. A compromised alerting system could be used to misdirect public safety resources, or lead members of the public into harm's way. Accordingly, the Commission proposes to require certification of performance of required security measures, as discussed in greater detail below. Should State EAS Plans also describe the measures EAS Participants have taken to comply with the Commission's proposed security requirements? Should State EAS Plans include any additional information regarding their approach to cyber risk management, including if and how they use tools like the National Institute for Standards and Technology (NIST) Cybersecurity Framework (NSF), or other risk management construct, and how this has

been extended to their emergency alerting system? In the alternative, do the certifications proposed below provide adequate disclosures regarding EAS Participants' security efforts, obviating the need for the separate inclusion of such information in State EAS Plans?

### B. Building Effective Community-based Alerting Exercise Programs

#### 1. Live Code Tests

94. Section 11.45 of the Commission's EAS rules provides in pertinent part that "[n]o person may transmit or cause to transmit the EAS codes or Attention Signal, or a recording or simulation thereof, in any circumstance other than in an actual National, State or Local Area emergency or authorized test of the EAS." The Commission adopted this restriction because it found that a specific prohibition against the misuse of the EAS audio Attention Signal and codes was necessary in light of the "enormous detriment to the system" that might result from improper use. As a general matter, the EAS audio Attention Signal is used exclusively to alert the public that an emergency message is about to be distributed. Section 11.31(e) lists the "live" event header codes that are used for alerts in specific emergency situations, e.g., tornadoes, tsunamis, and other natural and weather-related emergencies, as well as the specific test codes that are to be used for national periodic, required monthly and required weekly tests, as well as for practice/demonstration warnings. In the Live Code Testing Public Notice, the Bureau noted that EAS Participants have expressed a desire to use live EAS header codes and the EAS audio Attention Signal to conduct local public awareness and proficiency training EAS exercises, and stated that engaging in such activity would require a waiver of Section 11.31(c) of the Commission's EAS rules. The Bureau also provided the following guidance to SECCs on the recommended contents of their waiver requests:

> 1) A description of the test and test participants, including when the test is scheduled to occur, when it will conclude, and what notification is

being provided during the test (e.g., audio voiceovers, video crawls) to make sure the public understands that the test is not, in fact, warning about an actual emergency, plus a statement whether the proposed test is designed to substitute for a "RWT" (required weekly test) or a "RMT" (required monthly test) or would constitute a "special test," pursuant to 47 CFR 11.61;

2) An explanation why the EAS Participant or the state authority conducting such tests has concluded that use of live codes is necessary; e.g., what live code testing is expected to achieve that could not be achieved by using standard test codes;

3) A statement about how the test has been coordinated among EAS Participants and with state and local emergency authorities, as well as first responder organizations such as police and fire agencies; and

4) A description of those public information steps that have been taken before the test occurs to notify the public about the test (specifically, that live event codes will be used, but that no emergency is in fact occurring). This should include a statement about all media that have participated in the public awareness/information campaign (e.g., broadcasters, cable, print media, etc.).

Live code tests are currently performed as "special" tests under Section 11.61. A "special" test may fulfill an EAS Participant's weekly testing obligation provided that the test includes transmission of the EAS header codes and End of Message (EOM) codes, and may fulfill an EAS Participant's monthly testing obligation provided that the test also includes the emergency alerting Attention Signal and emergency message. In either case, the test message must meet a minimum standard of accessibility, as discussed in further detail below.

95. The Commission proposes to amend its EAS rules to authorize EAS Participants to conduct periodic EAS exercises using live event header codes, provided that they are used in a non-misleading manner, and that steps are taken to prevent public confusion prior to and during the test. Specifically, the Commission proposes to amend Section 11.61 to include "Live Code Tests" as a separate category of alerting exercise that may be undertaken periodically provided that:

1) The state or local entity provides accessible notification during the test (e.g., audio voiceovers, video crawls) to make sure the public understands that the test is not, in fact, warning about an actual emergency;

2) Coordinates the test among EAS Participants and with state and local emergency authorities, as well as first responder organizations such as Public Safety Answering Points (PSAPs), police and fire agencies; and

3) Notifies the public before the test (specifically, that live event codes will be used, but that no emergency is in fact occurring).

The Commission further proposes to amend Section 11.45 to exempt state-designed EAS live code exercises from the Commission's prohibition against false or misleading use of the EAS Attention Signal. The Commission seeks comment on these proposals.

96. Benefits. Would expanding the Commission's Part 11 rules to permit live code testing facilitate opportunities for system verification, proficiency building, and raising public awareness about EAS? The Commission seeks comment on whether, as certain SECCs claim, using a live code enables more realistic system verification because use of a live code is the only way to determine how EAS equipment will react to certain live event header codes that are not activated by default in EAS equipment. Further, the Commission seeks comment on whether live code testing promotes alert originator proficiency by providing an opportunity for alert

originators to practice selecting an appropriate event code for simulated emergency events, and practice crafting a message that informs the public of the occurrence of that specific event that would effectively motivate the public to take protective action. The Commission also seeks comment on whether live code testing facilitates opportunities for EAS stakeholders to raise public awareness about EAS. Some SECCs requesting a live code waiver state that their live code testing will coincide with "Severe Weather Preparedness Week" scheduled in their state, and the live code presents a visual crawl that is distinct from the visual crawl associated with test messages that better facilitates schools' businesses' and homeowners' own emergency preparedness drills. The Commission seeks comment on this claim. Finally, the Commission seeks comment on the extent to which live code testing offers superior public awareness and proficiency training opportunities than RMT and RWTs because they present testing conditions that more accurately reflect actual emergency conditions.

97. Notification and Outreach. The Commission seeks comment regarding the steps that EAS stakeholders could take to minimize any public confusion that may result from live code testing. The Commission seeks comment on the methods used by EAS Participants to inform the public that the Attention Signal they hear does not indicate an actual emergency. Is it necessary to codify specific notification procedures, or are available best practices sufficient? The Commission seeks comment on the extent to which outreach to first responder agencies has mitigated public confusion about the use of live codes. How can first responder organizations, such as PSAPs, be utilized as an integral part of an alerting exercise in a manner that harnesses their potential as a nexus for emergency information? The Commission seeks comment on whether the Commission's proposed rule adequately circumscribes the use of the emergency alerting attention signal in a manner that maximizes its utility while minimizing over-alerting and public confusion.

98. Frequency of Live Code Testing. How often should live code testing occur? The Commission observes that some EAS stakeholders have requested a waiver of the Commission's EAS rules to conduct live code tests as often as annually. The Commission seeks comment on whether the removal of this regulatory burden would lead EAS stakeholders to engage in more frequent live code testing. If so, the Commission seeks comment on whether it should limit how often live code tests may occur in a particular geographic area, and, if so, on what that limit should be. The Commission observes that its EAS rules currently allow special tests to be conducted as often as daily. Are there steps that the Commission should take to prevent over-alerting and alert fatigue? On the other hand, should SECCs be required to conduct live code EAS tests at certain predetermined intervals in order to ensure that emergency managers in each state have opportunities for system verification, proficiency training, and public awareness outreach?

99. Cost Savings. Would this action remove regulatory burdens for EAS stakeholders and reduce costs? The Commission seeks comment on the anticipated extent of these cost savings. The Commission also seeks comment on any operational concerns that EAS stakeholders believe to be implicated by this proposal.

### 2. EAS PSAs

100. EAS Participants may use Public Service Announcements or obtain commercial sponsors for announcements, infomercials, or programs explaining the EAS to the public to increase awareness of the EAS. The Commission's rules state that "[s]uch announcements and programs may not be a part of alerts or tests, and may not simulate or attempt to copy alert tones or codes." Since that time, the Commission has granted requests for waiver to use the emergency alerting Attention Signal in PSAs to entities other than EAS Participants in order to raise public awareness about EAS. The Commission has also granted similar requests from

FEMA to use the emergency alerting Attention Signal in WEA PSAs provided that the PSA presents the tones in a non-misleading manner. In light of the value of the success of these PSAs, in the WEA Fourth NPRM, the Commission proposed to allow the use of the WEA Attention Signal in WEA PSAs, subject to the same limitation.

101. Consistent with the Commission's approach to the use of the emergency alerting attention signal in PSAs in the WEA Fourth NPRM, the Commission proposes to amend Section 11.46, which currently prohibits the use of the EAS alert tones or codes in otherwise permitted PSAs, to allow federal, state and local government entities to issue PSAs that use the EAS header codes and Attention Signal, provided that they are presented in a non-misleading and technically harmless manner. In so doing, the Commission allows entities other than EAS Participants to conduct EAS PSAs, and allow such PSAs to be used in connection with testing exercises that may include use of live event codes and the emergency alerting Attention Signal. The Commission seeks comment on these proposals. The Commission seeks comment on whether limiting the use of PSAs to EAS Participants and federal, state, and local government entities offer an optimal balance between ensuring that the emergency alerting Attention Signal is not over-used, on the one hand, and ensuring that the public is familiar with the EAS and understands its public benefits on the other hand? The Commission seeks comment on whether this is the appropriate subset of entities who should be able to use the emergency alerting Attention Signal in PSAs.

102. How can the Commission ensure that PSAs designed to raise public awareness about EAS do not have the unintended consequence of causing public confusion about whether the use of the EAS header codes and Attention Signal signify that an actual emergency is occurring? The Commission seeks comment on whether it should require entities that wish to use PSAs to coordinate with other EAS Participants and state and local authorities and the public

to minimize any confusion. As with the use of the EAS header codes and Attention Signal for live code EAS tests, should entities seeking to use the EAS header codes and Attention Signal for EAS PSAs provide notification during the PSA to make sure the public understands that the use of the EAS header codes and Attention Signal does not, in fact, signify the occurrence of an actual emergency? Should entities seeking to use the EAS header codes and Attention Signal for use in EAS PSAs be required to coordinate the test among EAS Participants and with state and local emergency authorities, as well as first responder organizations such as PSAPs, police and fire agencies?

103. The Commission seeks comment on whether there is a negative public perception of EAS that deserves to be redressed, and on whether the public has a clear understanding of what EAS is. In its requests for waiver, FEMA stated that "many people are startled or annoyed when hearing the WEA Attention Signal for the first time." The Commission notes that the WEA Attention Signal is a loud, attention-grabbing, two-tone audio signal that uses frequencies and sounds identical to the distinctive and familiar Attention Signal used by the EAS. The Commission seeks comment on whether alerts become more annoying when multiple alerts are received at the same time on a variety of platforms. The Commission also notes that it has received a number of complaints from individuals stating that the EAS Attention Signal is intrusive, and annoying. Accordingly, the Commission seeks comment on the public perception of EAS, and the EAS Attention Signal. To this point, the Commission also seeks comment on whether PSAs would be a useful tool for changing public perceptions about EAS for the better by, for example, providing them with information on how EAS saves lives and helps people to protect their property. As a testament to the success of the WEA PSA in this regard, FEMA offers that it has earned over $30 million in free media, and that the WEA PSA is currently the most played FEMA PSA. The Commission seeks comment on the success of any EAS PSAs

that EAS Participants have issued pursuant to Section 11.46. Further, the Commission seeks comment on additional steps that EAS stakeholders could take to improve the efficacy of EAS PSAs at raising public awareness about, and shifting public perceptions of EAS. What effect on public perception would likely result were EAS PSAs allowed to be conducted in connection with EAS tests, including live code tests?

### 3. Accessible Alerting Exercise

104. Accessibility is a crucial aspect of alerting exercises because members of communities with disabilities or with limited English proficiency are particularly vulnerable to being excluded from community preparedness initiatives. Accordingly, in order to substitute for an RMT, a live code test must "comply with the visual message requirements in Section 11.51," and in order to substitute for an RWT, it must comply with both the aural and visual requirements contained therein. Recently, the Bureau granted a request from Emergency and Community Health Outreach (ECHO), in partnership with Twin Cities Public Television (tpt) and FEMA, for a waiver of the Commission's rules to allow use of the WEA and EAS attention signal, as well as an audible portion of the EAS tones in PSAs, in conjunction with providing EAS PSAs in languages other than English, including Spanish, Hmong and Somali. The Bureau reasoned that including the EAS Attention Signal in educational media materials is essential to ensure that members of the public, including individuals with limited English proficiency, are familiar with EAS as an alert and warning methods.

105. The Commission seeks comment on how to best ensure that community-based alerting exercises address the accessibility needs of individuals with limited English proficiency and individuals with disabilities. Specifically, the Commission seeks comment on the extent to which live code testing may be used by local emergency managers to target the particular needs of communities with accessibility needs, such as individuals with sensory disabilities and

individuals with limited English proficiency, and on how to better prepare such communities for emergencies through PSAs.

106. Accessible Live Code Testing. Is an accessible video crawl or full-screen replacement slide sufficient to overcome the public's preconception of the meaning of the Attention Signal? Are there additional steps that the Commission should take to ensure that the public is not misled or confused by state use of live codes for testing purposes? For example, might persons with cognitive or intellectual disabilities benefit from color-coding a border around different categories of warning, such as weather, terrorism, or earthquake? What technical and operational issues might be implicated by such an approach? The Commission observes that many entities requesting waiver of the Commission's Part 11 rules in order to conduct a live code test do so because of their concern that a "test" code might not be relayed through law enforcement communication, thus weakening the designation of a "statewide exercise." In this way, does live code testing facilitate the transmission of EAS tests over a larger variety of media, and therefore improve their accessibility?

107. Further, the Commission observes that live code testing often does not occur in a vacuum, and is requested to supplement larger efforts to raise public awareness of emergency response resources, such as during a "Severe Weather Preparedness Week." Does live code testing promote and facilitate such community engagement? Do such events provide opportunities for those that might not normally be able to access the emergency alerting attention signal to create community response mechanisms that ensure that some community members, such as those who do not speak English or those with disabilities, are not left behind during an emergency? What role should community stakeholders, including those who deliver alerts as well as those who benefit from the receipt of alerts, play in the design, execution, and subsequent evaluation of live code tests and subsequent alerts? How can the Commission work with public

safety officials, SECCs, EAS Participants and other stakeholders to facilitate the inclusion of the entire community, including non-English speakers and those with disabilities, in such planning, execution and evaluation? Would the Commission's proposed testing rules provide transparency and allow collection of best practices results that would enhance this facilitation role? How should broadcasters and other EAS Participants, as well as PSAPs and emergency managers that coordinate live code tests, be equipped with the tools necessary to serve multilingual communities and communities of individuals with disabilities? Could tests be designed to allow broadcasters and other EAS Participants to share resources during an emergency, such as non-English speaking personnel and air time, to ensure that non-English speakers maintain access to EAS and emergency information?

108. How, if at all, should the Commission conduct outreach and gather feedback on the ability of public safety officials, SECCs, EAS Participants and other stakeholders to plan and execute community tests and exercises to reach populations with limited English proficiency and individuals with disabilities? How should the Commission evaluate the results? What steps, if any, should the Commission take in response to any such information it may collect? For example, should the Bureau conduct outreach to EAS Participants and other stakeholders in particular regions that have non-English speaking communities to gather information about best practices for ensuring alerts reach non-English speaking communities? What accountability measures should be instituted or encouraged if the tests fail to reach citizens due to their lack of English proficiency or disability?

109. Accessible PSAs. The Commission seeks comment on whether EAS PSAs in languages other than English are particularly effective at informing individuals who would otherwise not be able to understand the contents of an English-language EAS message about how to respond should they hear the common alerting Attention Signal. The Commission notes that

notwithstanding the ubiquity of the EAS and its familiar audible signal, the tpt/ECHO waiver request indicates that at least one population, i.e., recently arrived individuals with limited English proficiency, was not familiar with the EAS Attention Signal, and needed the PSAs to become familiar with these sounds and their meaning. Are there other groups or individuals for which EAS PSAs would provide this value? Would it be helpful if EAS PSAs were made available in American Sign Language (ASL) in order to better meet the needs of certain individuals with hearing loss? To what extent can PSAs transmitted over the Internet, including via OTT services, offer enhanced utility and accessibility to the public, as well as to individuals with disabilities?

### C. Leveraging Technological Advancements in Alerting

110. In this section, the Commission seeks comment on the extent to which the communications infrastructure underlying the nation's alerting capability should be – and already is – taking steps to leverage technological advancements to improve the content, accessibility and security of emergency alerts. In addressing these issues, the Commission intends to initiate a dialogue about creating a voluntary industry roadmap for further enhancing the capability of the nation's alerting infrastructure to carry a Presidential Alert in a manner consistent with consumer expectations of IP-based communications technologies.

