

INDUSTRY ADVISORY

Understanding Security for Your EAS Equipment

Best Practices, FCC Compliance, and Recommendations for Users

September 2026 | Revision 2.0

Updated from the original 15 January 2014 industry advisory.

Twelve years ago, Digital Alert Systems advised broadcasters that EAS devices should never be exposed directly to the public Internet, that default passwords should be changed, that networks should be segmented, and that security patches should be applied promptly. Those recommendations have aged unusually well. In 2026, several of them are no longer merely prudent operational practice: they are now reflected directly in the FCC's EAS rules, **effective 29 September 2026**.

THE 2026 FCC BASELINE

New 47 C.F.R. § 11.35(d) requires EAS Participants to apply security controls not only to EAS equipment, but also to studio-transmitter-link equipment and remotely managed equipment that routes, processes, or inserts content into the participant's programming. The three required controls are: strong or alternative authentication, prompt installation of manufacturer security patches and security-related software/firmware updates, and a firewall or comparable network-segmentation practice that limits remote management access to authorized devices and users.

The central lesson for 2026 is simple: EAS cybersecurity is no longer about securing one encoder/decoder. It is about securing the alerting path and the systems that can influence what reaches air.

1. What Has Changed Since 2014

The 2014 paper correctly treated EAS equipment as a networked critical system rather than an isolated broadcast appliance. Since then, the surrounding environment has become more interconnected: IP-based studio and transmitter links, remote management, centralized operations, automation interfaces, AoIP, virtualized infrastructure, cloud-connected services, enterprise identity systems, and continuous vendor update mechanisms are now common parts of broadcast operations.

That connectivity improves flexibility and manageability, but it also enlarges the attack surface. An attacker may not need to compromise the EAS encoder/decoder itself. A weak credential, exposed remote-management interface, compromised router, automation system, studio-transmitter link, or other device capable of routing or inserting content can create the same public-safety consequence: a false alert, altered alert, or failure to transmit a real one.

The threat is practical, not theoretical

- Internet-wide scanning makes exposed management interfaces easy to discover.
- Credential stuffing, password reuse, and unchanged factory credentials remain common paths to unauthorized access.
- Known vulnerabilities remain exploitable when software and firmware are not updated.
- Remote operations and shared enterprise credentials can turn one compromised account into access across multiple facilities.
- Used or 'gray-market' equipment may arrive with obsolete software, residual configurations, or retained credentials.
- Ransomware and general IT compromise can reach broadcast and alerting systems when those systems share flat or weakly segmented networks.

The FCC cited evidence from the 2023 nationwide EAS test indicating that approximately 23% of reported EAS equipment units were using outdated software or equipment no longer receiving regular software updates. In FCC 26-38, the Commission treated that condition as a material public-safety and national-security concern.

2. The FCC's 2026 EAS Cybersecurity Rules

On June 25, 2026, the FCC adopted targeted cybersecurity requirements in FCC 26-38. The rules amend § 11.35, Equipment Operational Readiness. They become effective 60 days after publication in the Federal Register.

2.1 Scope: protect more than the EAS box

The rule applies to security controls for:

- EAS equipment;
- studio-transmitter-link equipment; and
- any remotely managed equipment that routes, processes, or inserts content into the transmission of the EAS Participant's programming.

This is an important shift in regulatory perspective. The compliance boundary follows the broadcast path that can affect public warning, not simply the chassis labeled 'EAS.' Stations should inventory the systems in that path and determine which ones fall within the rule's functional description.

2.2 Passwords and authentication

Before equipment is used to broadcast to the public, an EAS Participant must:

- change any default password;
- use a strong password, or a reasonably sufficient alternative authentication measure;
- change a password whenever there is reason to believe it has been compromised; and
- not reuse that password for other accounts, equipment, applications, or services.

For the FCC rule, a strong password means at least 15 characters and no dictionary words.

The Commission expressly permits alternative authentication methods such as out-of-band authentication, one-time-password devices, and single- or multi-factor cryptographic authentication. This makes enterprise SSO and MFA particularly useful where supported and properly implemented.

