Digital Alert Systems

BY ELECTRONIC FILING

Marlene H. Dortch
Secretary
Federal Communications Commission
45 L Street NE
Washington, DC 20554

Re: Comments of Digital Alert Systems, Inc. on the FCC 26-38 Further Notice of Proposed Rulemaking (PS Docket Nos. 25-224, 15-94, and 15-91)

Dear Ms. Dortch:

Digital Alert Systems, Inc. (DAS) submits these comments in response to the Commission's Further Notice of Proposed Rulemaking in FCC 26-38.

This is the first of two separate filings DAS is submitting in response to the FNPRM. DAS has divided its comments because the Commission's proposals present two related but distinct sets of technical and policy questions. This filing addresses measures to improve the security, precision, interoperability, and public usefulness of CAP and legacy EAS alerting. DAS's companion filing separately addresses the proposed authorization and certification of software-based EAS implementations.

In this filing, DAS addresses five principal issues: requiring valid digital signatures for CAP-formatted EAS messages; developing a practical, role-based framework for authenticating legacy EAS alerts; establishing a universal alert message identifier that can follow an alert across multiple distribution paths; using CAP geographic information to improve EAS targeting and support more advanced geofencing capabilities; and developing standardized symbols for emergency alerts.

DAS generally supports the Commission's efforts in each of these areas, which collectively offer an opportunity to strengthen authentication, reduce unnecessary duplicate alerts, improve geographic relevance, support more consistent presentation across warning platforms, and make emergency information more understandable and accessible. Implementation, however, should preserve the reliability and backward compatibility of the existing EAS architecture while creating a practical path toward richer and more secure public warning capabilities. DAS therefore recommends approaches that build upon existing CAP structures, certified EAS equipment, established alerting roles, and supplemental mechanisms such as Textual Data Exchange, rather than placing new or incompatible demands on the legacy EAS Protocol.

Respectfully
/s/
Edward Czarnecki, PhD
Vice President, Government and International

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

Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of Notice of Proposed Rulemaking -	)	PS Docket 25-224
Modernization of the Nation's Alerting Systems; Wireless	)	PS Docket 15-94
Emergency Alerts; Amendment of Part 11 of the	)	PS Docket 15-91
Commission's Rules Regarding the Emergency Alert System	)	

COMMENTS OF DIGITAL ALERT SYSTEMS, INC.

ON THE FURTHER NOTICE OF PROPOSED RULEMAKING
PART I: Authentication, Message Identification, Geotargeting, and Alert Symbology

Contents

1 Requiring EAS Participants to Reject Unsigned CAP EAS Messages

DAS supports the proposal to require EAS Participants to reject CAP-formatted EAS messages that lack a valid digital signature. [1] Current rules require rejection of a CAP message that includes an invalid digital signature, but they do not require rejection of an unsigned CAP message. That distinction leaves a class of EAS inputs without cryptographic assurance of source or message integrity.[2]

1.1 Security and Public-Safety Rationale

CAP can carry richer and more precise warning information than the legacy EAS Protocol, but those benefits depend on confidence that the message received is the message issued by an authorized source. An unsigned message may be syntactically valid and operationally processable while remaining unverifiable. In a system designed to interrupt programming and convey official protective-action information, that is a material security gap.

The principal risks are straightforward:

- **Spoofing and false activation.** An attacker or unauthorized system could create a CAP message that appears to originate from a legitimate source.
- **Tampering or substitution.** Alert text, geography, timing, or instructions could be modified in transit, in storage, or by an intermediary system.
- **Operational error.** Misconfigured feeds, stale files, production-test crossover, or unauthorized internal access can produce messages that look valid but are not trustworthy.
- **Loss of public confidence.** False or manipulated alerts can undermine trust in EAS and in official emergency communications more broadly.

Digital signatures do not resolve every authorization, configuration, or cybersecurity issue. They do, however, provide a necessary baseline for validating the origin and integrity of messages. A uniform rule is also operationally clearer: a CAP EAS message is eligible for processing only if it carries a signature that validates successfully.

[1] Modernization of the Nation's Alerting Systems; Protecting the Nation's Communications Systems from Cybersecurity Threats; Wireless Emergency Alerts; Amendment of Part 11 of the Commission's Rules Regarding the Emergency Alert System, FCC 26-38, Report and Order and Further Notice of Proposed Rulemaking, PS Docket Nos. 25-224, 22-329, 15-91, and 15-94 (released June 29, 2026) (FCC 26-38).

[2] See 47 C.F.R. § 11.56(c); FCC 26-38, paras. 41-42 and App. B (proposed § 11.56(c)).

1.2 Operational Experience

The Commission declined to require signatures on every CAP EAS alert responding to concerns that certain state and local alerting authorities were not then using IPAWS or CAP-based digital signatures. That was a transitional judgment about implementation readiness, not a finding that unsigned CAP messages were secure.[3]

The available operational record now supports a stronger baseline. The 2023 nationwide EAS test produced 20,682 unique filings. Twenty-three test participants reported receipt complications involving XML digital signatures, and 17 reported retransmission complications. The 23 receipt reports represented approximately 0.1 percent of all unique filings. Those results do not eliminate the need for careful certificate and key management, but they indicate that signature validation is manageable at national scale.[4]

The relevant failure modes are known: expired or invalid certificates, incorrect trust anchors, clock errors, signing-system misconfiguration, and modification of a message after signing. These are operational and lifecycle-management issues. The appropriate response is improved testing, monitoring, and certificate administration, not continued acceptance of unauthenticated messages.