#### 1. Cable Force Tuning and Selective Override

111. The EAS "force tuning" provisions allow wireless and digital cable service providers and wireline video service providers to satisfy the general requirement that they transmit EAS audio and visual information over all channels by automatically tuning the subscribers' set top boxes (STB) to a designated channel (usually an otherwise empty control channel) that carries the required audio and video EAS message. The Commission's "selective override" provisions allow cable service providers to elect not to deliver EAS audio and visual

information over channels that are carrying news or weather related emergency information with state and local EAS message. Such elections are made pursuant to a written agreement between the cable service provider and broadcaster. Use of selective override by the cable service provider is voluntary.

112. The Commission has received requests that it reexamine the selective override policy. Most recently, for example, the NAB requested that the Commission "permit local television stations to opt out of cable system-wide overrides, provided such stations participate in the EAS system." NAB contends that cable overrides "disrupt viewers' access to the critical, often life-saving emergency information provided by local television broadcasters, including shelter-in-place or evacuation directions, storm pathways, and the status of power outages . . . [and] frequently cause confusion and distress among viewers." NAB proposes that cable operators be required to "implement 'selective override,' so that certain [broadcast] channels can be selectively omitted during a cable system's EAS interruption," thus providing local broadcast television stations with the ability to opt out of the cable system's universal forced-tuning of all cable channels, enabling the station to offer uninterrupted emergency information.

113. The Commission is also aware of reported instances where force tuning STBs has caused the subscriber's picture and audio to freeze, sometimes requiring a reboot of the STBs to restore normal access to channels. Viewers have claimed that during the period when the force tuned alert was active, they were unable to change channels and were stuck on the force-tuned EAS channel for extended periods of time. For example, on March 30, 2015, an in-house test conducted by a cable service provider was inadvertently distributed beyond the cable provider's test environment equipment to cable subscribers across several states, force-tuning most, if not all of them to a control channel where they were denied access to programming for approximately ten minutes. Commission staff has learned that over two million STBs likely

were affected in that one example alone.

114. The Commission seeks comment on the propriety of its selective override and forced tuning rules in an evolving alerting landscape. Specifically, the Commission seeks comment on whether its existing cable force tuning and selective override provisions continue to serve the public interest, and whether technological advancements should impact that analysis. The Commission seeks comment on the extent to which alerting functions incorporate (or are being modified to incorporate) advanced technology, in order to improve functionality and better support the conveyance of emergency information. Finally, the Commission seeks comment on technical issues that may suggest that forced tuning has an unacceptably negative impact on consumers viewing force tuned broadcast and cable channels.

115. Impact of Technological Advancements. In light of technological advancements or other factors that may impact cable operators' capacity to implement selective override, should selective override remain an acceptable voluntary EAS alternative for cable systems, or should all cable system providers refrain from interrupting local broadcast programming where the broadcast provider is participating in the EAS system and thus transmitting state and local EAS alerts? Alternatively, are there reasons why smaller cable systems (e.g., those serving fewer than 5,000 subscribers), would need the selective override option, in contrast to the larger systems, and would a regime that maintained the option for smaller cable systems only – while larger systems uniformly delivered broadcast-originated state and local EAS alerts, news or weather-related emergency information – make sense? If smaller cable providers need this exception, should it be permanent? If not, for how much time should smaller cable systems fit into an excepted category?

116. Have technological advancements enabled cable operators' ability to selectively override broadcast signals? For example, cable services now benefit from the introduction of

digital technologies, including "smart" STBs. How do these and related technologies affect the use of selective override? Have STB and headend technologies advanced to the point where selective override on a channel-by-channel basis can be readily programmed into cable equipment, without imposing undue burdens on cable providers? Is it reasonable to assume that all content delivered by STB shall be interruptible, such that EAS warnings could be delivered in banner form or otherwise for all content (without directing the subscriber to another channel through force tuning or by other means)? Have technological advances in EAS equipment made it easier and more affordable to engage in selective override? The Commission notes in this regard that some parties maintain that force tuning via the STB is not the only way that MVPD EAS Participants can display EAS information.

117. Does the widespread and growing availability of programming distributed by IP-based networks, including STBs and "smart" TVs capable of "on-screen" graphical user interface (GUI) user input, suggest that greater user control with respect to EAS acknowledgement and/or feedback should be supported or encouraged? Do the Commission's current cable force tuning and selective override requirements affect emergency operators' ability to leverage these technological advancements to rapidly and efficiently obtain feedback from consumers, in response to EAS messages? What regulatory obstacles exist that might unnecessarily impede greater consumer interaction with received alerting messages? Would facilitating this interaction introduce the capability for crowdsourced citizen feedback during emergencies and disasters that would improve community, state and national response? What possible consequences or potential for abuse, if any, would need to be addressed in harnessing this capability?

118. Delivery of EAS Messages through Different Platforms. Looking only at the content of the EAS messages transmitted through the EAS system, are there or can there be any

differences between the EAS messages that consumers see when viewing the alert on their local broadcast channel as compared to the EAS alert transmitted by a cable system provider? Are those EAS messages always identical in a given geographic area regardless of whether it is transmitted over the air or through a cable provider's system? Should they be identical? Specifically, has the implementation of Common Alert Protocol (CAP)-based alerting made it more likely that cable providers can relay more detailed EAS alert information (e.g., based upon the enhanced text in a CAP message) than what has been possible in the past or via the traditional broadcast-based EAS architecture? If so, have cable providers been originating EAS messages that have a greater emergency response value when using the force tuning option? Is there a significant difference in the accessibility of alerts offered by broadcasters and cable providers? To what extent, if at all, do cable franchise agreement provisions govern whether cable operators may participate in selective override where local broadcast providers are delivering state and local EAS alerts, news or weather-related emergency information? How should any differences in the actual EAS messages impact the Commission's analysis of the force tuning and selective override issues? Does the variation stemming from selective override complicate response from community emergency managers?

119. Technical Issues. Can STB technology advancements significantly reduce the risk that force tuning will cause the picture and/or audio to freeze, or lock out consumers from changing back to the channels they were watching? Are there any changes to the manner in which force tuning is implemented that could ensure that subscribers are not locked on the designated EAS channel? More broadly, are there steps or precautions cable service providers could take to prevent such events in the future? In light of technological advancements, does any public interest benefit remain by allowing cable service providers to satisfy their requirements to transmit EAS audio and visual information by force tuning? If not, would the immediate ("flash

cut") elimination of the force tuning option create any avoidable or unnecessary hardships, and, if so, would a sunset period for force tuning provide any relief?

### 2. EAS on Programmed Channels

120. As discussed above, the Part 11 EAS rules allow wireless and digital cable provider EAS Participants to comply with their obligations to deliver EAS messages by force tuning viewers to a channel that carries the alert or test. The rules limit the obligation of a cable EAS Participant to deliver EAS to "programmed channels," which, under the current rules do not include "channels used for the transmission of data such as interactive games," "channels used for the transmission of data services such as Internet," or "channels used for the transmission of data services such as Internet access."

121. The Commission initially seeks comment on what basis exists today, when technical advances have expanded the scope of programming and other services delivered by cable and other MVPD EAS Participants, to distinguish channels as "programmed channels" for purposes of receiving EAS messages. Is there a technical basis to continuing the distinction among channels? If so, is there some other basis that would be more suitable for making this distinction? For example, should the distinction be based on channels that are made available for consumer use versus channels not for consumer use and/or not part of the services that EAS Participants offer their customers? Channels not for consumer use would include diagnostic channels used to monitor the health and quality of the system, those used to transfer and manipulate metadata necessary to create the user interface (e.g., the program guide), or those used to deliver broadband access. Would it serve the public interest to require EAS Participants to support EAS alerts on all channels over which they offer services to the consumer? Is there a reason to exempt any such channels from the Commission's EAS rules?

122. The Commission also seeks comment on the public safety benefits that could be

derived from requiring that EAS Participants support EAS alerts over all channels that are part of the service package offered to the consumer. To what extent would requiring support for EAS alerts on all such channels increase the likelihood that the public will receive potentially life-saving alerts? To what extent might such channels offer opportunities to improve alert quality or accessibility? Further, what additional costs, if any, would EAS Participants expect to result from requiring EAS alerts to be supported on all channels that are part of the service package offered to the consumer by the EAS Participant? Would this approach fully address National Security and community alerting needs in the evolved technology landscape for typical residential consumers? Would this approach require hardware and/or software replacement? What standards, if any, would be affected by these proposed changes? How long should the Commission expect that it would take industry to comply with this alternative approach?

### 3. EAS Alerting and Emerging Video Technology

123. The Commission has consistently striven to ensure that, as technologies evolve, EAS continues to meet consumer expectations for basic emergency communications. For example, in preparation for the transition to digital television, Commission staff held a series of ex parte meetings with affected industry segments to ensure that the EAS would continue uninterrupted throughout the HD transition. As a result, when the Commission ultimately adopted the rules that included wireline video providers among EAS Participants, the record reflected almost unanimous support for the new rules. Now, emerging technologies are changing the EAS landscape again. A wealth of video content is now available to consumers online. For instance, Multichannel Video Programming Distributors (MVPDs) are beginning to offer IP-based versions of their programming, including providing consumers with apps to view content. Broadcast television is exploring IP-based offerings as well. A number of other entities are also entering the video space. Accordingly, in this section the Commission seeks to initiate a

conversation regarding how the EAS may remain durable as the ways in which consumers view content evolves.

124. In order to implement the Commission's statutory obligations in a manner consistent with the public interest, the Commission seeks to understand whether and how the way in which consumers view content has changed consumer expectations for how they will receive EAS messages. In this regard, the Commission seeks to ensure that EAS alerts endure and remain reliable as technology advances. The Commission seeks comment on the extent to which entities offering content outside of traditional broadcast or pay TV modes of architecture are making EAS alerts available to consumers. From a technical perspective, what hardware, software, and standards updates would need to be addressed before alerts could be delivered via alternative means, such as via IP-based platforms? Are the potential issues with offering alerts outside traditional broadcast or pay TV delivery mechanisms? What kind of strategies could be employed to standardize the availability of alerts across technologies, applications, and platforms? To what extent are these efforts already underway?

125. The Commission further seeks comment on whether consumers have an expectation that alerts will be durable across different technology platforms. Do consumers expect that the alerts provided with programming offered via traditional technologies would still be provided when programming is offered through some other means, such as through an online offering? To the extent that commenters believe the Commission should take action to address consumer expectations with respect to receiving EAS alerts through new technologies, on what statutory basis would the Commission take such action? Commenters should also address any possible unintended consequences of Commission action.

126. The Commission seeks comment on whether EAS alerts offered through different technologies may have a greater potential to meet the emergency information needs of the public

than do alerts offered via traditional media. What, if any, potential do these services have to improve EAS geo-targeting, for example, by using a devices' geolocation technology when the consumer is viewing content over the Internet? The Commission seeks comment on this assertion. Could alerts via non-traditional platforms offer consumers greater personalization options? For example, could consumers elect to receive alerts for geographic areas other than the location in which their device is located, in order to remain vigilant of prospective threats to loved ones living in other parts of the country? Further, the Commission seeks comment on how new technologies could facilitate consumer feedback on, and interaction with alert content. Could the text crawl of such alerts potentially contain clickable URLs and phone numbers directing the recipient to additional resources and information about developing emergency situations? The Commission seeks comment on the extent to which the advancements in technology may allow for customer feedback on alerts, such as confirming that an individual is threatened by a certain emergency condition, or enabling that individual to request specific emergency assistance by interacting with an alert. The Commission seeks comment on whether these technologies could give rise to a cycle of information sharing consistent with a "many-to-one/one-to-many" alerting dynamic.

#### 4. WEA Alerts to Tablets

127. Section 10.10 of the Commission's WEA rules defines a "mobile device" as "the subscriber equipment generally offered by CMS providers that supports the distribution of WEA Alert Messages." Pursuant to Section 10.500, support for the distribution of WEA Alert messages entails "(a) Authentication of interactions with CMS Provider infrastructure; (b) Monitoring for Alert Messages; (c) Maintaining subscriber alert opt-out selections, if any; (d) Maintaining subscriber alert language preferences, if any; (e) Extraction of alert content in English or the subscriber's preferred language, if applicable; (f) Presentation of alert content to

the device, consistent with subscriber opt-out selections . . . ; and (g) Detection and suppression of presentation of duplicate alerts." Electing to participate in WEA entails a commitment by the Participating CMS Provider "to support the development and deployment of technology for . . . mobile devices with WEA functionality." Pursuant to the Commission's CMS Provider election procedures, Participating CMS Providers must support WEA on at least one device. The Department of Homeland Security's (DHS) report on WEA penetration strategy states that "[t]he most significant WEA penetration gap over the long term regarding mobile wireless devices is the lack of WEA capability in the tablet computers." DHS recommends that the Commission should find a way to encourage Participating CMS Providers and tablet computer manufacturers to add WEA capability to their tablet offerings that have wireless cellular data connectivity.

128. The Commission seeks comment on whether it should consider tablets that consumers use to access mobile services as "mobile devices" under the Commission's Part 10 WEA rules. Do 4G LTE-enabled tablets currently support the distribution of WEA messages? If not, the Commission seeks comment on what, if any, standards, software, or hardware modifications would be required to enable 4G-LTE-enabled tablets to support the distribution of WEA messages? Would 4G-LTE tablets be able to receive WEA alerts when they are connected to a Wi-Fi network or other unlicensed spectrum, based on the user's preference (such as when the user is at home and connected to their own Wi-Fi network), but while the tablet still remains within range of the Participating CMS Providers' 4G-LTE network? The Commission seeks comment on any costs commenters believe would likely be attendant to providing WEA alerts to 4G LTE-enabled tablets. The Commission also seeks comments on any benefits likely to result from the delivery of WEA alerts to 4G LTE-enabled tablets. Specifically, the Commission seeks comment on whether modernizing alerting platforms in this manner would increase the likelihood that individuals would receive potentially life-saving alerts by requiring that they be

transmitted to the devices and services they use most. Are Participating CMS Providers prepared to develop a voluntary roadmap for providing WEA alerts to 4G LTE-enabled tablets?

### 5. Technological Potential for Improvements in Accessibility

129. The Commission seeks comment on the potential of new and emerging technologies to improve alert accessibility. In particular, the Commission seeks comment on the state of technology for machine-generated translation (i.e., the use of software to translate text or speech from one language to another), to provide emergency alerts in non-English languages, and whether and how such technology could be leveraged by both the EAS and WEA systems. Are languages such as Spanish, that share a character set with English, more easily machine translatable than languages that use other character sets? How advanced are machine translation technologies for English to ideographic languages, such as Chinese? Could such translators be incorporated into EAS equipment? The Commission also seeks comment on the potential utility of platform-based video relay service capabilities to enhance the understanding of alerts and warnings for individuals with hearing and vision disabilities. The Commission seeks comment on these questions in order to gain a better understanding of achievable alert accessibility technologies.

130. Further, the Commission seeks comment on the ability of OTT alerting to improve EAS alert personalization. Could OTT EAS alerting be leveraged to improve alert accessibility for all Americans, including those with sensory disabilities those with limited English proficiency? For example, could the availability of URLs make it possible for alert content to be presented in languages other than English and in American Sign Language (ASL)? Could consumers personalize alert preferences with respect to text size, crawl speed, and contrast based on their unique needs? Could alerting via OTT services facilitate the use of symbols as accessible replacements or supplements to alert messages? Is it technically feasible and should

consumers be given the ability to control the volume of the emergency alerting Attention Signal or audio message, independent of the volume settings in place for other activity on their device, in order to ensure that the alert is audible from anywhere in the home, or at least is appropriate for the user who may be deaf or hard of hearing? Similarly, is it technically feasible and should there be a requirement for any consumer, with or without a disability, to be given the flexibility and capability to control other settings of the alerting signals and audio levels, such as the type and intensity of vibrations and flashing lights, in order to accommodate their individual needs? Alternatively, would it be appropriate to enable users to lower the volume of an EAS alert in certain circumstances?

131. In the WEA NPRM, the Commission seeks comment on the feasibility of providing WEA messages in languages other than English and on the extent to which accessibility requirements would improve the presentation of multimedia content in WEA messages. Would extending WEA rules to include tablets and other mobile devices, as defined in the Commission's Part 10 rules, further enhance the accessibility of alerting to the public and to persons with disabilities? To what extent should WEA messages be subject to Commission accessibility requirements? Would the larger screen of tablet computing devices enable them to provide WEA messages that are more accessible to individuals with visual disabilities?

