



PUBLIC NOTICE

Federal Communications Commission
45 L Street NE
Washington, DC 20554

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

DA 22-828
Released: August 5, 2022

PUBLIC SAFETY AND HOMELAND SECURITY BUREAU URGES EMERGENCY ALERT SYSTEM (EAS) PARTICIPANTS TO TAKE IMMEDIATE STEPS TO SECURE EAS EQUIPMENT

PS Docket No. 15-94

In this Public Notice, the Public Safety and Homeland Security Bureau (PSHSB or Bureau) advises communications providers that participate in the EAS (EAS Participants)¹ to take steps to secure their EAS equipment against risks impacting devices that are publicly accessible from the Internet. On August 1, 2022, the Federal Emergency Management Agency (FEMA) issued an advisory on a potential vulnerability in certain EAS encoder/decoder devices that have not been updated to most recent software versions.² FEMA observes that if EAS devices are not up-to-date, an unauthorized actor could issue EAS alerts over the EAS Participant's infrastructure.

EAS Participants must ensure that their EAS equipment's monitoring and transmitting functions are available whenever the stations and systems are operating.³ PSHSB has previously warned EAS Participants about this vulnerability and encouraged them to secure their EAS equipment by installing current security patches and using firewalls.⁴ The Bureau again urges all EAS Participants, regardless of the make and model of their EAS equipment, to upgrade their equipment software and firmware to the most recent versions recommended by the manufacturer and secure their equipment behind a properly configured firewall as soon as possible.

In addition, the Bureau urges EAS Participants to take the following steps to improve their cyber hygiene:

- Install software security patches issued by the manufacturer as soon as they become available.
- Change default passwords.
- Continually monitor EAS equipment and software and review audit logs to detect and report incidents of unauthorized access.

¹ 47 CFR 11.2(b) (radio and television broadcasters, wireless and wired cable television systems, satellite radio and television providers, and wireline video providers).

² See FEMA, *IPAWS Advisory: Emergency Alert System Vulnerability* (Aug. 1, 2022), <https://content.govdelivery.com/accounts/USDHSFEMA/bulletins/3263326>.

³ 47 CFR § 11.35.

⁴ See E-mail from Lisa M. Fowlkes, Chief, PSHSB, FCC to EAS Participants (April 24, 2020 2:03 am EDT) ("We are aware of various reported instances of EAS equipment connected to the internet with weak or otherwise inadequate network security and/or unsecure device setting configurations that potentially leave them vulnerable to IP-based attacks.").

- Review the list of recommended best practices to address potential data security vulnerabilities issued by the Communications Security, Reliability, and Interoperability Council in 2014.⁵

The Commission emphasizes that, under its rules, EAS participants are “responsible for ensuring that EAS Encoders, EAS Decoders, Attention Signal generating and receiving equipment, and Intermediate Devices used as part of the EAS . . . are installed so that the monitoring and transmitting functions are available during the times the stations and systems are in operation.”⁶ The Commission’s rules establish that failure to receive or transmit EAS messages during national tests or actual emergencies because of an equipment failure may subject the EAS Participant to enforcement.⁷

We encourage EAS Participants to contact their EAS equipment manufacturers with any specific questions regarding the security of EAS equipment. Please contact Steven Carpenter, Public Safety and Homeland Security Bureau at (202) 418-2313 or steven.carpenter@fcc.gov with questions about this Public Notice or for further information on the Commission’s rules and policies.

-FCC-

⁵ Communications Security, Reliability and Interoperability Council IV, Initial Report, EAS Security Subcomm. Report at 10-13 (2014), https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG3-EAS_SECURITY_INITIAL_REPORT_062014.pdf.

⁶ 47 CFR § 11.35(a).

⁷ *Id.*; see generally 47 CFR §§ 1.80 *et seq.* See also *Enforcement Bureau Reminds Emergency Alert System (EAS) Participants Of Compliance Obligations*, FCC Enforcement Advisory, DA 21-10 (Jan. 7, 2021).