1.3 Impact on Non-IPAWS CAP Systems

The direct effect on alerting authorities that distribute via IPAWS should be minimal to none, since IPAWS already signs alerts distributed through its system. The Commission reports that more than 2,000 federal, state, local, tribal, and territorial alerting authorities use IPAWS. Signed CAP alerting is therefore established practice, not an experimental capability.[5]

The remaining issue is the extent of non-IPAWS CAP distribution that still relies on unsigned messages. State networks, local relay systems, specialized public-safety workflows, and broadcaster-specific feeds may use CAP outside IPAWS. The Commission should require a focused inventory, developed with state emergency communications committees, emergency management agencies, alert-origination vendors, EAS manufacturers, and EAS Participants, before the rule becomes effective.

---

[3] Amendment of Part 11 of the Commission's Rules Regarding the Emergency Alert System; Wireless Emergency Alerts, 33 FCC Rcd 7086, 7095-96, paras. 20-21 (2018).

[4] Federal Communications Commission, Report: October 4, 2023 Nationwide Emergency Alert Test, at 8, 17-22 (2024); FCC 26-38, para. 44. The test report describes 20,682 unique filings and reports 23 receipt explanations and 17 retransmission explanations involving XML digital-signature issues.

[5] FCC 26-38, para. 43; FEMA, IPAWS Alerting Authorities - Agencies and Organizations (listing more than 2,000 federal, state, local, tribal, and territorial alerting authorities using IPAWS).

A non-IPAWS system that originates or distributes CAP messages for EAS processing should not remain indefinitely exempt from authentication. Where signing is not currently supported, the system should be upgraded, reconfigured, or transitioned. The work may include signature generation, certificate issuance and renewal, key protection, preservation of signed content through intermediaries, and testing against deployed EAS equipment.

1.4 Implementation and Transition

For EAS Participants using modern CAP-capable equipment, implementation should generally be straightforward because the equipment already validates signed CAP messages. For current DASDEC deployments, the option to reject unsigned CAP messages is already available; implementation may require only a simple configuration review by checking that the option to only rejected unsigned messages is enabled. The DASDEC would not require a software update. Removing any option to allow unsigned messages would be provided in a future normal periodic software update.

The Commission should pair the requirement with four practical safeguards:

1. Provide a reasonable transition period, including a state-level inventory of non-IPAWS CAP paths and a pre-compliance testing window.
2. Coordinate clear guidance on trust anchors, certificate issuance, renewal, revocation, expiration monitoring, key protection, and reliable time synchronization.
3. Require systems to preserve signed content, prohibit unapproved post-signature modification, and log or alarm on unsigned and invalidly signed messages.
4. Require contingency procedures for certificate failure, signing-system outages, or key compromise, with manufacturer and alerting-authority coordination rather than routine fallback to unsigned CAP.

These measures address the Commission's legitimate concern that authentication failures could delay or reject valid alerts. They also avoid converting temporary implementation limitations into a permanent reduction in the security baseline.

1.5 Conclusion

DAS therefore supports requiring EAS Participants to reject all CAP-formatted EAS messages that do not include a valid digital signature. The Commission should close the remaining authentication gap while providing a reasonable transition for any non-IPAWS systems that still require remediation.

2 Authentication of Legacy EAS Alerts

The Commission also seeks comment on the feasibility, effectiveness, and cost of authenticating legacy EAS alerts. DAS supports further development of legacy authentication, but the Commission should not assume that every EAS Participant and every alerting authority must hold the same type of signing

credential. A practical design must reflect the distinct roles of originators, state relays, Local Primary stations, downstream participants, manufacturers, and test systems.[6]

2.1 Role-Based Credential Architecture

A FEMA-rooted or FEMA-coordinated trust framework could issue certificates or provide related trust services for authorized federal, state, local, tribal, territorial, and relay entities. Manufacturers of Commission-authorized EAS equipment would implement the technical capability to generate, protect, and use those credentials and to create a compact supplemental authentication packet, such as the EAS Data Exchange (EDX) approach we recommend below in Section 4.. EAS Data Extension (EDX) is an open and backward-compatible mechanism for conveying supplemental digital information immediately following the existing EAS header.[7]

A compact authentication object could include a hash of the canonical legacy EAS header, a four-digit year, signer or authority identifier, certificate or key identifier, replay-protection data, and a signature or other authentication value. Receiving devices should be able to validate the object using cached trust anchors and certificate information so that real-time Internet access is not required during alert processing.

2.2 Local Primary Translation and Relay

The Local Primary case requires special handling. A Local Primary station may receive a signed IPAWS CAP message, validate it, map it into a legacy EAS header, and transmit the legacy version over the air. Downstream stations may monitor that Local Primary source without receiving the original CAP message directly.