### D. Securing the EAS

132. As described below, several high-profile and other less widely-known EAS security breaches in recent years have demonstrated that there are significant vulnerabilities in the nation's EAS infrastructure that must be addressed comprehensively. The Commission is concerned about the severity, frequency and nature of the risks associated with these EAS attacks and the related implications for the readiness of the nation's critical means of alerting and informing citizens of threats to safety of life and property, consistent with the Commission's

statutory mission. The Commission starts to address those concerns with the proposals in this NPRM, including those discussed in this section and upon which the Commission seeks comment, which will help to ensure that the nation is better prepared in its ability to alert citizens of such threats, particularly to support the need of the President to communicate with the public during times of emergency and the need to ensure the system is reliable and secure in advance, in order to preserve that capability.

### a. Recent EAS Security Incidents

133. February 11, 2013 Incident. On February 11, 2013, unidentified hackers accessed EAS equipment at several TV stations to perpetrate a "zombie attack" hoax. The false alerts affected television stations KRTV in Great Falls, Montana, WBUP and WNMU in the vicinity of Marquette, Michigan, and other stations in Michigan, Utah, New Mexico and California. The stations were vulnerable to this particular attack because they failed to change manufacturer default passwords on their EAS equipment, install firewalls, or take other appropriate security measures, which left the equipment easily accessible from the Internet.

134. October 24, 2014 Incident. On October 24, 2014, station WSIX-FM in Nashville, Tennessee aired a false emergency alert during the broadcast of the nationally-syndicated "The Bobby Bones Show." Bobby Bones, the show's host, ran an audio clip from a November 9, 2011 nationwide EAS test that contained the live EAN code reserved for Presidential EAS activations. Mr. Bones' apparent intent was to mock a local cable company's airing of a mandatory monthly EAS test during the second game of the 2014 World Series. The "gag," however, had serious consequences: the clip was replayed by other radio stations, as well as cable TV and wireline video television systems in 32 states and the District of Columbia. Indeed, for approximately two hours, more than half a million television subscribers found their set top boxes locked on a false EAS message stating that regular programming had been interrupted by order of the White House.

Had an appropriate authentication mechanism or date validation EAS protocol been established and installed on equipment that received the false alert, this incident likely would have been prevented.

135. Other Incidents. While the incidents described above are perhaps the most widely known EAS security breaches in the recent past, they are not isolated. Other, less notorious system breaches have occurred that also generate cause for serious concern. One fairly common scenario in this regard involves inadvertent activation/improper test alerts. For example, in December 2010, an unauthorized EAN alert was issued by WBLE, a radio station operating in northwest Mississippi. According to WBLE, a part-time engineer attempting to issue a required monthly EAS test accidentally pressed the wrong button and issued an EAN alert instead. This error, according to AT&T, affected approximately 17,000 U-verse subscribers in their Memphis Video Hub Office (VHO). The impact was similar to that of the Bobby Bones Show Incident in that subscribers' set top boxes were force tuned to the designated EAS alert channel and remained locked on that channel for approximately four-and-a-half hours. Proper originator authentication included in the EAS protocol would have prevented the incident.

136. Additionally, on June 26, 2007, a government contractor installing satellite equipment in Springfield, Illinois triggered an accidental EAN activation when he incorrectly left the receiver connected to a state EAS transmitter before final testing of that delivery path had been completed. The false EAS alert repeatedly interrupted programming for three or four minutes at a time and, in Chicago, triggered channel switchovers to a single area broadcaster, WGN. Proper originator authentication included in the EAS protocol would have prevented the incident.

137. Improper retransmission of dated EAS alerts, similar to the Bobby Bones Show incident, are also somewhat common. On February 12, 2013, for example, WIZM-FM in La

Crosse, Wisconsin inadvertently triggered an EAS warning on neighboring station WKBT-DT by playing a recording of the Zombie Attack Hoax incident during its morning show. Another inadvertent retransmission occurred in a September 2010 advertisement for ARCO/BP aired by stations in several states including Oregon and Kansas. The advertisement included the EAS attention signal and header codes from an EAS RWT that triggered EAS devices in multiple stations nationwide. The inclusion of originator authentication or date validation in the EAS protocol would have prevented the incident.

138. Collectively, the incidents described above reveal an unacceptably high risk of unauthorized EAS signal broadcasts and insufficient real-time Commission awareness of, and visibility into the possible negative impacts of unauthorized alerts. In combination, they point to troubling security vulnerabilities associated with the nation's EAS. Unless appropriate actions are taken to enhance the broadcast network security environment through which the nation's EAS operates, these risks, vulnerabilities, and resulting problems are likely to persist, and indeed grow. That potential is likely to be exacerbated by the Nation's ongoing national transition to CAP alerts because of the increasing reach and number of originators capable of transmitting alerts.

**b. Earlier Commission-Related Efforts**

139. Until now, the Commission has sought to ensure EAS security by encouraging EAS Participants to voluntarily adopt EAS security best practices. These efforts, however, have not always borne the intended fruits of a highly secure, highly reliable and unquestionably credible system. Indeed, the record tends to suggest a certain level of complacency by at least some EAS Participants with respect to system security. A brief discussion of that history illustrates the shortcomings of the voluntary approach and further highlights the need for the new approach the Commission explores below.

140. Best Practices – CSRIC IV. On June 18, 2014, CSRIC IV unanimously adopted a set of voluntary best practices to be recommended to the EAS Participant community for the improvement of EAS security. Shortly thereafter, on November 7, 2014, the Bureau sought comment on CSRIC IV's recommendations. Surprisingly, the Commission received no substantive comments from EAS Participants, which raises questions regarding the extent to which EAS Participants are taking appropriate measures to manage security risk and ensure system performance at the levels necessary to achieve national public safety goals.

141. Also on November 7, 2014, the Bureau released a Public Notice announcing an inquiry into the impact of false EAS alerts on the security, reliability and integrity of EAS. As part of this inquiry, the Bureau held meetings with EAS Participants, FEMA, equipment manufacturers and other EAS stakeholders. The record developed through these activities suggests that the EAS' present authentication methodology warrants further examination in terms of its adequacy, systemic security, and reliability.

142. Bobby Bones Show Incident and Other Assessments. As discussed above, Commission staff studied the Bobby Bones Show Incident, a separate "zombie attack" hoax and other similar incidents to identify causes and issues associated with EAS security. All of these incidents involved a lack of built-in EAS user authentication and validation procedures, as well as weak implementation of other readily employable security best practices that would have prevented such unauthorized actors from entering and misusing the system.

### 2. Improving EAS Network Security

143. Unauthorized EAS alerts generate a host of ills, from consumer inconvenience and frustration over TV lockouts, to broad public fear and confusion about the existence and nature of threats. False alerts divert public safety and other government resources from other important activities, impose costs on licensees that have to deal with many of the consequences

of false alerts and, ultimately, desensitize the public to legitimate alerts. The Commission, consistent with its fundamental public safety mandate, must ensure that the public has complete confidence in the EAS as one of the nation's essential public safety communications tools. Thus, if EAS Participants cannot effectively secure the system through voluntary mechanisms, the Commission must explore regulatory solutions to achieve EAS security. Accordingly, the Commission now proposes rules designed to safeguard the EAS and maintain continued public trust in the system.

144. In this section, the Commission seeks comment on proposals intended to decrease the likelihood of false or malicious EAS broadcasts, and to codify best practices consistent with CSRIC IV's recommendations. The Commission also proposes rules requiring the reporting of false alerts, i.e., alerts issued in situations other than a bona fide emergency, test, or public awareness campaign, and lockouts, and new rule changes for alert authentication and validation. The Commission also believes that these proposed rules – backed by an annual certification of specific actions from EAS Participants demonstrating adherence to the security best practices recommended by CSRIC IV – will fundamentally enhance the security of the EAS and help provide a baseline of actions from which to initiate risk management processes to protect the EAS. Additionally, the proposed reporting requirements would provide a minimum set of actions to assist in the communication of incident detection and response. These proposals are intended to complement, rather than replace, the Commission's current support for voluntary implementation of best practices developed through cooperation with industry and advisory bodies. Each proposal is intended to be flexible, so commenters should describe in detail how they propose to implement any preferred approach they may have, and how those choices advance the goals of this NPRM. The Commission encourages EAS Participants to examine all of their approaches to managing security risk, including planning and recovery, to inform their

recommendations for improvements.

145. Also, the Commission invites alternative proposals from commenters on how best to promote EAS security. Commenters should support such proposals with sufficient information and analysis to provide a basis for thorough consideration. Given the importance of ensuring the authenticity and security of presidential EAN messages, the Commission also seeks comment on whether its proposed changes are sufficient for all EAS messages, or whether additional measures should be taken to secure particular alerts, such as the EAN. Assuming such additional measures are indicated, commenters should describe them and explain how they would better secure the EAS. Finally, commenters should address relative costs and benefits of the Commission's proposed rules as well as any proffered alternative proposals.

**a. Annual Certification**

146. In light of the issues raised above, the Commission proposes action to ensure that EAS Participants are following EAS security best practices, which in turn will make the Commission's nation's alerting system more secure and reliable. The Commission proposes that EAS Participants must submit an annual reliability certification form that attests to performance of required security measures with a baseline security posture in four core areas, as described in the following sections. The Commission believes this annual certification would establish minimum expectations for security, and provide the Commission with the necessary assurances that EAS Participants are adhering to industry best practices and therefore taking appropriate measures to secure the EAS. The Commission believes this requirement would be minimally burdensome, and would allow EAS Participants ample flexibility in implementing core security mechanisms based on the individual entity's particular needs. As an initial matter, the Commission seeks comment on whether an annual certification would achieve these objectives, and on the relative costs and benefits of this approach. The Commission expects that the

information required to make a determination by the certifying official is readily available as part of the Participant's normal operations, and that the amount of legal and management review is negligible given that the best practices to which they certify are well known and have been carefully assessed by industry in the CSRIC process. The Commission estimates that certification should add an average of fifteen minutes to the annual update of the "identifying information" section in ETRS, resulting in an increased cost to industry of approximately $549,360 per year. If additional legal and management review would be required, the Commission assumes it would only be required the first year to ensure appropriate internal processes were in place and would amount to no more than an average of one hour per company for an additional $2,179,440 the first year. For those EAS Participants who are not using best practices, the Commission estimates it should take no more than four hours per device to perform the necessary changes, resulting in an estimated cost of $879,040 to industry. The Commission seeks comment on the accuracy of the estimates of the expected number of Participants that are not using best practices, the accuracy of the assumptions underlying the amount of time required for compliance, and the accuracy of cost estimates. Are there additional costs that are not sufficiently captured by these proposed cost estimates? Administratively, should the "identifying information" section of ETRS be used to provide an EAS Participant's certification, or should a different mechanism be used for making and recording the certification? Is it reasonable and efficient to require the certification to be part of the current required annual update of ETRS identifying information? What ways might there exist to further reduce the burden on EAS Participant while achieving the same result? Would the longer term burden be reduced by including a provision to review the certification requirement in five years with the intent to sunset the requirement if it becomes clear that Participants are effectively managing cybersecurity risk through mature implementation of the NIST Cybersecurity Framework or

suitable equivalent as demonstrated through the planned cyber risk assurance meetings and Sector Annual Report recommended by CSRIC IV?

147. Further, the Commission seeks comment on each of the four core elements that would be addressed in the annual certification. Particularly, the Commission asks whether these four areas of certification provide sufficient assurance that security best practices are being followed. Are there any additional – or alternative – areas that should be subject to certification to achieve system security assurance aims? Are there measures that the Commission or industry stakeholders can take to ensure performance of the proposed security measures are minimally burdensome for all EAS Participants, from the largest broadcasters and cable systems to the smallest independent operators? For example, could industry organizations at the national and state levels work with their members to conduct outreach to smaller and less resourced EAS Participants to educate them and otherwise help them to successfully certify their compliance with the security guidelines the Commission proposes today? What, if any, should the Commission's role be in such an outreach effort? The Commission notes in this regard that the Bureau has already released a Public Notice reminding EAS Participants of the EAS security best practices recommended by the CSRIC IV Initial EAS Security Report and has participated in a number of industry-related panels discussing cybersecurity as well as a webinar on cybersecurity for broadcasters. Are there other outreach steps in the CSRIC IV Final EAS Security Report that the Commission should undertake to raise public awareness regarding EAS security and to help EAS Participants incorporate EAS security best practices?

**(i) Patch Management**

148. A basic network security hygiene practice for any communications- and computer-based system – EAS included – is ensuring that the system runs up-to-date, secure software and firmware. This practice is included in various best practice documents, surveys and

security guidelines, including one of the "first five" controls from the SANS Institute Critical Security Controls, control CSC 3-2. For more than a decade, the Commission and a series of communications security authorities and expert bodies have stressed the importance of regular system patching and updating, starting with Network Reliability and Interoperability Council (NRIC) V, and continuing through NRIC 7, CSRIC 2, and CSRIC 3. Despite continued attention to patching as a needed part of basic security hygiene, attackers continue to exploit unpatched systems. According to Verizon's 2015 Data Breach Investigations Report, 99.9 percent of all computer system exploits target vulnerabilities that have persisted for at least a year. Additionally, SANS control CSC 6-1 – updating to the most current software and firmware version and patch level – would be the recommended mitigation strategy in 24 percent of all incidents Verizon reviewed.

149. In the Bobby Bones Show incident, for example, vendors with properly updated software and firmware for their EAS equipment resisted the false alert. Others, whose system software/firmware were unpatched, either broadcast the false alert or queued it for later broadcast. Had all equipment been updated to the latest version and in the correct configuration, it is highly likely the alert would not have been rebroadcast.

150. Proactive management of system vulnerabilities tends to reduce or eliminate the potential for exploitation and involve considerably less time and effort than responding after an exploitation has occurred. Accordingly, the Commission proposes, and seeks comment on, requiring EAS Participants to certify annually that they keep their systems updated with the latest firmware and software patches. The Commission observes that three of the thirteen best practice controls recommended by CSRIC IV cover patch management. Specifically, Recommended Control No. 1 states that "EAS participants should regularly monitor EAS Manufacturer information resources (e.g., websites) to obtain vendor patch/security notifications and services

to remain current with new vulnerabilities, viruses, and other security flaws relevant to systems deployed on the network"; Recommended Control No. 6 states that EAS Participants should "regularly seek and install software updates and patches"; and Recommended Control No. 7 states that they should "expedite general system updates and security patching."

151. Would effective implementation of best practice Control Nos. 1, 6 and 7 be assured by requiring participants to certify that they have followed a program to identify and install updates and patches to EAS devices and attached systems in a timely manner, verified EAS devices are running the current version and patch level of software and firmware, and verified that systems connected to EAS devices are running the current version and patch level of software and firmware? If so, is that sufficient to demonstrate basic security hygiene in the EAS? What alternatives would be acceptable if a participant does not comply with the above elements? Should the Commission allow participants to instead certify the measures they have taken to provide equivalent security or the explanation of how the above elements do not apply to their network? How extensive should such descriptions or explanations be? What issues could arise from requiring that the certification apply to both EAS equipment and all network equipment on the same network? Are there any reasons to refrain from applying the certification requirement to all network equipment connected to an EAS device? Is an annual performance certification from an EAS Participant sufficient? If not, what is a more appropriate interval for filings attesting to performance of required security measures? Alternatively, should the Commission require EAS Participants to update their systems when a patch or update is released and report that they have done so to the Commission? How much time would EAS Participants need to comply with a requirement to identify, acquire, test, apply and verify such updates? Are any of the specific actions proposed above unnecessary, and, if so, why? Alternatively, what other measures should be included in the certification?

152. The Commission seeks comment on the cost of complying with an annual requirement to certify as part of the required information in ETRS that systems are fully patched and running the most current firmware. Since ensuring proper patching and updating is already a common best practice across the communications sector, the Commission assumes that, for most EAS Participants, there would be no additional cost related impact to keeping EAS related systems current. Is this a reasonable assumption? Are there other factors that should be taken in to account when determining whether complying with this particular best practice would require additional effort? Would the benefits from increased performance of required security measures for EAS Participants who are not currently practicing them outweigh the costs of filing? The Commission requests that commenters be specific about costs and provide support and documentation accordingly.

