PUBLIC NOTICE

Federal Communications Commission
445 12th St., S.W.
Washington, D.C. 20554

News Media Information 202 / 418-0500
Internet: http://www.fcc.gov
TTY: 1-888-835-5322

DA 14-1626
Released: November 7, 2014

PSHSB ISSUES ADVISORY TO EAS PARTICIPANTS TO CHECK EQUIPMENT FOR POSSIBLE QUEUING OF UNAUTHORIZED EAS MESSAGE FOR FUTURE TRANSMISSION; REQUESTS COMMENT ON IMPACT OF UNAUTHORIZED EAS ALERTS AND ANNOUNCES INQUIRY INTO CIRCUMSTANCES OF RETRANSMISSION OF UNAUTHORIZED EAS MESSAGE IN SEVERAL STATES

PS Docket No. 14-200

Comment date: December 5, 2014
Reply date: December 19, 2014

On October 24, 2014 at 8:21 a.m., Eastern Daylight Time, an unauthorized Emergency Alert System (EAS) message was transmitted in several states. The incident occurred when a syndicated radio broadcast inappropriately transmitted a recording of an EAS alert with an Emergency Action Notification (EAN) event code. EAN codes are used to automatically interrupt programming for a message from the President of the United States to alert the public of a national emergency.[1] EAS alerts with an EAN event code are designed to be automatically received and retransmitted by EAS Participants, but in this case, use of the EAN was unauthorized and caused public confusion and inconvenience for consumers in those states.[2] This incident did not involve the Federal Emergency Management Agency's (FEMA) Integrated Public Alert and Warning System (IPAWS), but affected only the commercial service provider side of the EAS. This Public Notice seeks comment on how unauthorized EAS alerts, including this EAN incident, affect EAS Participants, public safety and other government and local agencies, as well as the public. We also request comment on ways EAS Participants and EAS equipment can improve message authentication going forward.

Advisory: Possible False Alert Queued for Future Date

The EAN alert message that was erroneously transmitted on October 24, 2014 had a date/time-stamp for a future date. Based on discussions with EAS equipment manufacturers and other EAS stakeholders, it is possible that some EAS equipment that did not broadcast the message on October 24,

[1] *See* 47 C.F.R. § 11.2(a).

[2] *See* 47 C.F.R. § 11.2(d) (including broadcast stations, cable systems, wireline video systems, wireless cable systems, Direct Broadcast Satellite (DBS) Services and Satellite Digital Audio Radio Services among the entities required to comply with the Commission's EAS Rules, and defining them as "EAS Participants").

2014, queued it for transmission on a future date.[3] The Public Safety and Homeland Security Bureau (PSHSB or Bureau) advises EAS Participants to immediately check with their equipment manufacturers to determine if they have this alert in queue for a future date, and if so, what steps they should take to eliminate the false alert before it is transmitted.[4]

PSHSB Inquiry

Participation in the national EAS is mandatory for EAS Participants. The purpose of the EAS is to provide timely and accurate alerts and warnings so that members of the public may act quickly to protect themselves and their families.[5] Thus, any false EAS alert undermines the reliability of the system. The Commission is working with Federal government partners,[6] state and local governments, EAS Participants, and EAS equipment manufacturers to enhance the security, integrity and reliability of the EAS. Accordingly, the Bureau, in coordination with FEMA and DHS, is commencing this inquiry into the technical, operational and policy implications of this incident. PSHSB has opened a public docket and invites members of the public to file comments on the effects and implications of this incident as they relate to the efficacy and improved operation of the EAS.[7] In particular, PSHSB is interested in receiving comment on the following questions:

- *Impact to EAS Participants.*
  - To what extent have EAS Participants been directly affected by unauthorized EAS alerts, including unauthorized EANs? To what extent have National Primary and Local Primary EAS Participants been affected by unauthorized alerts? To what extent have Participating National EAS Participants been affected, and in which specific service areas? To the extent EAS Participants have received unauthorized EAS alerts, how has EAS equipment responded?
  - Is there a difference in whether or how an unauthorized EAN or other EAS alert is received and transmitted among different types of EAS Participants (*i.e.*, broadcast versus cable versus other types of EAS Participants)? How does EAS equipment handle the absence of an End of Message (EOM) code?

[3] *See*, *e.g.*, MONROE ELECTRONICS, INC., DIGITAL ALERT SYSTEMS, CANCELLING UNAUTHORIZED EAN QUEUED EVENT (2014), *available at* http://www.digitalalertsystems.com/pdf/DAS%20FSB-103014R1.0.pdf (last visited Nov. 4, 2014).

[4] *Id*.

[5] *See* 47 C.F.R. § 11.1. The Commission was established for "purposes of, among other things, the national defense and the promotion of safety of life and property through the regulation of wire and radio communications networks. *See* Section 1 of the Communications Act of 1934 (as amended), 47 U.S.C § 151; *see also* Review of the Emergency Alert System; Independent Spanish Broadcasters Association, The Office of Communication of the United Church of Christ, Inc., and the Minority Media and Telecommunications Council, Petition for Immediate Relief, EB Docket No. 04-296*, Fifth Report and Order*, 27 FCC Rcd 642, 644, ¶ 2 (2012) (stating that modernizing the EAS is necessary and consistent with the Commission's statutory goals).