2026 PASSWORD PRACTICE

Do not carry forward the 2014 assumption that passwords must be changed on a fixed calendar merely because time has passed. Modern NIST guidance generally favors long, unique credentials, blocklists for weak/common passwords, password managers, and changes when compromise is suspected or confirmed. For EAS-regulated equipment, however, the FCC's specific 15-character, no-dictionary-word, no-reuse requirements control.

2.3 Security patching

EAS Participants must promptly install security patches and security-related software and firmware updates issued by equipment manufacturers. The FCC allows testing before production installation, but testing must begin promptly and be completed within a timeframe consistent with industry best practices.

The rule does not define a universal number of days. The practical answer is therefore process discipline: know what equipment you own, subscribe to vendor security notices, assess updates quickly, test when operationally necessary, document the decision, and deploy without letting 'testing' become an indefinite parking lot.

2.4 Firewall or comparable segmentation

The FCC requires a network firewall or comparable network-segmentation practice that limits remote management access to authorized devices and authorized users. In the Order, the Commission specifically points to dedicated VLANs, DMZs, physically isolated management networks, router filtering, and other methods that prevent unauthorized public-Internet access.

The operational objective is straightforward: management interfaces for EAS and related air-chain systems should not be openly reachable from the public Internet.

3. Recommended EAS Security Practices for 2026

The FCC's three controls are a regulatory floor, not a complete security architecture. The following practices update the original 2014 recommendations using current NIST, CISA, and CIS guidance.

Issue	2026 Best-Practice Recommendation
Governance and ownership	Assign a named owner for EAS cybersecurity. Maintain a current inventory of EAS and related air-chain systems, their software/firmware versions, network locations, administrators, and vendor support status.
Secure by default	Do not place EAS or related management interfaces directly on the public Internet. Disable unneeded services and ports. Remove or disable unused accounts.
Network segmentation	Place EAS and related management functions on a dedicated VLAN, protected management network, or equivalent segmented zone. Apply least-privilege rules between EAS, business IT, automation, AoIP, and transmitter networks.
Remote access	Require remote administration to traverse a controlled path such as a managed VPN, zero-trust access service, or hardened jump host. Avoid direct port-forwarding to device web interfaces.
Identity and access	Use named user accounts rather than shared logins where possible. Apply least privilege and role-based access. Prefer SSO and MFA for enterprise environments.

Passwords	Meet the FCC minimum: 15+ characters, no dictionary words, no reuse, no defaults. Prefer randomly generated credentials stored in an approved password manager when password authentication is used.
Patching	Track manufacturer notices and software lifecycle status. Establish a written, risk-based patching process with expedited handling for actively exploited or critical vulnerabilities.
Configuration management	Back up known-good configurations. Record changes to network, user, alert-forwarding, audio, GPIO, automation, and remote-management settings.
Logging and monitoring	Enable and preserve available audit/security logs. Review failed logins, account changes, remote access, configuration changes, and unusual device behavior.
Physical security	Keep EAS and associated network equipment in controlled areas. Restrict console, USB, serial, and local-network access to authorized personnel.
Incident response	Have a short, executable playbook for suspected unauthorized access: isolate, preserve evidence, revoke credentials, contact the vendor, validate software/configuration, restore from a trusted state, and document actions.
Lifecycle and procurement	Do not treat unsupported equipment as indefinitely serviceable. Include software support, vulnerability response, secure update capability, authentication, logging, and lifecycle commitments in purchasing decisions.

4. Practical Implementation Guidance

4.1 Build an EAS security inventory

Start with the systems that can affect EAS transmission. For each device or service, record the manufacturer, model, serial number, software/firmware version, IP address or hostname, management method, network zone, user accounts, remote-access path, support status, and the person or group responsible for maintenance. Include related routers, automation interfaces, STL systems, AoIP devices, master-control systems, and other remotely managed components that can route or insert content.

4.2 Draw the management path

A simple diagram is one of the most effective security tools a station can maintain. Show what can reach the EAS device, what the EAS device can reach, where the firewall boundaries are, where remote users enter, and which ports/protocols are actually required. Anything that appears on the diagram without a clear operational purpose is a candidate for removal or restriction.

