Digital Alert Systems

Security Advisory

New FCC EAS Cybersecurity Requirements Take Effect September 29, 2026

The FCC has adopted new cybersecurity requirements for Emergency Alert System Participants. **These rules take effect on September 29, 2026.**

The requirements apply to EAS equipment, studio-transmitter-link equipment, and certain remotely managed equipment that routes, processes, or inserts content into an EAS Participant's programming.

For most EAS Participants, the immediate compliance review should focus on three areas:

1. Passwords and Authentication

Before "covered equipment" (the rule applies to all station equipment, not just the DASDEC) is used to broadcast to the public:

- Change all default passwords
  (The DASDEC already requires you to change the default password on initial setup.)
- Passwords must be at least 15 characters long (the DASDEC allows passwords of this length).
- Passwords must not contain any dictionary words.
- A password used to meet the requirement cannot be reused for other accounts, equipment, applications, or services.
  (Example: Do not use the same passwords for your DASDEC and other station equipment.)
- Change a password whenever you believe it has been compromised.

The FCC also permits reasonably sufficient alternative authentication methods. For DASDEC users, this includes Single Sign-On (SSO) support such as OpenID Connect or TACACS+.

2. Security Updates

EAS Participants **must promptly install manufacturer-issued security patches and security-related software and firmware updates**.

DASDEC users should verify that their systems are running current, supported Digital Alert Systems software and continue to monitor security and software-update notices.
Check our website ***www.digitalalertsystems.com*** for the latest available release.

Testing before production deployment is permitted, but testing must begin promptly and be completed within a timeframe consistent with industry best practices.

(continues next page)

Digital Alert Systems
100 Housel Ave. | Lyndonville | NY | 14098
585-765-1155 | fax 585-765-9330
www.digitalalertsystems.com

Revision: 1.0 Publication: SCNDAS-91626

3. Firewalls and Network Segmentation

Covered equipment must be protected by a network firewall or a comparable network-segmentation practice that restricts remote management access to authorized users and devices.

Acceptable approaches may include firewalls, dedicated VLANs, DMZs, isolated management networks, router-based filtering, and other network controls.

What DASDEC Users Should Do Now

Before September 29, review each DASDEC installation and confirm that:

- [ ] The DASDEC is protected by an appropriately configured firewall or equivalent network segmentation.
- [ ] Current security-related DASDEC software updates have been installed (Check our website www.digitalalertsystems.com for the latest available release)
- [ ] Default passwords have been changed.
- [ ] Passwords meet the FCC's new 15-character requirements.
- [ ] Remote management is limited to authorized users and devices.

Digital Alert Systems has long recommended strong access controls, network segmentation, firewall protection, and timely software updates for EAS equipment. These basic practices are now part of the FCC's EAS cybersecurity requirements.

More details are in the FCC rules outlined below.

Effective Date: September 29, 2026
Rule: 47 C.F.R. § 11.35(d)
FCC Order: FCC 26-38

Questions about securing or updating your DASDEC?

Contact Digital Alert Systems at support@digitalalertsystems.com