PUBLIC NOTICE

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

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

DA 19-1144
Released: November 5, 2019

PUBLIC SAFETY AND HOMELAND SECURITY BUREAU SUPPLIES GUIDANCE REGARDING THE EMERGENCY ALERT SYSTEM ALERT VALIDATION REQUIREMENTS

In this Public Notice, the Public Safety and Homeland Security Bureau (Bureau) of the Federal Communications Commission (FCC or Commission) provides guidance to Emergency Alert System (EAS) Participants[1] regarding the requirement that they validate Common Alerting Protocol (CAP)-formatted alerts distributed by the Federal Emergency Management Agency's (FEMA) Integrated Public Alert and Warning System (IPAWS) before transmitting them to the public.

Section 11.56 of the Commission's rules requires EAS Participants to "configure their systems to reject all CAP-formatted EAS messages that include an invalid digital signature."[2] To validate a CAP-formatted EAS message from IPAWS, the EAS device confirms that the digital signature associated with the CAP EAS alert matches the alert contents, and that the signature was created by the certificate included in the alert. Validating the certificate itself requires checking it against a chain of certificates for IPAWS stored in the EAS device, including a trusted root certificate. If any of those certificates cannot be validated, or if any has reached its expiration date, the EAS device will reject the alert as invalid and not process it for transmission to the public. FEMA has informed the Bureau that one of the certificates issued for IPAWS and installed in all EAS devices expires on November 8, 2019.[3] Although the certificate authority issued the replacement certificate on October 28, 2019,[4] FEMA and EAS Participants are concerned that this may not provide sufficient time to update all EAS devices.[5]

The Bureau recognizes that the late availability date of the replacement certificate at issue may leave insufficient time for some EAS Participants to update their EAS devices with the new certificate information prior to the November 8, 2019, expiration date. After the precise time on that date that the certificate expires, and until installation of the replacement certificate information, such EAS Participants

[1] The Commission's rules define EAS Participants as radio broadcast stations, including AM, FM, and low-power FM stations; Class A television and low-power TV stations; cable systems; wireline video systems; wireless cable systems; direct broadcast satellite service providers; and digital audio radio service providers. *See* 47 CFR § 11.11(a).

[2] 47 CFR § 11.56(c).

[3] Phone call from David Munson, Attorney Advisor, Policy and Licensing Division, Public Safety and Homeland Security Bureau, FCC, et al., to Mark Lucero, Chief, IPAWS Engineering, FEMA, et al. (October 22, 2019) (Lucero Phone Conversation).

[4] Email from Mark Lucero, Chief, IPAWS Engineering, FEMA, to David Munson, Attorney Advisor, Policy and Licensing Division, Public Safety and Homeland Security Bureau, FCC (October 29, 2019).

[5] *See*, *e.g.*, Lucero Phone Conversation; Phone call from David Munson, Attorney Advisor, Policy and Licensing Division, Public Safety and Homeland Security Bureau, FCC, to Harold Price, President, Sage Alerting Systems (October 25, 2019).

will be unable to process and transmit to the public CAP-formatted EAS alerts distributed by IPAWS. These EAS Participants, therefore, will be unable to meet their general obligation to receive and process CAP-formatted national EAS alerts (including the Emergency Action Notification alert), Required Monthly Tests, or Required Weekly Tests.[6]

The Bureau notes that over-the-air national EAS messages initiated by Primary Entry Point stations, as well as state and local alerts initiated by State Primary and other non-IPAWS sources, are not affected by this situation.[7] The Bureau also observes that Wireless Emergency Alerts, which are relied on to distribute emergency information to handsets, are also unaffected by this situation.

This situation thus affects EAS equipment readiness. Section 11.35(b) of the Commission's rules provides that if "an EAS Encoder, EAS Decoder or Intermediary Device used as part of the EAS to decode and/or encode messages formatted in the EAS Protocol and/or the Common Alerting Protocol becomes defective, the EAS Participant may operate without the defective equipment pending its repair or replacement for 60 days without further FCC authority."[8] Section 11.35(c) further provides that if repair or replacement of the defective equipment is not completed within 60 days, an informal request for additional time must be submitted to the FCC.[9] Such request "must explain what steps have been taken to repair or replace the defective equipment, the alternative procedures being used while the defective equipment is out of service, and when the defective equipment will be repaired or replaced."[10]

Accordingly, EAS Participants that are unable to complete installation of the new, replacement certificate information for IPAWS prior to November 8, 2019, and therefore are unable to validate (and transmit to the public) CAP-formatted EAS alerts distributed by IPAWS, may continue to operate their EAS equipment for a period of up to 60 days from November 8, 2019, i.e., up to and including January 7, 2020, without additional FCC authority. EAS Participants are expected to make reasonable and good faith efforts to complete such installation prior to the expiration of this 60-day period.

If an EAS Participant is unable to complete installation of the new certificate information prior to the expiration of this 60-day period, it must submit an informal request for additional time. Given that equipment readiness of multiple EAS Participants might be affected by this situation, we partially waive, for good cause and on our motion,[11] the requirement in Section 11.35(c) relating to informal requests for additional time (beyond 60 days) to make equipment compliant, by modifying the FCC office with which such requests must be filed. Specifically, EAS Participants must file such informal requests via email to the FCC at the following email address: alerting@fcc.gov.[12] Such requests must include an explanation

[6] *See*, *e.g.*, 47 CFR §§ 11.51(m), 11.56, 11.61.

[7] Primary Entry Point (PEP) stations are private or commercial radio broadcast stations that cooperatively participate with FEMA to provide EAS alerts to the public, and are the primary source of initial broadcast for a Presidential Alert. *See* 47 CFR § 11.18(a). State Primary stations are tasked with initiating the delivery of EAS alerts other than the Presidential Alert. *See id*. at § 11.18(c).

[8] *Id.* at § 11.35(b). This provision also requires logging of "the date and time the equipment was removed and restored to service." *Id*. In this case, however, the EAS device would not be taken out of service, but rather would be unable to validate CAP alerts for transmission to the public until the new certificate information for IPAWS was installed. Accordingly, only the date and time that this CAP functionality was locked out (*i.e.*, Nov. 8, 2019) and then restored would be logged.

[9] *Id*. at § 11.35(c).

[10] *Id*.

[11] *See* 47 CFR § 1.3.

[12] While section 11.35(c) of the Commission's rules provides that such informal requests should be sent to the relevant Enforcement Bureau Regional Field Office (*see* 47 CFR § 11.35(c)), given the potential number of informal

of the steps the EAS Participant has taken to complete the installation, and the date by which the EAS Participant anticipates installation will be completed.

The foregoing applies only to CAP-formatted alerts distributed by IPAWS; EAS Participants must continue to monitor, receive and process legacy EAS alerts formatted in the EAS Protocol[13] as they normally would.

For additional information about these EAS requirements, please contact David Munson of the Public Safety and Homeland Security Bureau by phone at (202) 418-2921 or by email at david.munson@fcc.gov.

- FCC -

(Continued from previous page)
requests that could be involved, we are tailoring that instruction with respect to informal requests made in connection with the expiring IPAWS certificate situation (only) to allow for their expedited processing.

[13] *See* 47 C.F.R. §11.31.