[6] FEMA, the National Weather Service (NWS) and the Department of Homeland Security (DHS).

[7] The FCC's Enforcement Bureau is responsible for investigating possible violations of the Communications Act and the Commission's rules. This Public Notice and request for comment in no way limits or affects any enforcement activities that may be undertaken in connection with the false EAS alert on October 24, 2014.

- *Message Authentication.*
    - How do EAS Participants determine the authenticity, or lack thereof, of an alert message?
    - How is EAS equipment programmed to manage message authentication?
    - There have been several stories in the press and on listserv discussions about the use of "strict time" filters on EAS equipment.[8] Indeed, FEMA staff recently recommended that EAS equipment be programmed with these filters as a short-term fix.[9] To what extent, if any, have EAS Participants implemented this recommendation?
    - More generally, what actions can be taken, either technically or operationally, to enhance EAS alert authentication?
    - What control mechanisms do EAS Participants and their industry associations have in place to assess network integrity, accepted risk, and effectiveness of mitigation measures?

- *Public Safety and Government Agency Impact.*
    - What impact do public safety agencies and other state and local government agencies experience when there is an unauthorized EAS alert? Is the impact different if it is an EAN alert? For example, have government agencies received calls from consumers about unauthorized EAS alerts? Have Public Safety Answering Points (PSAPs) received 911 calls as a result of unauthorized EAS alerts? If so, what was the nature of these calls?
    - What actions, if any, have state and local governments, including public safety agencies, taken to mitigate public confusion when there have been unauthorized alerts? Were any of these actions part of a joint effort with EAS Participants and/or Federal government agencies? If so, were those efforts effective? What actions do such agencies plan to take in the event of an unauthorized alert in the future?
    - What additional actions, if any, can be taken in the future to avoid or mitigate the effects of an unauthorized alert?
    - What actions should government agencies and EAS Participants take to better educate the public about the EAS?

- *Public Impact*. What effect, if any, do unauthorized alerts have on members of the public, including those with disabilities and those who do not speak English as a primary language?

Our action today builds upon the recommendations contained in the Communications Security, Reliability and Interoperability Council (CSRIC) report on EAS security and reliability.[10] In that report,

[8] *See*, *e.g.*, *SBE Issues Warning about Strict Time Setting*, RADIOMAGONLINE (Oct. 27, 2014, 2:09 PM); Randy Stein, *EAS Community Buzzing Over False National Alert*, TV TECHNOLOGY (Oct. 27, 2014, 4:13 PM) (stating that the EAS listserv maintained by the Society of Broadcast Engineers (SBE) is buzzing about the event).

[9] *See* Mark Lucero, *IPAWS EAS Feed Notifications (Inappropriate EAN)*, 48 EAS DIGEST 6 (Oct. 24, 2014, 3:51 PM) ("If possible, configure your EAS device to NOT FORWARD an EAS message with a header . . . that does not match the current date and time, i.e. configure to enforce 'strict time.'").

[10] Today, the Bureau is releasing a public notice to ensure that EAS Participants are aware of EAS security best practices that CSRIC has recently recommended to the Commission. *See* Public Safety and Homeland Security

CSRIC recommended several steps EAS Participants can take to enhance the security of their EAS equipment. In parallel with this Public Notice, the Bureau is seeking comment on EAS Participants' implementation, to date, of those best practices.[11]

Procedural Matters

Pursuant to sections 1.415 and 1.419 of the Commission's rules, 47 CFR §§ 1.415, 1.419, interested parties may file 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 who 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.

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

People with Disabilities: To request materials in accessible formats for people with disabilities (Braille, large print, electronic files, audio format), send an e-mail to fcc504@fcc.gov or call the Consumer and Governmental Affairs Bureau at (202) 418-0530 (voice), (202) 418-0432 (tty).

Parties wishing to file materials with a claim of confidentiality should follow the procedures set forth in section 0.459 of the Commission's rules. Casual claims of confidentiality are not accepted. Confidential submissions may not be filed via ECFS but rather should be filed with the Secretary's Office following the procedures set forth in 47 C.F.R. § 0.459. Redacted versions of confidential submissions may be filed via ECFS. Parties are advised that the Commission looks with disfavor on claims of confidentiality for entire documents. When a claim of confidentiality is made, a public, redacted version of the document should also be filed.

Bureau Seeks Comment on Implementation of Emergency Alert System Security Best Practices, *Public Notice*, DA 14-1628 (PSHSB 2014) (seeking comment on the implementation of voluntary security best practice recommendations, as part of the Commission's larger effort to develop effective and proactive private sector-driven cyber risk management).

[11] *See id.*

For further information, contact James Wiley, Policy and Licensing Division, Public Safety and Homeland Security Bureau at (202) 418-1678 or james.wiley@fcc.gov.

The Public Safety and Homeland Security Bureau issues this Public Notice under delegated authority pursuant to Sections 0.191 and 0.392 of the Commission's rules, 47 C.F.R. §§ 0.191, 0.392.