**(ii) Account Management**

153. A second basic security hygiene practice is proper control, assignment and management of user and administrative accounts. Poor password practices are directly responsible for the Zombie Attack Hoax that had an impact on multiple stations in the northern and western regions of the nation. Due to stations not changing the manufacturer default passwords on their Internet-accessible equipment, hackers were able to log in, generate and send false EAS alerts. As a result, the Commission issued an urgent notice to change default passwords on EAS devices.

154. Despite the existence of well-known user account management best practices, the security breaches described above show that a number of EAS Participants fail to follow them. Thus, the Commission proposes a rule that would require EAS Participants to certify that they are following specific, common, EAS user account management best practices. Had such a rule been in effect at the time of the Zombie Attack Hoax, the targeted entities would have had

certifications on file with the Commission that they had changed the default password for the system, had removed or disabled improper accounts, and routinely enforced complex passwords. The Commission believes such certifications, submitted upon penalty for false statements, would have induced the stations to change their default passwords, thus preventing the Zombie Attack Hoax. The Commission seeks comment on this belief and on its underlying analysis.

155. Accordingly, the Commission seeks comment on rules requiring EAS Participants to certify annually that they have a control system in place to restrict access to EAS devices, that all EAS devices and connected system passwords have been changed from the default passwords, that password complexity is required, and that default, unnecessary, and expired accounts have been removed or disabled. Would these requirements be sufficient to ensure proper control over EAS device access? If not, what other user account management requirements should be added? What account management alternatives would be acceptable in lieu of these specific elements? In that vein, should participants be required instead to certify as to measures taken to provide equivalent security, or to explain how the account management elements described do not apply to their network? How extensive should such descriptions or explanations be? Should they apply to both EAS equipment and all network equipment on the same network? Should the ETRS identifying information section be used to provide an EAS Participant's certification? Is there a better method of recording certification? Is it reasonable and efficient to require certification as part of the currently required annual update of ETRS identifying information?

156. The Commission also seeks comment on the costs of complying with this particular element of the certification process. Since accepted best practices require basic account management, the Commission assumes that there would be little or no additional effort required to implement those best practices. Is this a reasonable assumption? The Commission

requests that commenters be specific about costs and their sources.

### (iii) Segmentation

157. In the Zombie Attack Hoax, outside actors used default passwords to gain remote Internet access to EAS devices allowing them to transmit false alerts. Had the impacted stations implemented best practices to prevent unauthorized remote access, it is far less likely that the intruders would have been able to penetrate the systems and log in with the default password. A firewall or other architectural separation would have impeded their ability to discover, access and utilize the EAS devices, and would likely have prevented the intrusion. Further, proper remote access security would have provided indications of the access attempt to system administrators who, in turn, could have acted upon that information to safeguard the system.

158. Accordingly, the Commission proposes requiring EAS Participants to certify annually that they have achieved a minimum level of segmentation of the EAS system. The Commission defines segmentation here for certification purposes as a category of best practice-based actions that logically group and compartmentalize assets and restrict trusted access to those compartments. Specifically the Commission proposes that EAS Participants certify that none of their EAS devices is directly accessible through the Internet, (for example, by configuring a firewall to deny access from the public Internet) and that any other type of remote access is properly secured and logged. The Commission believes this would have prevented the fraudulent remote access experienced in the Zombie Attack Hoax and in other similar attacks. The Commission specifically seeks comment on the effectiveness and desirability of the proposed rule. Would such a requirement adequately ensure proper separation of EAS equipment from Internet-connected network equipment? What other specific actions normally included in best practices to segregate control traffic from public access should be included in the certification? What segmentation alternatives would be acceptable to prevent unauthorized

remote access? Should participants be required to certify as to the taking of specified measures or, in lieu of those measures, explain how the elements described do not apply to their network? How extensive should such descriptions or explanations be? The Commission also seeks comment on the definition and use of segmentation as a category of certification items. Should the ETRS identifying information section be used to report EAS Participants' certification, or should a different mechanism be employed?

159. The Commission seeks comment on the cost of complying with an annual certification requirement that EAS devices are not directly accessible from the Internet. The Commission further seeks comment on the cost of complying with a requirement that any means of remote access is properly secured and logged. Since accepted best practices (as well as recommendations in vendor guides and industry publications) specify a firewall or other method of segmenting the EAS device from the Internet, the Commission's assumption is that there would be no additional cost associated with having to institute these best practices. Is this a reasonable assumption? Are there other factors that should be taken in to account when determining whether complying with the best practice would require additional effort?

#### (iv) Annual Certification of CAP Digital Signature Validation

160. Based on comments received in response to the Commission's inquiry into the Bobby Bones Show Incident, it is apparent that EAS Participants may opt not to filter CAP messages based on the digital signature parameter, or may only filter based on digital signature for selected CAP monitoring sources. This raises the risk that even if State or Local authorities include a digital signature in a CAP-formatted message, EAS Participants may disregard the signature if the message was received from a source other than IPAWS-OPEN. By ensuring, and accordingly certifying, that their equipment is configured to validate CAP digital signatures on

all CAP messages that include them, EAS Participants increase the security of the entire system by ensuring that CAP messages are unmodified and have been sent by a party with a valid digital certificate and, thus, are trustworthy messages.

161. The Commission seeks comment on the effectiveness and desirability of rules requiring EAS Participants to certify annually that their EAS devices are configured to validate digital signatures on CAP messages if the source of the CAP message includes this feature. Are there any technological or other barriers to certifying devices that are configured to validate digital signatures? If so, what actions could be taken to mitigate or remove those barriers?

162. The Commission also seeks comment on the cost of complying with an annual requirement to certify, as part of the required information in ETRS, that EAS devices are configured to validate digital signatures on CAP messages for all CAP messages that include a digital signature. The Commission requests that commenters be specific about costs and their sources.

### b. False Alert Reporting

163. There currently is no requirement that EAS Participants report to the Commission or FEMA that they have generated a false EAS alert or what circumstances led to the false alert; thus requiring the Commission to rely on reports from the public and the press. This situation has often hampered the Commission's real-time awareness and ability to respond to a crisis or emergency associated with these activities. The Commission's experience over the last decade of collecting and analyzing communications network outage data through its Network Outage Reporting System (NORS) shows the value of acquiring network reliability data. False EAS alerts, if reported, could similarly provide situational awareness about the health of the EAS to the Commission in real time, and facilitate the Commission's ability to take action to mitigate the effects of the alert.

164. Accordingly, the Commission proposes, and seeks comment on, a rule requiring EAS Participants to report the issuance or retransmission of a false EAS message via ETRS. Should an initial report including only EAS header codes, source, area affected, and time discovered of the false message be required? Is that information sufficient for an initial report? Is it reasonable to require such information or should less be required of the initial report? What other information should be included? The Commission also seeks comment on whether EAS Participants should be required to file their false alert report in ETRS within thirty minutes of identification of a false EAS message transmission. Is there a more appropriate time frame for a required initial report? Should a final report be required 72 hours after the initial report that includes an explanation of the root cause of the improper transmission? What other information should be included? Is that time frame long enough for EAS Participants to provide a final report? Is there a more appropriate time frame for the final report? Should any information in the final report be considered confidential? If so, what information should be covered as such? The Commission seeks comment on the effectiveness and appropriateness of using the ETRS as a reporting tool. Is there a better method of reporting false message transmission?

165. Finally, the Commission requests comments on the costs, burdens and benefits of the proposed mandatory reporting requirement; whether the requirement would promote the reliability, resiliency and security of EAS services; and whether the Commission could more narrowly tailor the requirement or otherwise pursue an alternative that would maximize the potential benefits to society or would accomplish the proceeding's objectives in a less costly, less burdensome, or more effective manner. Based on similarities with the Commission's Part Four outage reporting requirements for the notification and initial reports, the Commission estimates that complying with the reporting requirement will require approximately fifteen minutes for the initial report and forty-five minutes for the final report, for a total of one hour and an estimated

cost of $46,400 per year. The Commission seeks comment on the reasonableness and accuracy of this estimate. Commenters should be specific about costs and their sources.

### c. Lockout Notifications

166. As described above, the Bobby Bones Show Incident's audio clip did not contain the EOM code to return subscribers to regular programming. This resulted in 667,195 AT&T U-verse customers across the United States being locked out for several hours, unable to change their television to other programming while leaving them wondering what was happening. During this lockout period, the viewers were left confused about the validity of the alert, placing the credibility of the alert messaging system in question. The Commission believes that viewers must be able to rely on the alerting system for timely, accurate alerting information on which they can depend. The Commission believes that EAS reliability would be greatly enhanced by taking necessary steps to prevent the conditions that would result in the inability of devices to resume normal operation after an EAS alert. The Commission believes this would further public safety interests and address credibility issues that currently linger with the current system. Mandatory reporting via ETRS of instances when EAS Participant equipment causes, contributes to, or participates in a lockout that adversely affects the public would assist the Commission in identifying and assessing the nature and extent of the lockout issue, as well as the impact of false alerts reported separately.

167. Accordingly, the Commission seeks comment on a proposed rule to require all EAS Participants to report instances when their EAS equipment causes, contributes to, or participates in a lockout that adversely affects the public (e.g., when multiple cable STBs cannot return to normal operation due to the failure to receive an EOM signal or otherwise correctly process an EAS alert). Is this definition of a lockout sufficient to capture all such events where the public's access to cable programming a cable-based alerts are concerned? The Commission

seeks comment on whether there are some lockouts below a certain threshold that would be unnecessary to report because of limited effect on consumers. To what extent would excluding some lockouts from reporting requirements reduce the burden on EAS Participants? What threshold would strike an optimal balance between minimizing costs and keeping the Commission informed of significant incidents? Is there a better reporting method or definition for what constitutes a lockout that would provide the Commission with the appropriate amount of information to monitor and address this issue? Given that such false EAS alert-driven lockouts can have a significant impact on potentially millions of viewers, should an initial report should be required within fifteen minutes of identification of such an incident? Is there a more appropriate timeframe for a required initial report? The Commission also seeks comment on the scope of information that should be included with a lockout notification. For example, would the date and time, message source, affected device type(s), and estimate of the number of devices affected be sufficient for an initial report? If not, what other information should be included? Should a final report be required seventy-two hours after the initial report including the root cause of the incident? Is that time frame sufficient to provide a complete and thorough final report? The Commission seeks comment on the effectiveness and appropriateness of using the ETRS as a reporting tool for this type of incident.

168. Finally, the Commission requests comments on the costs, burdens and benefits of the proposed mandatory reporting requirement; whether the requirement would promote the reliability, resiliency and security of EAS services; and whether the Commission could more narrowly tailor the requirement or otherwise pursue an alternative that would maximize the potential benefits to society or would accomplish the proceeding's objectives in a less costly, less burdensome, or more effective manner. The Commission estimates that complying with the reporting requirement will require approximately fifteen minutes for the initial report and forty-

five minutes for the final report, for a total of one hour and an estimated cost of $800 per year. The Commission seeks comment on the reasonableness and accuracy of this estimate. The Commission requests that commenters be specific about costs and their sources.

### d. Alert Authentication

169. The EAS Protocol does not currently include a method to ensure that an alert received by EAS equipment was originated by an authorized source, i.e., that the message is "authenticated." EAS equipment will respond as designed to any Presidential Alert regardless of the actual originator or broadcaster. There are two approaches, described below, that could effectively address this issue. The first approach leverages the existing features of digital signatures available on CAP-formatted messages – transmitted via IPAWS-OPEN or other IP-based connections, and the second approach explores the possibility of adding analog authentication mechanisms to EAS Protocol messages.

170. CAP allows for the use of a digital signature to be used as one method of message authentication. A message may be authenticated by using a digital signature when a federal, state or local CAP alert originator signs a CAP message using its unique originator key, and that signature is decrypted using a single decryption key provided by FEMA/DHS. An EAS Participant can know that a message was sent from a trusted source if it contains a digital signature that can be decrypted by the FEMA/DHS-provided key. Currently, all IPAWS-OPEN-originated CAP messages require digital certificate authentication, but some state and local CAP systems do not, and EAS Participants may elect not to filter CAP messages on the digital signature parameter for all, or only for selected CAP monitoring sources. As EAS Participants and federal authorities comply with CAP-related requirements in accordance with the EAS Second Report and Order, there is a clear and practical opportunity, presumably, to implement digital signature EAS authentication concurrently with those efforts. The Commission believes

digital signature authentication for CAP messages adds a significant layer of security to EAS. Thus, the Commission proposes to require that EAS Participants process and validate digital signatures when handling CAP-formatted EAS alerts, and discard as invalid any CAP message where the digital signature does not match an authorized source from FEMA or from a designated source specified in the State EAS Plan.

171. Accordingly, the Commission seeks comment on the desirability and feasibility of discarding CAP formatted EAS alerts where the digital signature is invalid. What barriers to the implementation of such a rule exist? Is a requirement for all EAS Participants to treat as invalid any CAP-formatted message signed with an invalid signature sufficient to achieve the desired goals? The Commission also seeks comment on the desirability and feasibility of digital signature authentication for all CAP messages, not only those originated by IPAWS-OPEN. Should the Commission require all CAP-formatted messages to be digitally signed? Are there any technical barriers to such a requirement? Is the current process for digitally signing CAP messages for IPAWS-OPEN sufficient? Could it be effectively used for all CAP messages? Should the Commission specify a method of ensuring that all EAS Participants can properly authenticate the alert originators they are responsible for monitoring, or should that be specified within the State EAS Plans? Are State EAS Plans the appropriate location for defining the authentication process for State and Local digital signatures? What impact would there be to state and local authorities from requiring all CAP-formatted EAS messages be digitally signed? Is this rule – in conjunction the certification requirement described above – the most effective and efficient means of ensuring performance of required security measures? If not, what other methods of ensuring performance of required security measures should be adopted? Would any of the questions or proposals in this paragraph apply equally to the WEA system? If so, then to what extent? Commenters should include detail concerning such proposals, including costs and

benefits of applying these types of security measures to the WEA system.

172. While CAP digital signatures can provide authentication for messages propagated via IPAWS-OPEN or other IP-based systems, they do not address traditional analog EAS messages transmitted over the air using the EAS Protocol. To address this issue previous commenters have suggested two methods of adding analog authentication mechanisms to EAS Protocol messages. Some EAS stakeholders support the use of an analog version of the CAP digital signature to confirm the authenticity of EAS messages originated in the EAS Protocol. To confirm the authenticity, Monroe proposes a solution of adding a unique message ID or authenticator after the existing EAS header codes. As an example, their TDX solution utilizes Audio Frequency Shift Keyed (AFSK) data in the audio portion of the message to provide an analog version of the CAP digital signature to be decoded downstream. Monroe suggests that "the use of only a few bits of data could suffice as an authenticator value," and that "such a solution would not overly burden the EAS message, lasting only two to four seconds, and would significantly improve message security." According to Monroe, such a solution would allow authentication of EAS Protocol messages without reference to an ulterior authentication source. There may be other potential solutions leveraging an analog version of the CAP digital signatures that would prevent retransmission of unauthorized audio alerts. If such an analog version of a digital signature had been in use during the Bobby Bones Show Incident, EAS equipment would have treated the unauthorized EAN alert as inauthentic because it lacked a signature. The same is true in the case of the February 12, 2013 retransmission of the Zombie Attack Hoax, and in the case of the ARCO/BP Advertisement Incident. Additionally, utilizing such an analog signature would have prevented the airing of a number of mistaken test events where an EAN was sent instead of a required test alert, including the December '10 Unauthorized EAN and the Springfield, Illinois Incident.

173. A second solution to EAS alert authentication that could be applied to alerts formatted in the EAS Protocol is a Virtual Red Envelope (VRE) system. While the EAS's predecessor, the Emergency Broadcast System (EBS), used red envelopes to send authentication codes to EAS Participants so that the EAS Participant could confirm the authenticity of subsequent alerts, this proposed virtual solution would use "IPAWS servers to distribute a short validation code as part of the Required Weekly Test." The Broadcast Warning Working Group (BWWG) advises that such a method could maintain fidelity to the EAS Protocol by appending the validation field to the end of the EAS message header. The message would be considered valid only if the validation code provided in the most recent required monthly test (RMT) matched a corresponding code included in the EAN message. Under the VRE model, "[t]he code match would compel the recipient equipment to automatically and immediately proceed to forward the entire enhanced EAS message in accordance with the Commission's EAS requirements." On the other hand, if the code did not match, this would trigger an alarm within the VRE system which would prompt manual authentication of the message. If a VRE system had been in use during the Bobby Bones Show Incident, EAS equipment would have treated the unauthorized Presidential EAS alert as inauthentic because it would have lacked an authentication code. Further, if the alert used for the first Nationwide EAS test in November 2011 had contained an authentication code, that code would not have matched the authentication code specified for alerts received in October 2014, which would have prevented retransmission. If EAS equipment were programmed to respond to such a mismatch by holding such an alert for manual inspection, the inspection would have revealed that the message was not sent by a trusted source, and it could have been discarded.