4.3 Use allowlists, not broad trust

Where practical, permit management and control traffic only from known administrative systems or subnets. A firewall rule that permits 'any internal host' is better than public exposure, but it is still broader than necessary. Treat the business LAN, guest Wi-Fi, contractor networks, and general user endpoints as separate trust zones.

4.4 Make patching auditable

1. Identify how the manufacturer announces security updates.
2. Record the current software/firmware version and support status.
3. When an update is issued, determine whether it is security-related and whether known exploitation or exposure increases urgency.
4. Begin testing promptly when testing is needed.
5. Install the update, verify successful installation, and confirm EAS operation afterward.
6. Document the date, version, tester/installer, and any reason for delay.

4.5 Treat remote access as privileged access

Remote EAS management should be exceptional in privilege even when routine in frequency. Use individual accounts, MFA where available, centralized identity when appropriate, access logging, and a controlled network path. Remove access promptly when an employee, contractor, or service provider no longer needs it.

5. Applying These Practices to DASDEC

Current DASDEC software provides several controls that can help EAS Participants implement the FCC's requirements and broader best practices. Actual configuration remains the responsibility of the EAS Participant and should be coordinated with the organization's IT/security policy.

- Current DASDEC software supports passwords up to 16 characters, allowing use of a 15- or 16-character credential that meets the FCC length requirement.
- The platform requires replacement of the factory-default password at first sign-in.
- Current software blocks common/prohibited passwords and helps prevent password reuse.
- Account lockout after repeated failed logins helps slow brute-force attacks.
- DASDEC supports role-based user access and enterprise SSO integrations. Version 5.4 added OpenID Connect support, complementing earlier TACACS+ support.
- Version 6 uses a modernized operating platform and adds network/security options including support for CIDR notation.
- DASDEC software updates and vendor notices should be incorporated into the station's documented patch-management process.

IMPORTANT: THE FIREWALL IS AN ARCHITECTURE CONTROL

No EAS encoder/decoder should be expected to substitute for the station's network security architecture. The FCC rule is directed to the EAS Participant: the participant must place EAS and related remotely managed systems behind a firewall or comparable segmentation practice and restrict remote management to authorized devices and users.

6. Passwords, SSO, and more: What 'Good' Looks Like in 2026

Password guidance has evolved substantially since 2014. The old model emphasized complexity rules and frequent forced changes. Modern guidance places greater weight on length, uniqueness, resistance to known/common passwords, password-manager use, and multi-factor or cryptographic authentication. The FCC's rule adds a specific regulated minimum for covered EAS-related systems.

For password-based DASDEC access

- Use a unique 15- or 16-character password that contains no dictionary words.
- Generate it randomly rather than trying to invent a memorable phrase.
- Store it in an approved enterprise password manager rather than on paper taped to the rack, in a shared spreadsheet, or in an unencrypted email.
- Use individual accounts where operationally feasible; avoid a single shared administrator credential.
- Change it immediately if compromise is suspected, staff with knowledge of it depart, or the credential has otherwise been exposed.

For enterprise environments

SSO can reduce the number of device-specific credentials and make account provisioning, revocation, auditing, and role assignment more consistent. The security benefit depends on protecting the identity provider itself, limiting administrative roles, and ensuring that emergency access procedures remain available during identity-system outages.

7. If You Suspect Unauthorized Access

A station should have a short incident-response sequence that engineering and IT can execute without improvisation:

1. Contain the exposure. Block public access, disable the suspect remote-management path, or isolate the affected network segment as operationally appropriate.
2. Preserve evidence. Save available device, firewall, VPN, identity-provider, and system logs before they roll over.
3. Revoke and replace affected credentials, tokens, API keys, or certificates.
4. Contact the equipment manufacturer and internal security/IT personnel. Determine whether a known vulnerability or compromised configuration is involved.
5. Validate the device. Confirm approved software/firmware, user accounts, network settings, alert-forwarding rules, audio paths, and automation interfaces.
6. Restore from a trusted configuration or reinstall software if integrity cannot be established.
7. Test EAS operation after recovery and document the incident, corrective actions, and lessons learned.