174. Accordingly, the Commission seeks comment on the desirability and feasibility of including a unique message ID and/or authenticator ancillary to the EAS Protocol header codes

and how to accomplish this in a manner that respects technological neutrality. The Commission seeks comment on the advantages and disadvantages of including a digital signature in CAP- and EAS Protocol-formatted EAS messages. The Commission also seeks comment on the desirability and feasibility of adopting a VRE solution to alert authentication that includes an authentication code within the EAS alert. Is a technical solution currently available that would allow the community to rapidly implement such a capability? What advantages and disadvantages would such a solution have? What would the impact of requiring such a solution be on small and medium businesses? What would the costs of such an implementation be? Should one, two or all of these solutions be required? Should each be considered an independent means of compliance?

**e. Alert Validation**

175. Alert message "validation" refers to a technical check of a message by EAS equipment that allows for confirmation that a message received is in fact a valid EAS message. The sole method currently available to EAS equipment for performing alert message validation makes use of a time stamp, which contains an inherent ambiguity in that no year parameter is specified in the time stamp. EAS equipment, therefore, is not always capable of determining whether an alert is valid. The Broadcast Warning Working Group (BWWG) notes that "[i]f a fake EAS event is sent or an operator makes a mistake but has the right credentials and timestamp, it will be propagated as programmed, even if it is a recording of a previous alert."

176. EAS alert validation could be improved by revising Section 11.31 of the Commission's EAS rules to include a year parameter "YYYY" in the time stamp ("JJJHHMM"), and requiring devices to ensure the expiration time of the alert is in the future. If a year field had been included in the time stamp during the Bobby Bones Show Incident, EAS equipment would have recognized that it was dated and, thus, could have prevented the unauthorized EAS alert

from being processed as valid by downstream equipment. Such date validation also could have prevented the ARCO/BP Advertisement Incident and the Springfield, Illinois Incident since they were also caused by replay of previous outdated alerts.

177. Further, the Station identification (ID) header code ("LLLLLLLL") could be a useful validation parameter if the station ID parameter is based on a static designation, such as a station's Physical System ID (PSID), and if EAS Participants accurately maintain the station ID parameter of their EAS equipment as well as the station IDs of the facilities they are assigned to monitor. If EAS equipment always verifies that the station indicated by an alert's station ID header code matches the station ID of an EAS Participant's assigned monitoring sources, use of station ID as a validation parameter could increase the security and reliability of the EAS ecosystem by not retransmitting EAS messages that have originated from outside its area.

178. Accordingly, the Commission seeks comment on the desirability and feasibility of amending Part 11.31 to include a year parameter in the time stamp, and to require devices to only transmit valid alerts. What hardware or software changes would be necessitated by adding a year parameter to the time stamp? How could any costs associated with this change be mitigated? Should the Commission define as valid only alerts with an expiration time in the future? Are there other validation criteria the Commission should consider based on the date-time fields? Are there other actions that the Commission should specify EAS Participants must take based on date-time fields? The Commission also seeks comment on the desirability and feasibility of requiring that the station ID header code be anchored to a static identifier, and on amending the Commission's EAS rules to require alert validation based on the station ID header code. Is PSID an appropriate unique station identifier suitable for use as the station ID header code? Are there other existing identifiers that would be more suitable? Is requiring devices to validate that the station ID header code matches one of the monitoring stations listed in the State EAS Plan, alone

or in combination with other methods, a reasonable and effective way of ensuring stations do not retransmit alerts from unauthorized sources?

179. There are some indications that checking for interstitial alerts as a means of alert validation might have prevented the Bobby Bones Show Incident. Recent recommendations from CSRIC IV, however, advise against discarding all interstitial alerts, as some such alerts may be damaged or otherwise inappropriate for retransmission, and some such alerts may be valid and appropriate. In light of the CSRIC IV recommendations on this issue, the Commission seeks comment on the desirability and feasibility of revising Part 11 of the rules to require discard of none, some or all interstitial alerts.

180. Finally, the Commission requests comments on the costs, burdens and benefits of the above proposed changes; whether the changes would reduce the incidence of inadvertent or false alerts; and whether the Commission could more narrowly tailor the changes or otherwise pursue an alternative that would maximize the potential benefits to society or otherwise would accomplish the proceeding's objectives in a less costly, less burdensome, and/or more effective manner. In the Sixth Report and Order, the Commission estimated the total cost to EAS Participants to modify software and firmware to accommodate the "six zeroes" nationwide location code at $2.2 million. Would the changes to include a year parameter and to check validity based on time and the station ID header code entail similar costs and would that estimate be accurate for this purpose?

### 3. Confidentiality and Information Sharing

181. In this section, the Commission seeks comment on the degree of confidentiality that should be provided for security certifications and reporting-related information submitted to the Commission via ETRS. Under Sections 0.457(d)(1)(vi) and 4.2 of the Commission's rules, the Commission currently treats reports that are filed in its Network Outage Reporting System

(NORS) as presumptively confidential, thus allowing such reports to be withheld from routine public inspection. This presumption recognizes both the "likelihood of substantial competitive harm from disclosure of information" and the Commission's concern that "the national defense and public safety goals that we seek to achieve by . . . these . . . reports would be seriously undermined if we were to permit these reports to fall into the hands of terrorists who seek to cripple the nation's communications infrastructure." The Commission currently shares NORS reports with the Department of Homeland Security (DHS), which may "provide information from those reports to such other [federal] governmental authorities as it may deem to be appropriate."

182. Treatment of Certification-Related Information. The Commission seeks comment on whether it should treat certification-related information with the same confidentiality as the Commission treats NORS information. The Commission recognizes that the EAS presents a somewhat different set of circumstances than NORS. EAS is not a revenue-generating apparatus designed by EAS Participants as part of the delivery of services to customers for remuneration. Rather, EAS is a system that exists solely for the generation of critical public safety messages. Further, EAS Participants do not risk competitive disadvantage due to disclosure of the kind of information the Commission now seeks. Against this backdrop, the Commission must weigh the public's presumed benefit in being able to assess, in real time, the security of its EAS, and the Commission tends to generally favor disclosure over confidentiality. In the alternative, should the Commission treat certification-related information as presumptively confidential, as it does in DIRS?

183. The Commission tentatively concludes that the act of filing an annual certification should not be treated as presumptively confidential; however, the Commission recognizes that the data reported on the certification should be treated as presumptively confidential. The

Commission recognizes the potential utility in treating as presumptively confidential information submitted in addition to annual certifications that describe alternative measures employed by the EAS Participant to mitigate the risks of nonconformance with certification elements. Accordingly, the Commission proposes the act of filing, and the contents of that addenda to EAS Participants annual certifications describing alternative approaches to performance of required security measures should be treated as presumptively confidential. The Commission believes this approach and rationale are consistent with other similar certification reporting requirements. The Commission seeks comment on these tentative conclusions, and on its analysis.

184. Treatment of Reporting-Related Information. Following the same underlying rationale for treatment of certifications above, the Commission tentatively concludes that the mere fact that an EAS Participant has filed a false alert report or lockout notification, as described in this NPRM, should not be treated as presumptively confidential. The Commission seeks comment on this tentative conclusion.

185. The Commission believes that a need exists to presumptively treat as confidential the information submitted by an EAS Participant pursuant to reporting on the issuance or retransmission of a false EAS message via ETRS, or on instances when an EAS Participant's equipment causes, contributes to, or participates in an incident that adversely affects the public and equipment does not return to normal operation after receiving an EAS alert. The Commission recognizes that some of the information in both contexts may contain material that, if disclosed, could potentially cause substantial competitive harm to the EAS Participant or even undermine national defense and public safety. Conversely, the same information may provide valuable insight into EAS vulnerabilities, information detailing specific corrective action(s) taken, the need for specific corrective action(s), or reasons why the EAS may have functioned sub-optimally. Given these competing concerns, the Commission tentatively concludes that

treating such information in a presumed confidential manner is justified. The Commission seeks comment on this view. The Commission also seeks comment on whether there are sound reasons why it should treat submissions related to EAS annual certifications, false alert reporting, and lockout notifications differently with respect to their respective presumptive confidential treatment.

186. Sharing with Other Entities. In the Commission's effort to strengthen the nation's public alert and warning systems as community-driven public safety tools capable of ensuring that the public can receive and respond to alerts issued by alerting authorities in an effective, timely manner, it will be essential to integrate and enhance timely cooperation and information exchanged among federal, state and local officials. The Commission therefore seeks comment on whether, if it adopts presumptively confidential reporting and certification requirements, as proposed above, the Commission should share the information with other federal agencies, as it deems appropriate and consistent with the requirements of Section 0.442 of its rules? Should the Commission restrict such sharing to only certain named federal agencies? The Commission asks for commenters to share their views not only on the extent and limits of such sharing, but provide underlying rationale to support their views. With which state entities, if any, should the Commission share this information? With which non-governmental entities, if any, should it share this information?

187. The Commission further seeks comment on whether information should be shared under Part 11 with the National Coordinating Center for Communications (NCC), a government-industry initiative led by DHS representing 24 federal agencies and more than 50 private-sector communications and information technology companies. Would access to data collected pursuant to Part 11 contribute to the NCC's mission? Under what terms, if any, should such access be provided? Should the Commission instead leave to the discretion of the EAS

Participants what Part 11 information they chose to share with the NCC? Would the Commission's sharing of Part 11 information with NCC discourage Part 11 reporting? Is there a subset of data proposed to be collected under Part 11 that the Commission should share with the NCC while upholding the confidentiality presumption that the Commission proposes be established for information submitted pursuant to Part 11? Would the sharing of Part 11 data in aggregate or generalized form be useful to NCC? Finally, it would appear that such information sharing would not have any appreciable cost impact. The Commission seeks comment on this view.

188. Conditions on Sharing. The Commission seeks comment on whether before it should allow data sharing with other entities as it did in the Sixth Report and Order that a state be required to first certify that it will keep the data obtained confidential and that it has in place confidentiality protections in place at least equivalent to those set forth in the federal Freedom of Information Act (FOIA). If the Commission allows the sharing of Part 11 information to another entity, what conditions, if any, should be placed on the use of such information? Should use of Part 11 information by shared entities be restricted to activities relating to protecting public safety, health or national security? Should the entities with which the Commission authorizes the sharing of information be limited in terms of access to the ETRS database on a "read-only" basis? Balancing EAS Participant interest in confidentiality with the need for timely sharing of information when appropriate, it would seem that Part 11 information sharing should be permitted by the Commission only if stringent measures are in place to protect the data from public disclosure. The Commission seeks comment on this analysis and what measures, if any, should be in place if the Commission shares Part 11 information with any appropriate entity.

189. Given the national security and critical infrastructure concerns with having access to this data, what additional assurances can the Commission provide to ensure that any Part 11

information shared with appropriate entities will be properly safeguarded? Should personnel charged with obtaining Part 11 information be required to have security training? Should the identity of these individuals be supplied to the Commission? Should states be required to report breaches of confidentiality of information obtained as a result of compliance with the Commission's Part 11 rules? Should an EAS Participant be permitted to audit a state's handling of its information submitted in accordance with Part 11?

190. Potential Alternative, Incremental Approach. One way for the Commission to gain experience on the best path forward for the sharing of confidential information under the Commission's proposed Part 11 rules may be to study the issues involved by developing an interim information sharing capability. As appropriate, the Commission may implement a prototype exchange of Part 11 information sharing with interested states and EAS Participants on mutually agreeable terms, as a means of building confidence among stakeholders and informing its development of proposed rules. As another example, the Commission could seek to establish a negotiated, temporary information-sharing program with the NCC for a specified period of time (e.g., eighteen months), after which time the program would be evaluated by the Commission, NCC, its members and other stakeholders for its effectiveness and whether it should continue unchanged, continue with modifications, or be terminated. The Commission seeks comments on this possible incremental approach.

191. In addition to any EAS information that the Commission ultimately may receive through the reporting processes outlined in this NPRM, the Commission may also obtain information through other sources (public and non-public) revealing vulnerabilities in the EAS. While the Commission proposes to treat information contained in certifications as presumptively confidential, as discussed above, it does not presently have an established regime for other information that it may receive that is in addition to information received through the reporting

processes. As potential threats increase, and as the Commission receives more information on related threats to EAS and its potential vulnerabilities, should the Commission establish a set of controls within the Commission to limit the distribution of and otherwise safeguard the information that it receives? For example, should such information be treated as presumptively confidential as well? Further, should there be specific methodologies for the handling of information on EAS vulnerabilities, beyond simply the confidential treatment of that information? Should the Commission apply physical and IT security controls to protect information regarding EAS vulnerabilities, and limit access to such information on EAS vulnerabilities to a validated subset of Commission staff? The Commission asks commenters to address whether and what controls should be used in the Commission's handling of such information, and the duration for which such controls should remain in force or effect. The Commission seeks comment on these or other potential approaches to the treatment of information that reveals potential vulnerabilities in the system, and to the designation and handling of such information once received by the Commission. The Commission also asks commenters to address whether the designation, treatment and handling processes proposed ought to concern both the physical EAS architecture as well as IT security controls, or just one of those areas and, if the latter, which and why?

192. The Commission also seeks comment on the extent to which EAS stakeholders, including EAS Participants and EAS equipment vendors, should take measures to ensure that potential architectural or configuration vulnerabilities are safeguarded from inappropriate public disclosure. For example, the Commission observes that EAS equipment manufacturers may provide encoder/decoder information available to users on public websites, including default equipment passwords. Despite the Commission's proposal to require participants change default equipment passwords, does such practice create potential vulnerabilities? The Commission asks

commenters whether information on the EAS architecture, including equipment instructions, can be subject to safeguards, and if so by what means? For example, should instructions be made available only to validated entities and thus, not made publicly available on websites? How could the effectiveness in increasing security of such a restriction be measured compare to the costs of administering such a program and of limiting access to operators, maintainers, and researchers? What other measures should stakeholders take to keep information regarding EAS architecture and configuration secure? To the extent the Commission were to take measures to ensure that information on EAS architectural and IT configuration vulnerabilities is made more secure, what specific legal and regulatory authorities would apply?

#### 4. Reach of Proposed EAS Security Rules

193. As a logical extension of the Commission's discussion above of the costs and operational issues associated with implementing new security measures for EAS, the Commission seeks comment on whether its proposed security rules should apply to all EAS alerts, and to all EAS Participants. Specifically, the Commission seeks comment on whether the Presidential Alert may warrant additional and/or heightened security measures, whose implementation costs may exceed the benefits when applied to local alerts that are issued more commonly, and that have a less immediate impact on national security. In the discussion below, the Commission seeks comment on whether to except EAS Participants currently designated as PN stations from some or all of the security requirements it proposes. The Commission also seeks comment on potentially excusing EAS Participants that qualify as "small businesses" under the Small Business Association (SBA) standard for their respective industries from some or all of the security requirements the Commission proposes today.

194. EAN Only. Would applying the above-proposed security measures to the EAN only recognize that the Presidential Alert presents heightened security concerns and more

complex technical implementation issues than other EAS alerts? On the other hand, would application of enhanced security rules to the EAN risk dividing the Part 11 rules into two separate sets of requirements that may be burdensome or incompatible to implement using a unified EAS protocol, or when implemented in the same EAS equipment. In light of the fact that EAS Participants maintain only one piece of EAS equipment for both the Presidential Alert and all other alerts, notwithstanding their distinct functionalities and purposes, would an EAN-only approach obviate any technical or financial benefit that might result from limiting application of security measures to the Presidential Alert? Does the fact that alert authentication and validation are automated processes similarly undermine the potential for cost savings that might result from forbearing from applying the proposed heightened security measures on all but the Presidential Alert? If EAS equipment is capable of providing heightened security for one kind of alert, would there be any reason not to provide that functionality for all alerts? Additionally, would improving alert authentication and validation for the EAN require changes to the EAS header codes that would be best applied consistently to all alerts?