The 2026 FCC Order did not adopt the broader 2022 proposal for mandatory EAS cybersecurity risk-management plans. That does not make planning unnecessary. It simply means that a practical incident-response and security program remains a best practice beyond the three specific controls now required by § 11.35(d).

8. 2026 EAS Cybersecurity Compliance Checklist

- ☐ All factory-default passwords on covered equipment have been changed before public operation.
- ☐ Each password used for compliance is at least 15 characters, contains no dictionary words, and is not reused elsewhere.
- ☐ Alternative authentication, where used, is reasonably sufficient to mitigate unauthorized-access risk.
- ☐ Passwords are changed whenever compromise is suspected or known.
- ☐ The station has identified EAS equipment, STL equipment, and remotely managed systems that route, process, or insert content into programming.
- ☐ Manufacturer security patches and security-related firmware/software updates are tracked.
- ☐ Testing of security updates begins promptly when needed and does not create indefinite deployment delay.
- ☐ Installed versions are verified after patching.
- ☐ EAS and related management interfaces are not directly exposed to the public Internet.
- ☐ A firewall, VLAN, DMZ, isolated management network, router filter, or comparable segmentation control restricts remote management.
- ☐ Remote-management access is limited to authorized users and authorized devices.
- ☐ Unnecessary services, ports, accounts, and remote-access paths are disabled.
- ☐ Access is removed promptly when personnel or contractor status changes.
- ☐ Security and operational logs are retained long enough to support troubleshooting and incident investigation.
- ☐ Known-good configuration backups and recovery procedures exist.

9. Conclusion

The most striking thing about revisiting the 2014 guidance is not how much of it has become obsolete, but how much of it has become compulsory. The basic architecture was right: do not expose EAS equipment directly to the Internet;

change default credentials; segment networks; restrict remote access; apply patches; use least privilege; train staff; and plan for recovery.

The 2026 FCC rules convert three of those ideas into explicit minimum controls and broaden the regulatory focus to other remotely managed systems that can affect the programming path. Broadcasters should treat compliance as the starting line. The objective is not merely to satisfy a checklist, but to preserve the integrity and availability of a public-warning capability that the public must be able to trust when it matters.

References and Current Guidance

- Federal Communications Commission, Modernization of the Nation's Alerting Systems; Protecting the Nation's Communications Systems from Cybersecurity Threats, FCC 26-38, Report and Order and Further Notice of Proposed Rulemaking (adopted June 25, 2026; released June 29, 2026), especially paras. 18-23 and Appendix A, 47 C.F.R. § 11.35(d).
- National Institute of Standards and Technology, Digital Identity Guidelines: Authentication and Authenticator Management, NIST SP 800-63B-4 (2025).
- Cybersecurity and Infrastructure Security Agency, Cross-Sector Cybersecurity Performance Goals 2.0 (2025).
- National Institute of Standards and Technology, Cybersecurity Framework (CSF) 2.0 (2024).
- Center for Internet Security, CIS Critical Security Controls v8.1 (2025).
- National Institute of Standards and Technology, Security and Privacy Controls for Information Systems and Organizations, NIST SP 800-53 Rev. 5 (2020, as updated).
- National Institute of Standards and Technology, Guidelines on Firewalls and Firewall Policy, NIST SP 800-41 Rev. 1.
- National Institute of Standards and Technology, Secure Software Development Framework (SSDF), NIST SP 800-218 (2022).
- Digital Alert Systems, Understanding Security for Your EAS Equipment: Best Practices and Recommendations for Users (Jan. 15, 2014).
- Digital Alert Systems, Version 6 Software for DASDEC-III Platforms (2026) and Version 5.4 security/SSO materials (2024).

This advisory is provided for general informational purposes and is not legal advice. EAS Participants should review the final FCC rules, applicable effective dates, manufacturer documentation, and their own network and operational requirements.

100 Housel Ave., P.O. Box 535, Lyndonville, NY 14098
 +1(585)765-2254 fax +1(585)765-9330
www.digitalalertsistemas.com