195. Exception for PN Stations. Are security concerns attendant to participation in EAS less pronounced for PN stations than key EAS sources in light of the fact that they are not monitored by other EAS Participants? Would the severity of an EAS security breach be directly related to the designation of the attacked EAS Participant in the EAS alert distribution hierarchy? If so, does that militate for a graduated application of the security provisions proposed above such that key EAS sources are subject to stricter security requirements than PN stations? Should the application of the Commission's security rules be even more granular, for example, with NP stations being subject to more strict security requirements than Relay stations?

196. Small Entities. Would it be preferable to allow the EAN to be delivered only by more sophisticated or secure systems, preserving the flexibility for smaller EAS Participants alert

originators at the state and local levels to participate in state and local alerting without the need for certain additional security measures? If the Commission were to except small entities from application of some or all of its security rules, is the SBA size standard the appropriate metric for determining whether a business should be considered "small," or would another standard be appropriate and, if so, on what basis(es)?

### 5. Software-defined EAS Networking

197. In this section, the Commission initiates a dialogue about whether the level of administrative upkeep and oversight required to ensure that all security and performance updates required to maintain EAS equipment are uniformly implemented across a heterogeneous EAS system, and the level of coordination and planning needed to satisfactorily address the complex and varied threat vectors that exist for attacking EAS militate in favor of a new approach to EAS design. In particular, the Commission seeks comment on the efficacy of two potential software-defined networking approaches to a new EAS paradigm: 1) centralized configuration and management of EAS updates and security; and 2) virtualization of EAS equipment. The Commission also seeks comment on whether and how these approaches could be implemented in order to improve EAS security, and increase the consistency of EAS operations.

#### a. Centralized Configuration and Management

198. Centralization of EAS configuration and management entails logically connecting EAS equipment to a remote, central controller or database. In the Fifth Report and Order, the Commission declined to require that EAS equipment contain an Ethernet port, reasoning that the decision of how to fulfill CAP monitoring obligations is best made by EAS equipment manufacturers. That said, Trilithic commented that "we expect an Ethernet connection to be the input/output of choice for future (and present) EAS Encoder/Decoders." Using an Internet connection, either through Ethernet or wireless, the central controller could have visibility to

every piece of equipment in the EAS alert distribution network. By performing routine checks, the central controller could be able to distribute and install software patches to close security vulnerabilities in EAS equipment, as required. It could also control the distribution path of EAS alerts nationwide in a manner that precluded single points of failure. Centralization could supplement, rather than replace, traditional alert distribution mechanisms. A high-level depiction of a centralized EAS controller concept is depicted in Figure 1.

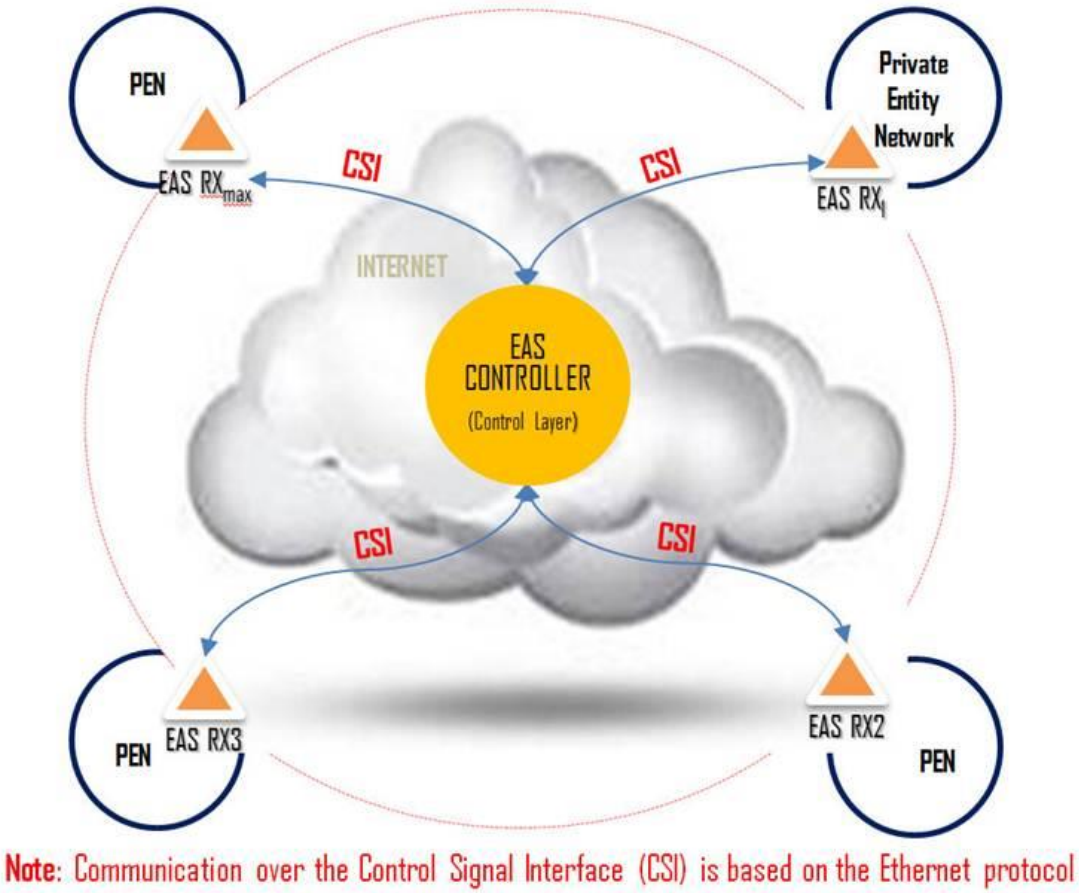


Figure 1: Diagram of Centralized EAS Configuration and Management Concept

199. The Commission seeks comment on whether a centralized configuration and management structure for EAS would result in significant security and operational benefits. The security of the EAS platform has been compromised on several occasions. While the Commission has proposed to adopt measures to further authenticate and validate EAS messages above, given the scope of human intervention required to completely inoculate the EAS against

unauthorized alerts and other security threats, is it possible that continued piecemeal modification of the Part 11 rules, even with greater diligence on the part of EAS Participants in adhering to security best practices, might not be sufficient to fully secure the EAS? The Commission seeks comment on whether a broader approach to EAS architecture design may be necessary. Particularly, as threats evolve, what steps should the Commission take now as a proactive response to such threats? Specifically, the Commission seeks comment on whether centralization has potential to augment EAS capabilities, whether it has the potential to improve EAS security and reliability, and on the engineering challenges and operational issues, including cost, that implementation would entail.

200. Augmented Capabilities. Would centralization of EAS configuration and management have the potential to transform EAS into a more capable system? If so, to what extent and in what ways? If the distribution pathway of alerts were configured by a central controller connected to EAS equipment via an Internet connection, could a centralized configuration and management model for EAS be used to ensure that no single point of failure exists in the EAS alert distribution hierarchy? Could a tiered control model be developed such that SECCs could continue to determine the distribution paths and monitoring assignments for alerts and EAS Participants, respectively, in their states, pursuant to a "no single point of failure" principle that could be maintained by a central controller? Relatedly, could the ability to configure EAS alert distribution pathways improve geo-targeting, especially if it is implemented for all EAS Participants, not just key EAS sources? Indeed, could such a model enable EAS alerts to be targeted to not only geographic areas, but to specific EAS Participants? In the cable environment, could the centralization concept be expanded to include a connection to STBs that would enable alerts to be targeted to specific individuals? Further, the Commission seeks comment on whether a centralized configuration and management model could be made capable

of ensuring that all EAS equipment across the nation is running the most up-to-date software available by performing periodic version checks of EAS software via the Internet. The Commission seeks comment on the extent to which this approach could bring uniformity and consistency to EAS equipment operation, and ensure that all EAS equipment is able to take advantage of the improvements that equipment manufacturers make available through software updates, obviating the risk of human error. The Commission also seeks comment on how the underlying heterogeneity of the EAS environment might complicate centralized control and uniform operation.

201. Improved Security, Reliability and Resiliency. Would central configuration and management increase EAS security and reliability by relying on a secure Internet connection for communication between EAS devices? The Commission seeks comment on whether a central controller could provide a more efficient and effective solution than is currently available to prevent and redress malicious attack on, or mistaken use of EAS by pushing a software patch to EAS equipment that could address the issue. How could the central controller detect misuse in the nationwide EAS network? How quickly could software patches be developed and deployed? Further, the Commission seeks comment on whether the central controller could provide an additional layer of alert authentication and validation for alerts transmitted via traditional EAS alert distribution systems? Would EAS equipment be capable of performing the alert validation and authentication procedures proposed above while concurrently using the Internet to request that the central controller confirm the validation and authenticity of each message? The Commission seeks comment on the alert authentication and validation processes that should be tasked to the central controller. Further, the Commission seeks comment on whether intermittent traffic between EAS receivers and the controller, such a data traffic to transmit a software update, could be encrypted. Would such communications be as vulnerable as, if not more

vulnerable than actual EAS alerts? What encryptions techniques would be best suited for this purpose? Finally, the Commission seeks comment on whether centralized configuration and management would improve EAS' resiliency. Could a centrally configured and managed EAS system continue to function properly after a catastrophic event that, for example, limited access to the Internet, or resulted in an electromagnetic pulse? In case of such an event, could all EAS equipment continue to operate pursuant to the most recent software update issued prior to the outage until a subsequent update is received? How would this level of resiliency compare with the current PEP-reliant model?

202. Engineering Challenges. Notwithstanding the tremendous potential benefits, could implementing centralized configuration and management of EAS present complex engineering challenges for EAS stakeholders? The Commission seeks comment on the engineering challenges implicit in developing a central controller, new EAS equipment, and protocols for communication between them. Specifically, the Commission seeks comment on the hardware, operating system, and software required to maintain a central controller. Would it be necessary to maintain multiple back-up copies of the controller on a fortified or cloud-based server to be used in the event of failure or attack? The Commission also seeks comment on whether and how EAS equipment would have to be redesigned. Would every EAS encoder/decoder require an Ethernet connection in order to successfully implement centralized configuration and management? Could EAS equipment connect to the Internet wirelessly? The Commission seeks comment on the optimal method of allocating responsibility for administrative tasks among nodes in a tiered control model, including if SECCs were to be given control over alert distribution pathways in their respective states. Could a centralized configuration and management EAS network design be implemented during an interim phase during which only some EAS equipment would be connected to the central controller? Does an

Ethernet port provide the optimal method of connecting EAS equipment to the Internet? If not, what would be the ideal method?

203. The Commission seeks comment on whether centralized configuration and management would also include the development of at least three new, secure protocols. First, the Commission seeks comment on whether a secure protocol would be necessary to govern all communications between the central controller and EAS equipment. The Commission also seeks comment on whether a second secure protocol would be required to describe the master-slave relationship between the central controller and EAS receivers. Third, the Commission also seeks comment on whether a secure protocol would be required to automatically hand over control from one controller to another in the event of such an equipment failure or attack. Are there are additional protocols, equipment upgrades or engineering challenges of which the Commission should be aware?

204. Operational Issues. What operational issues might be raised by centralizing control of EAS? The Commission seeks comment on what, if any entities are well positioned to take responsibility for managing the EAS controller. Would it be preferable to have only one entity assume this role in order to ensure accountability? Would this entity also have to assume liability for interoperability, system misuse and error? Could this entity be required to finance system conversion and subsequent upgrades? Further, the Commission seeks comment on whether such a model would likely require EAS manufacturers to open their devices to receiving "push" updates. What, if any impact would "push" updates have on MVPD EAS Participants that currently do their own failure testing and regression analysis of all software updates prior to installation in order to ensure that the new software will not jeopardize the proper functionality of their system? Would EAS Participants, including such MVPDs, welcome a system of EAS governance where they could externalize the costs of failure and regression testing of EAS

software to an entity charged with managing the central controller? Further, would a centralized model require vendors to disclose their customer lists to a third party? Do EAS equipment vendors maintain customer lists that could be shared, on a confidential basis, with the appropriate entity or entities?

205. Costs. What costs would EAS stakeholders expect to result from centralizing configuration and management of EAS? Would centralized configuration and management obsolete all legacy equipment, necessitating replacement? Would the augmented capabilities and improved security, reliability and resiliency potentially offered by centralization outweigh the costs? The Commission seeks comment on any steps that it could take to help minimize these costs, particularly for small businesses.

**b. Network Function Virtualization**

206. The Commission seeks comment on the benefits of virtualization of aspects of EAS equipment or alert distribution in the context of a wider transition among EAS Participants to IP-based platforms, and cloud-based network architectures and strategies in particular. Specifically, the Commission seeks comment on the benefits of virtualizing EAS equipment, operational issues and costs implicated by implementation, and on whether virtualization should be considered in the alternative, or as a complement to centralization.

207. Benefits. Would the virtualization of EAS equipment in the context of a larger industry-wide transition to cloud-based computing bring homogeneity, consistency and reliability to the EAS computing environment by allowing software to operate independently of the underlying hardware and operating systems produced by various equipment manufacturers? Specifically, could virtualizing EAS equipment result in a completely homogenous operating environment in which every EAS node (formerly EAS equipment) would be programmed to authenticate, validate, and process EAS alerts in an identical matter, with the caveat that users

could continue to specify which event codes should be carried by their EAS nodes based on the event's relevance to the geographic area in which the node is located, and the responsibilities of the alert originator? Would such a homogenous environment lead to alerts being processed in a more consistent manner? Is it likely that such a system would more reliably ensure that alerts are delivered to all intended recipients in a secure manner?

208. Operational Issues and Costs. Would the virtualization of EAS equipment implicate costs and operational issues for EAS equipment manufacturers, EAS Participants and alert originators not already subsumed within the costs of ongoing efforts to transition business operations to the cloud? Would a virtualized EAS architecture entirely obviate physical EAS equipment used for decades as the cornerstone of EAS alert transmission? The Commission seeks comments on the costs that might be imposed by such a transition, both in terms of short term equipment replacement, and long term savings on software updates, testing, and future hardware replacement. Would EAS software updates become less complex, and therefore less costly to develop? Similarly, would a homogenous operating environment for EAS reduce EAS costs for EAS Participants associated with failure testing and implementing equipment updates? Could virtualization reduce equipment costs in the long run by obviating the need for future hardware replacement? Would virtualization reduce the need for complexity in alert origination software? Would this increased simplicity lead to EAS alerts being more consistently delivered in an accurate manner?

209. Would virtualization add value to an EAS implementation that included a central controller? The Commission seeks comment on whether the system checking function of the central controller is sufficient to achieve consistency in function without the homogeneity of form that could be created by virtualization. Are there any additional benefits to a virtualized system not captured by centralized configuration and management? Would a virtualized

approach to EAS implementation be consistent with the Commission's operating principle of technological neutrality?

### 6. Preserving EAS Defense through Planned Diversity

#### a. Ensuring a Modern and Effective EAS Structure

210. The NPRM in its background section discusses the two complementary mechanisms by which EAS messages are transmitted: (1) through the traditional, broadcast-based EAS Protocol; and (2) through the newer, Internet-based, CAP-formatted, IPAWS system. The Commission seeks comment on how stakeholders believe those two systems should relate to each other going forward. For example, does it make sense to keep the two different systems solely for resiliency considerations? Can the Commission, FEMA and other Federal partners and EAS Participants sufficiently secure the broadcast-based EAS to achieve appropriate levels of resiliency and to ensure that this EAS path does not expose EAS more generally to undue security risks? Are the failure modes of the two paths sufficiently different to suggest an enduring unique value from both elements? Does a sufficient number of EAS Participants, particularly in rural and other underserved areas have the internet access or other technologies necessary to participate in the CAP-formatted system? Ultimately, does it make sense to migrate to one system? If so, over what time period? What should that new system look like? Would purely internet-based systems be overly reliant on the need for strong cybersecurity?

211. Are stakeholders confused or is there any inefficiencies the Commission should be aware of because there are two systems? Also, given the ways in which communications have changed since the EAS and its predecessor system was introduced, e.g., the introduction of social media alerts, WEA mobile alerts, and other technical innovations, does the Commission have an alerting system that is appropriate and tailored to today's communications landscape, both in terms of the technology in use and anticipated and in terms of the usage and

communication patterns of today's public? If not, does the Commission need a wholesale re-thinking of the alerting system or is the current system sufficiently flexible that the Commission can evolve it over time so that it remains appropriate in light of today's technology, usage patterns and emerging security threats?

### b. Securing the EAS Broadband Architecture

212. The current adoption of IPAWS-OPEN as a delivery method of alerts to all EAS participants in accordance with the Commission's requirements in the Fifth Report and Order, as well as its use in WEA, have increased the dependence of the EAS and related systems on broadband (i.e., IP) networks. This migration will entail a shift from the legacy environment for EAS which was marked by physical route diversity. The nature of IP systems, however, will not reproduce this security element; indeed, several of the proposals above depend on movement toward centralized management and virtualization, which involve significant dependence on IP that, in turn, will require highly reliable, redundant, and secure Internet connectivity to mimic the security that physical diversity in the legacy EAS network currently provides. The Commission seeks comment on the nature and extent to which new alerting technologies will create such dependencies. What methods of securing the EAS would best maintain at least an equivalent level of redundancy and security as the legacy daisy chain presently provides? What additional considerations does this shift require the Commission to take into account when testing the EAS system? Do existing and planned test strategies adequately cover all redundant paths used to disseminate the alert? As the Commission continues the focus on the IPAWS-OPEN path, does it risk less frequent use of the legacy broadcast paths? If so, what are the implications for seamless operation of legacy paths and the resiliency of the entire system, and how can the Commission mitigate any deficiencies that may arise from any reduced dependability?

213. Given the importance of physical security in maintaining the integrity of the EAS

system, what additional measures may be necessary to ensure access to EAS devices and the IP network that feeds them are protected from malicious damage or compromise? Are the existing practices and continuity of operation plans sufficient to ensure reliable delivery of EAS alerts to the public? What additional levels of redundant paths, equipment, power, and other services should be required to ensure operation? For example, in addition to the security measures proposed earlier in Section III(D)(2), what other methods could the Commission use to prevent IP-based attacks from compromising the EAS system? Should the Commission maintain a secondary broadcast EAS system based on legacy EAS in addition to and separate from the IPAWS-OPEN-based system?

### E. Compliance Timeframes

214. The Commission seeks comment on the timeframes in which the proposals in this NPRM, if adopted, could reasonably be implemented by EAS Participants. As discussed in greater detail below, the Commission proposes that EAS Participants must comply with its proposed rules that include new information collection requirements (i.e., the State EAS Plan rules, initial annual security certification, and security incident reporting requirements) within six months from the release of a Public Notice announcing Office of Management and Budget (OMB) approval of related information collection requirements, or within 60 days of a Public Notice announcing the availability of the Commission's relevant database to receive such information, whichever is later; with subsequent annual certifications due by June 30th of each calendar year. The Commission proposes that EAS Participants must comply with proposed alert authentication and validation measures within one year of the rules' publication in the Federal Register. The Commission notes that no action is required to comply with its live code test and PSA rules, and encourages EAS Participants to begin engaging in testing and outreach efforts pursuant to those rule amendments as soon as those rules become effective, thirty days

from the date those rules are published in the Federal Register. The Commission seeks comment on whether this framework appropriately balances the burdens of compliance with the need for rapid improvement of EAS organization, testing, outreach, and security. For ease of reference and comment, Figure 2, below, sets forth proposed timeframes for those instances where the Commission proposes specific implementation deadlines.

| PROPOSED RULE AMENDMENTS | PROPOSED COMPLIANCE TIMEFRAMES |
|---|---|
| **EAS Designations** | Rules would be effective within 30 days of publication in the Federal Register |
| **State EAS Plan Contents** | Within six months of release of a Public Notice announcing OMB approval of related information collection requirements, or within 60 days of release of a Public Notice announcing the availability of SEPFI to receive State EAS Plans, whichever is later |
| **Live Code Tests** | No action required; rules would be effective within 30 days of publication in the Federal Register |
| **EAS PSAs** | No action required; rules would be effective within 30 days of publication in the Federal Register |
| **Annual Certification** | For the first certification: within six months of the release of a Public Notice announcing OMB approval of related information collection requirements, or within 60 days of release of a Public Notice announcing the availability of ETRS to receive such reports, whichever is later.<br>For subsequent annual certifications: by June 30th of each calendar year. |
| **Reporting False Alerts and Lockouts** | Within six months of the release of a Public Notice announcing OMB approval of related information collection requirements, or within 60 days of release of a Public Notice announcing the availability of ETRS to receive such reports, whichever is later |
| **Authentication and Validation Measures** | Within 1 year of the rules' publication in the Federal Register |

Figure 2**:** Proposed Implementation Timeframes

215. State EAS Plan Rules. The Commission proposes that the new EAS Designations would take effect 30 days from the publication of final rules in the Federal Register, and to

require compliance with the Commission's State EAS Plan rules within six months of the release of a Public Notice announcing OMB approval of related information collection requirements, or within 60 days of release of a Public Notice announcing the availability of SEPFI to receive State EAS Plans, whichever is later. States should already have State EAS Plans in place, and the Commission's proposed rules would not require that states adopt any particular alerting strategy or necessitate any changes in alerting implementation. The Commission does not anticipate, however, that producing State EAS Plans that include the new elements the Commission proposes would require additional discussion, strategic planning, and outreach. This discussion may entail a rigorous assessment of state preparedness along the axes discussed above. For example, SECCs may need to perform outreach in order to ascertain the extent to which EAS Participants in their state are using alternative alerting mechanisms such as the satellite-based monitoring sources, highway signs or social media, and the extent to which they are prepared to leverage available technologies to implement "one-to-many, many-to-one" alerting. SECCs may also need to engage with key EAS sources in their state in order to aptly apply the Commission's proposed EAS Designations. The Commission seeks comment on whether requiring compliance with its proposed State EAS Plan rules within this proposed timeframe would provide SECCs with sufficient time to complete any required strategic planning, discussion and outreach necessitated by these proposed rules. Commenters are encouraged to specify an alternative timeline if compliance within six months is considered infeasible, or if compliance can be achieved earlier.

216. Alert Authentication and Validation Rules. The Commission proposes that EAS Participants should be required to comply with its alert authentication and validation rules within one year of the date of their publication in the Federal Register. In the Sixth Report and Order, the Commission provided EAS Participants one year to develop, test, and deploy any necessary

software updates to support the national location code and National Periodic Test (NPT) code, and to replace any EAS equipment that no was no longer supported by the manufacturer. The Commission seeks comment on whether the changes that may be necessitated by its proposed alert validation and authentication requirements may be accomplished through a software update, and reason similarly that EAS Participants may be expected to develop, deploy and test any required software updates within a year's timeframe. Alternatively, could compliance with some or all of the proposed rules be satisfied within a shorter timeframe? Given the importance to the nation's safety of securing the EAS, the Commission seeks comment on the shortest practicable amount of time in which these measures could be implemented. To the extent an alternative timeframe would be more appropriate, the Commission asks commenters to provide a detailed explanation.

217. Security Incident Reporting and Annual Security Certification. The Commission proposes to require initial compliance with its security incident reporting and annual security certification requirements within six months of the release of a Public Notice announcing OMB approval of related information collection requirements, or within 60 days of release of a Public Notice announcing that ETRS is capable of receiving such reports, whichever is later. With respect to subsequent annual certifications, the Commission proposes that this timeframe apply to the first certification, with subsequent certifications due by June 30 of each calendar year. The Commission expects that EAS Participants are already complying with most, if not all, of the best practices described above, and to the extent additional time is necessary to ensure that best practices are fully implemented, the Commission believes that 60 days provides a reasonable timeframe to accomplish that goal while also ensuring that security measures are taken as swiftly as possible. The Commission seeks comment on this proposed timeframe, and on its rationale.

218. Live Code Tests and EAS PSAs. The Commission proposes that its live code

testing and PSA rules would become effective thirty days from the date of their publication in the Federal Register. The Commission observes that no action is required in order for EAS Participants to comply with these proposed rules. Further, in the meantime, EAS Participants may continue to conduct live code tests as regularly scheduled pursuant to the guidance the Bureau provided in the Live Code Testing Public Notice. This proposed rule, if adopted, would alleviate the burden on EAS Participants to seek waiver of the Commission's rules in order to engage in this common practice. With respect to EAS PSAs, the Commission proposes to expand the set of entities that are permitted to conduct EAS PSAs, and to allow them to include the EAS header codes and Attention Signal. This proposed rule, if adopted, would allow EAS PSAs to become more flexible tools for community public safety outreach. The Commission believes it would serve the public interest for the proposed live code testing and PSA rules to become effective as soon as possible, and seeks comment on its rationale.

### F. Legal Authority

219. Under the Communications Act of 1934, as amended (Act), the Commission was established, among other things, to "make available rapid, efficient . . . wire and radio communication service with adequate facilities . . . for the purpose of the national defense" and "for the purpose of promoting safety of life and property." The Commission's regulation of emergency broadcasting, both of the EBS and EAS, has been grounded, in significant part, in Sections 1, 4(i) and (o), 303(r), and 706 of the Act. Additionally, the Commission has authority to impose EAS obligations on cable systems under Section 624(g) of the Act, regulate participation by Commercial Mobile Service in the emergency alerting process under the WARN Act, and to ensure that emergency information is accessible under the Twenty-First Century Communications and Video Accessibility Act.

220. In order to enable the President to reliably execute this authority in the public

interest, the Commission has long considered it necessary to ensure that the Commission's national alerting architecture is ready to transmit an alert authorized by the President (i.e., a Presidential Alert) in an appropriate situation. Further, the President has defined roles and responsibilities for federal agencies to create a "comprehensive system to alert and warn the American people" in several executive documents, specifically directing the Commission to "adopt rules to ensure that communications systems have the capacity to transmit alerts and warnings to the public as part of the public alert and warning system." The Commission seeks comment on whether this legal authority extends to mobile apps when offered by a covered entity.

221. In addition to the authorities discussed above, the Commission believes it has authority to adopt alert authentication and validation rules, require security certifications, and collect false alert and lockout reports from EAS Participants. First, the Commission has express authority under Title III to make changes to alert authentication and validation and to require EAS security certifications from Title III licensees. Title III directs the Commission to "maintain the control of the United States over all channels of radio transmission" and charges the Commission with protecting the viability of local broadcasting. Section 303 of the Act states that the Commission shall "[p]rescribe the nature of the service to be rendered by each class of licensed stations" where public convenience, interest, or necessity requires and encourage the effective use of radio in the public interest. Further, the Act prohibits the transmission or rebroadcast of "false distress signals," a prohibition that includes false or fraudulent EAS alerts. Finally, the Commission believes that its authority to assure that the EAS is delivered in a secure fashion extends to requiring EAS Participants to provide reports that would allow the Commission to investigate, study, and be aware of any potential issues that may preclude the secure and reliable transmission of the EAN. Fraudulent EAS alerts create widespread public

confusion and even panic. The Commission seeks comment on its authority under all the foregoing provisions discussed in this section to adopt the proposals in this NPRM, all of which are primarily intended to prepare the nation's alerting infrastructure for successful transmission of a Presidential Alert. The Commission also seeks comment on whether there are other sources of legal authority for the Commission to enact these rules. To the extent commenters believe that additional sources of authority would be necessary or relevant to allowing the Commission to address commenters' concerns, the Commission encourages commenters to offer additional sources of authority on which it may rely for this purpose.

## III. PROCEDURAL MATTERS

### A. Ex Parte Rules

222. The proceeding initiated by this Notice of Proposed Rulemaking shall be treated as "permit-but-disclose" proceedings in accordance with the Commission's ex parte rules. 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.

### B. Comment Filing Procedures

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

- Electronic Filers: Comments may be filed electronically using the Internet by accessing the ECFS: http://apps.fcc.gov/ecfs/.
- Paper Filers: Parties that choose to file by paper must file an original and one copy of each filing. If more than one docket or rulemaking number appears in the caption of this proceeding, filers must submit two additional copies for each additional docket or rulemaking number.

  Filings can be sent by hand or messenger delivery, by commercial overnight courier, or by first-class or overnight U.S. Postal Service mail. All filings must be addressed to the Commission's Secretary, Office of the Secretary, Federal Communications Commission.

  1. All hand-delivered or messenger-delivered paper filings for the Commission's Secretary must be delivered to FCC Headquarters at 445 12th St., SW, Room TW-A325, Washington, DC 20554. The filing hours are 8:00 a.m. to 7:00 p.m. All

hand deliveries must be held together with rubber bands or fasteners. Any envelopes and boxes must be disposed of before entering the building.

2. Commercial overnight mail (other than U.S. Postal Service Express Mail and Priority Mail) must be sent to 9300 East Hampton Drive, Capitol Heights, MD 20743.

3. U.S. Postal Service first-class, Express, and Priority mail must be addressed to 445 12th Street, SW, Washington DC 20554.

224. 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), 202-418-0432 (TTY).

### C. Regulatory Flexibility Analysis

225. As required by the Regulatory Flexibility Act of 1980, see 5 U.S.C. § 604, the Commission has prepared an Initial Regulatory Flexibility Analysis (IRFA) of the possible significant economic impact on small entities of the policies and rules addressed in this document. The IRFA is set forth in Appendix B. Written public comments are requested in the IRFA. These comments must be filed in accordance with the same filing deadlines as comments filed in response to this Notice of Proposed Rulemaking as set forth on the first page of this document, and have a separate and distinct heading designating them as responses to the IRFA.

### D. Paperwork Reduction Analysis

226. This document contains 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 this document, 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.

## IV. ORDERING CLAUSES

227. Accordingly, IT IS ORDERED that pursuant to 47 U.S.C §§ 151, 152, 154(i), 154(o), 301, 303(b), (g) and (r), 303(v), 307, 309, 335, 403, 544(g), 606, 613, 615 and 1302; The Warning, Alert and Response Network (WARN) Act, WARN Act §§ 602(a), (b), (c), (d), (f), 603, 604, and 606; Twenty-First Century Communications and Video Accessibility Act of 2010, Pub. L. No. 111-260 and Pub. L. No. 111-265, this Notice of Proposed Rulemaking IS hereby ADOPTED.

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

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

**List of Subjects**

47 CFR Part 11

Radio, Television, Emergency alerting.

For the reasons discussed in the preamble, the Federal Communications Commission proposes to amend 47 CFR part 11 to read as follows:

**PART 11 – EMERGENCY ALERT SYSTEM (EAS)**

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

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

2. Revise § 11.2 to read as follows:

**§ 11.2 Definitions.**

The definitions of terms used in part 11 are:

(a) Emergency Action Notification (EAN). The Emergency Action Notification is the notice to all EAS Participants and to the general public that the EAS has been activated for a national emergency. EAN messages that are formatted in the EAS Protocol (specified in §11.31) are sent from a government origination point to broadcast stations and other entities participating in the PEP system, and are subsequently disseminated via EAS Participants. Dissemination arrangements for EAN messages that are formatted in the EAS Protocol (specified in §11.31) at the State and local levels are specified in the State and Local Area plans (defined at §11.21). A national activation of the EAS for a Presidential message with the Event code EAN as specified in §11.31 must take priority over any other message and preempt it if it is in progress.

(b) EAS Participants. Entities required under the Commission's rules to comply with EAS rules, e.g., analog radio and television stations, and wired and wireless cable television systems, DBS, DTV, SDARS, digital cable and DAB, and wireline video systems.

(c) Wireline Video System. The system of a wireline common carrier used to provide video programming service.

(d) Intermediary Device. An intermediary device is a stand-alone device that carries out the functions of monitoring for, receiving and/or acquiring, and decoding EAS messages formatted in the Common Alerting Protocol (CAP) in accordance with §11.56, and converting such messages into a format that can be inputted into a separate EAS decoder, EAS encoder, or unit combining such decoder and encoder functions, so that the EAS message outputted by such separate EAS decoder, EAS encoder, or unit combining such decoder and encoder functions, and all other functions attendant to processing such EAS message, comply with the requirements in this part.

3. Revise § 11.18 to read as follows:

**§ 11.18 EAS Designations.**

(a) The Primary Entry Point System is a nationwide network of broadcast stations and other entities connected with government activation points. It is used to distribute EAS messages that are formatted in the EAS Protocol (specified in §11.31), including the EAN and EAS national test messages. FEMA has designated some of the nation's largest radio broadcast stations as PEPs. The PEPs are designated to receive the Presidential alert from FEMA and distribute it to local stations.

(b) A National Primary (NP) is the entity tasked with the primary responsibility of delivering the

Presidential alert to a state's EAS Participants. Thus, for a state that has a FEMA-designated PEP, that station would be designated as that state's National Primary. For a state that does not have a PEP, another station would act as National Primary.

(c) A State Primary (SP) is an entity tasked with initiating the delivery of a state EAS alert. A State Primary may be a broadcaster, a state emergency management office, or other entity authorized to and capable of initiating a state-based EAS alert. A State Primary and a National Primary may be the same broadcaster, but would need to be separately designated as such in any State EAS Plan.

(d) A Relay Station (RS) retransmits EAS messages, including the Presidential Alert and state and local alerts, to Local Primary (LP) sources for distribution to Participation National sources, and the public, as necessary.

(e) A Local Primary (LP) serves as a monitoring assignment for a Participating National (PN) entity. An LP source is responsible for coordinating the carriage of common emergency messages from sources such as the National Weather Service or local emergency management offices as specified in its State EAS Plan. If it is unable to carry out this function, other LP sources in the Local Area may be assigned the responsibility as indicated in State EAS Plans. LP sources are assigned numbers (LP-1, 2, 3, <u>etc</u>.) in the sequence they are to be monitored by other broadcast stations in the Local Area.

(f) Participating National (PN) entities transmit EAS National, State or Local Area messages. The EAS transmissions of PN sources are intended for direct public reception.

4. Revise § 11.21 to read as follows:

**<u>§ 11.21 State and Local Area plans and FCC Mapbook.</u>**

(a) EAS plans contain guidelines which must be followed by EAS Participants' personnel, emergency officials, and National Weather Service (NWS) personnel to activate the EAS. The plans include the following elements:

(1) A list of the EAS header codes and messages that will be transmitted by key EAS sources (National Primary (NP), State Primary (SP), Local Primary (LP), and State Relay (SR) stations);

(2) Procedures for state emergency management officials, the National Weather Service, and EAS Participant personnel to transmit emergency information to the public during an emergency using regulated alerting tools (e.g., EAS and WEA) as well as any non-regulated alerting mechanisms (e.g., highway signs, social media), including the extent to which the state's dissemination strategy for state and local emergency alerts differs from their Presidential Alerting strategy;

(3) A list of all entities authorized to activate EAS for state and local emergency messages (e.g., Police and Public Safety Answering Points (PSAPs)), whose transmissions might be interrupted by a Presidential Alert;

(4) Monitoring assignments to receive the Presidential Alert, and the primary and back-up paths for the dissemination of the Presidential Alert to all key EAS sources organized by operational areas within the state;

(5) State procedures for special EAS tests, Required Monthly Tests (RMTs), Required Weekly Tests (RWTs) and national tests designed to ensure that the system will function as designed when needed for a Presidential Alert, including a description of the extent to which State and Local WEA Tests are utilized by alert originators as a complement to the Presidential Alert distribution system to verify that WEA is capable of informing the public that a Presidential

Alert is presently being delivered over EAS;

(6) The extent to which alert originators coordinate "one-to-many" alerts with "many-to-one" community feedback mechanisms, such as 9-1-1, to make full use of public safety resources;

(7) Specific and detailed information describing the procedures for ensuring EAS Participants can authenticate the current assigned state, local and tribal originators, if the state initiates EAS messages formatted in the Common Alerting Protocol (CAP) signed with a digital signature as specified in the Organization for the Advancement of Structured Information Standards (OASIS) Common Alerting Protocol Version 1.2 (July 1, 2010), its EAS State Plan; and

(8) The SECC governance structure utilized by the state in order to organize state and local resources to ensure the efficient and effective delivery of a Presidential Alert, including the duties of SECCs, the membership selection process utilized by the SECC, and the proposed administration of the SECCs.

(b) The Local Area plan contains procedures for local officials or the NWS to transmit emergency information to the public during a local emergency using the EAS. Local plans may be a part of the State plan. A Local Area is a geographical area of contiguous communities or counties that may include more than one state.

(c) The FCC Mapbook is based on the consolidation of the data table required in each State EAS plan with the identifying data contained in the ETRS. The Mapbook organizes all EAS Participants according to their State, EAS Local Area, and EAS designation. EAS Participant monitoring assignments and EAS operations must be implemented in a manner consistent with guidelines established in a State EAS Plan submitted to the Commission in order for the Mapbook to accurately reflect actual alert distribution.

5. Revise paragraph (c) of § 11.31 to read as follows:

**§ 11.31 EAS protocol.**

* * * * *

(c) The EAS protocol, including any codes, must not be amended, extended or abridged without FCC authorization. The EAS protocol and message format are specified in the following representation.

Examples are provided in FCC Public Notices.

[PREAMBLE]ZCZC-ORG-EEE-PSSCCC+TTTT-YYYYJJJHHMM-

LLLLLLLL-(one second pause)

[PREAMBLE]ZCZC-ORG-EEE-PSSCCC+TTTT-YYYYJJJHHMM-

LLLLLLLL-(one second pause)

[PREAMBLE]ZCZC-ORG-EEE-PSSCCC+TTTT-YYYYJJJHHMM-

LLLLLLLL-(at least a one second pause)

(transmission of 8 to 25 seconds of Attention Signal)

(transmission of audio, video or text messages)

(at least a one second pause)

[PREAMBLE]NNNN (one second pause)

[PREAMBLE]NNNN (one second pause)

[PREAMBLE]NNNN (at least one second pause)

[PREAMBLE] This is a consecutive string of bits (sixteen bytes of AB hexadecimal [8 bit byte 10101011]) sent to clear the system, set AGC and set asynchronous decoder clocking cycles. The preamble must be transmitted before each header and End of Message code.

ZCZC—This is the identifier, sent as ASCII characters ZCZC to indicate the start of ASCII code.

ORG—This is the Originator code and indicates who originally initiated the activation of the EAS. These codes are specified in paragraph (d) of this section.

EEE—This is the Event code and indicates the nature of the EAS activation. The codes are specified in paragraph (e) of this section. The Event codes must be compatible with the codes used by the NWS Weather Radio Specific Area Message Encoder (WRSAME).

PSSCCC—This is the Location code and indicates the geographic area affected by the EAS alert. There may be 31 Location codes in an EAS alert. The Location code uses the codes described in the American National Standards Institute (ANSI) standard, ANSI INCITS 31-2009 ("Information technology—Codes for the Identification of Counties and Equivalent Areas of the United States, Puerto Rico, and the Insular Areas"). Each state is assigned an SS number as specified in paragraph (f) of this section. Each county and some cities are assigned a CCC number. A CCC number of 000 refers to an entire State or Territory. P defines county subdivisions as follows: 0 = all or an unspecified portion of a county, 1 = Northwest, 2 = North, 3 = Northeast, 4 = West, 5 = Central, 6 = East, 7 = Southwest, 8 = South, 9 = Southeast. Other numbers may be designated later for special applications. The use of county subdivisions will probably be rare and generally for oddly shaped or unusually large counties. Any subdivisions must be defined and agreed to by the local officials prior to use.

+ TTTT—This indicates the valid time period of a message in 15 minute

segments up to one hour and then in 30 minute segments beyond one hour; i.e., + 0015, + 0030, + 0045, + 0100, + 0430 and + 0600.

YYYYJJJHHMM—This is the year (YYYY), day in Julian Calendar days (JJJ) of the year and the time in hours and minutes (HHMM) when the message was initially released by the originator using 24 hour Universal Coordinated Time (UTC).

LLLLLLLL—This is the PSID identification of the EAS Participant, NWS office, etc., transmitting or retransmitting the message. These codes will be automatically affixed to all outgoing messages by the EAS encoder.

NNNN—This is the End of Message (EOM) code sent as a string of four ASCII N characters.

* * * * *

6. Amend § 11.32 by revising paragraph (a)(5) to read as follows:

**§ 11.32 EAS Encoder.**

(a) * * *

(5) Day-Hour-Minute and Identification Stamps. The encoder shall affix the YYYYJJJHHMM and LLLLLLLL codes automatically to all initial messages.

* * * * *

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

**§ 11.33 EAS Decoder.**

(a) * * *

(10) Message Validity. An EAS Decoder must provide error detection and validation of the

header codes of each message to ascertain if the message is valid. Header code comparisons may be accomplished through the use of a bit-by-bit compare or any other error detection and validation protocol. A header code must only be considered valid when two of the three headers match exactly, the Station ID header code matches one of the assigned monitoring sources as specified in the state plan and the expiration time is in the future. Duplicate messages must not be relayed automatically.

* * * * *

8. Add § 11.44 to subpart C to read as follows:

**§ 11.44 Security of EAS Participants.**

(a) Definitions. Terms in this section shall have the following meanings:

(1) Certification. An attestation by a Certifying Official, under penalty of perjury, that an EAS Participant:

(i) Has satisfied the obligations of subsection (b) of this section.

(ii) Has adequate internal controls to bring material information regarding network architecture, operations, and maintenance to the Certifying Official's attention.

(iii) Has made the Certifying Official aware of all material information reasonably necessary to complete the certification.

(2) Certifying Official. A corporate officer of an EAS Participant with supervisory and budgetary authority over network operations in all relevant service areas.

(3) Segmentation. A category of best practice actions for certification purposes that logically group and compartmentalize assets and restrict trusted access to those compartments.

(b) Annual EAS Security Certification. The identifying information required by the ETRS as

specified in §11.61(a)(3)(iv) shall include a Certification to the Commission by a Certifying Official of every EAS Participant as follows.

(1) Patch Management.

(i) An EAS Participant shall certify whether it has, within the past year:

(A) Followed a program to identify and install updates and patches to EAS devices and attached systems in a timely manner;

(B) Verified EAS devices are running the current version and patch level of software and firmware; and

(C) Verified systems connected to EAS devices are running the current version and patch level of software and firmware.

(ii) If an EAS Participant does not conform with the elements in paragraph (b)(1)(i) of this section it must certify:

(A) Whether it has taken alternative measures or remediation to meet or exceed the security provided by the current version and patch level, in which case it shall provide a brief explanation of such alternative measures or such remediation steps, the date by which it anticipates such remediation will be completed, and why it believes those measures are reasonably sufficient to mitigate such risk; or

(B) Whether it believes that one or more of the requirements of this paragraph are not applicable to its network, in which case it shall provide a brief explanation of why it believes any such requirement does not apply.

(2) Account Management.

(i) An EAS Participant shall certify that:

(A) All EAS device and connected system passwords have been changed from the default;

(B) Where passwords are used, password complexity is required; and

(C) Default, unnecessary, and expired accounts have been removed or disabled.

(ii) If an EAS Participant does not conform with all of the elements in paragraph (b)(2)(i) of this section, it must certify:

(A) Whether it has taken alternative measures to mitigate the risk of a unauthorized access or is taking steps to remediate any issues it has identified in complying with the above elements, in which case it shall provide a brief explanation of such alternative measures or such remediation steps, the date by which it anticipates such remediation will be completed, and why it believes those measures are reasonably sufficient to mitigate such risk; or

(B) Whether it believes that one or more of the requirements of this paragraph are not applicable to its network, in which case it shall provide a brief explanation of why it believes any such requirement does not apply.

(3) Segmentation.

(i) An EAS Participant shall certify that:

(A) All of its EAS devices are not directly accessible from the Internet; and

(B) If remote access to EAS devices is required, such access is properly logged and secured in accordance with industry best practices.

(ii) If an EAS Participant does not conform with all of the elements in paragraph (c)(3)(i) of this section, it must certify whether it believes that one or more of the requirements of this paragraph are not applicable to its network, in which case it shall provide an explanation of why it believes any such requirement does not apply.

(4) CAP Digital Signature Validation. An EAS Participant shall certify that EAS devices are configured to validate digital signatures on CAP messages if the source of the CAP message includes this feature.

(c) Other Matters.

(1) Confidential Treatment.

(i) The fact of filing or not filing an Annual EAS Security Certification and the responses on the face of such certification forms shall not be treated as confidential.

(ii) Information submitted with or in addition to such Certifications shall be presumed confidential to the extent that it consists of descriptions and documentation of alternative measures to mitigate the risks of nonconformance with certification elements, information detailing specific corrective actions taken with respect to certification elements, or supplemental information requested by the Commission or Bureau with respect to a certification.

(2) [Reserved]

9. Revise § 11.45 to read as follows:

**§ 11.45 Prohibition of false or deceptive EAS transmissions.**

(a) No person may transmit or cause to transmit the EAS codes or Attention Signal, or a

recording or simulation thereof, in any circumstance other than in an actual National, State or Local Area emergency or authorized test of the EAS; or as specified in §§11.46 and 11.61.

(b) All EAS Participants shall submit electronically a Notification to the Commission via ETRS:

(1) An initial report within 30 minutes of discovering the transmission of a false EAS alert by their station. The report shall include the time discovered, transmitted EAS alert fields, message source, and area covered by the transmission.

(2) An initial report within 15 minutes of discovering that EAS Participant equipment causes, contributes to, or participates in a lockout that adversely affects the public. The report shall include the time discovered, message source, and affected devices.

(3) Not later than 72 hours after discovering the event, the EAS Participant shall submit a final report to the Commission describing the root cause of the event, number of affected customers, and mitigation steps taken.

(c) Confidential Treatment.

(1) The fact of filing or not filing a false EAS alert report shall not be treated as confidential.

(2) Information submitted with or in addition to such reports shall be presumed confidential to the extent that it consists of descriptions and documentation of proprietary company information, root causes, or supplemental information requested by the Commission or Bureau with respect to an incident.

10. Revise § 11.46 to read as follows:

**§ 11.46 EAS code and Attention Signal Monitoring requirements.**

Public Service Announcements and commercially-sponsored announcements, infomercials, or

programs may be used to explain the EAS to the public, provided that the entity using the codes and Attention Signal presents them in a non-misleading and technically harmless manner.

11. Amend § 11.52 by revising paragraph (d)(1) and removing paragraph (d)(3), and redesignating paragraphs (d)(4) and (d)(5) as (d)(3) and (d)(4), respectively. The revision to read as follows:

**§ 11.52 EAS code and Attention Signal Monitoring requirements.**

* * * * *

(d) EAS Participants must comply with the following monitoring requirements:

(1) With respect to monitoring for EAS messages that are formatted in accordance with the EAS Protocol, EAS Participants must monitor two EAS sources.

* * * * *

12. Amend § 11.54 by revising paragraph (a) introductory text and paragraph (a)(1) to read as follows:

**§ 11.54 EAS operation during a National Level emergency.**

(a) Immediately upon receipt of a valid EAN message, or the NPT Event code in the case of a nationwide test of the EAS, EAS Participants must comply with the following requirements, as applicable:

(1) Analog and digital broadcast stations may transmit their call letters and analog cable systems, digital cable systems and wireless cable systems may transmit the names of the

communities they serve during an EAS activation.

* * * * *

**§ 11.55 [Amended].**

13. Amend § 11.55 by removing paragraph (b) and redesignating paragraphs (c) and (d) as paragraphs (b) and (c).

14. Amend § 11.56 by redesignating paragraph (c) as paragraph (d) and adding a new paragraph (c) to read as follows:

**§11.56 Obligation to process CAP-formatted EAS messages.**

* * * * *

(c) EAS Participants shall configure their systems to treat as invalid all CAP-formatted EAS messages that include a digital signature that does not match an authorized source from FEMA or from a designated source as specified in the state EAS plan.

15. Amend § 11.61 by revising paragraphs (a)(3)(iv)(A) and adding (a)(5) to read as follows:

**§11.61 Tests of EAS procedures.**

(a) * * * * *

(3) * * *

(iv) * * *

(A) EAS Participants shall provide the identifying information required by the ETRS initially no later than sixty days after the publication in the Federal Register of a notice announcing the approval by the Office of Management and Budget of the modified information collection

requirements under the Paperwork Reduction Act of 1995 and an effective date of the rule amendment, or within sixty days of the launch of the ETRS, whichever is later, and shall renew this identifying information on a yearly basis.

* * * * *

(5) Live Code Tests. Live Code Tests may be conducted to exercise the EAS and raise public awareness, provided that the entity conducting the test:

(i) Provides notification in accessible formats during the test (e.g., audio voiceovers, video crawls as described in § 11.51) to make sure the public understands that the test is not, in fact, warning about an actual emergency;

(ii) Engages in outreach pre-test to coordinates among EAS Participants and with state and local emergency authorities, as well as first responder organizations (e.g., Public Safety Answering Points (PSAPs)), police and fire agencies, and the public in order to notify them that live event codes will be used, but that no emergency is in fact occurring.

* * * * *

[FR Doc. 2016-05275 Filed: 3/23/2016 8:45 am; Publication Date: 3/24/2016]