The original CAP signature cannot simply be carried forward unchanged. The legacy EAS message is a derived representation that may select or transform the event code, location codes, valid time period, originator code, and other fields. The translated legacy header therefore needs its own integrity protection, while preserving a verifiable link to the original CAP message.

---

[6] FCC 26-38, paras. 45-48; Amendment of Part 11 of the Commission's Rules Regarding the Emergency Alert System; Wireless Emergency Alerts, 31 FCC Rcvd 594, 651, para. 139 (2016).

[7] For clarity, DAS uses EAS Data Extension (EDX) to refer generically to the concept of conveying supplemental digital information in association with an EAS message, with an EDX data block or mechanism referring to a generic implementation of that concept. TDX™ is Digital Alert Systems' implementation of EDX. As proposed here, EDX would be used to convey a unique message identifier and digital authentication/signature information. As proposed here, EDX would be used to convey a unique message identifier and digital authentication/signature information, and could be implemented through a publicly available interoperable specification by any EAS equipment manufacturer.

DAS recommends a role-limited relay attestation. The Local Primary credential would not confer new alert-origination authority. It would attest that:

- the device received and validated an authenticated CAP message;
- the device translated that CAP message into a specified canonical legacy EAS header;
- the device generated the corresponding over-the-air legacy transmission; and
- the supplemental authentication packet binds the translated header to the validated CAP source and to the Local Primary's relay role under the applicable State EAS Plan.

The packet could include the CAP identifier, a digest of the CAP message or relevant fields, the hash of the resulting legacy header, the signer role and relay identifier, and replay-protection data. Downstream equipment would validate the relay attestation using cached trust information rather than reconstructing the entire CAP validation process over the air. Including this data in the EAS addendum would also provide an effective means to detect, filter, and remove risk of airing duplicate EAS and CAP message equivalents.

2.3 Recommended Approach

The Commission should develop a standards and testing record around a FEMA-rooted or FEMA-coordinated trust architecture, role-limited credentials, offline validation, replay protection, and backward-compatible carriage following the legacy header. State EAS Plans should identify which entities are authorized to originate, translate, or relay authenticated legacy alerts.

3 Universal Alert Message ID for EAS

DAS supports development of a universal alert message identifier for EAS. The same underlying alert can reach an EAS Participant through IPAWS CAP, NOAA Weather Radio, legacy over-the-air relay, state networks, and Local Primary monitoring assignments. Current EAS duplicate detection compares relevant header information byte-by-byte; a change in any relevant field will cause two representations of the same alert to be treated as separate messages.[8]

A universal identifier would not solve every duplication issue, but it could materially improve duplicate suppression, logging, troubleshooting, and CAP-to-legacy correlation if it is authenticated and consistently implemented.

[8] FCC 26-38, para. 55.

3.1 Implementation in CAP and Legacy EAS

For CAP, the Commission should build on existing CAP identification and reference elements. An authorized originator or origination system should assign a stable identifier when the alert is created and preserve the identifier and references through updates, corrections, and cancellations.[9]

For legacy EAS, the identifier should not be added to the existing header code string. The header is constrained and widely deployed. Instead, an updated device could carry the identifier in a supplemental EDX block following the standard header. Older equipment would continue to process the legacy header, while updated equipment could use the supplemental identifier for correlation and logging.

3.2 Operational Benefits and Duplicate Detection

A universal identifier could support:

- duplicate suppression when the same alert arrives via CAP and the legacy relay with non-identical header fields;
- correlation of a Local Primary's translated legacy alert with the authenticated CAP source;
- consolidated logging of received copies, relays, updates, cancellations, and failures;
- faster troubleshooting across originators, State Emergency Communications Committees, EAS Participants, and manufacturers; and
- cross-platform accountability under a "One message, many paths" model.

The identifier should become the preferred correlation mechanism when it is present, valid, and authenticated. Existing header-based duplicate detection should remain as a fallback during transition and for legacy messages that do not include the supplemental data.

An unauthenticated identifier must not be used as the sole basis for suppressing an alert. Otherwise, a forged message carrying the identifier of a valid alert could be used to suppress the alert. The identifier is not itself an authentication control; it must be covered by the CAP signature or by authenticated legacy supplemental data.

3.3 Incident, Message, and Relay Identifiers

The Commission should define what the identifier represents. At least three concepts must be distinguished:

- **Incident or alert-thread identifier.** Groups related messages concerning the same underlying event.

---

[9] OASIS, Common Alerting Protocol Version 1.2, §§ 3.2.1, 3.3.4.1 (July 1, 2010) (defining the CAP identifier, references, incidents, and XML digital-signature mechanism).

- **Message-instance identifier.** Distinguishes the original alert from updates, corrections, cancellations, and reissuances.
- **Relay or transmission identifier.** Identifies a specific retransmission, translation, or local copy.

Duplicate suppression should prevent the repeated presentation of the same message, not suppress a legitimate update or cancellation merely because it relates to the same incident. A useful framework should therefore support both a stable alert-thread identity and a distinct message-instance identity.

3.4 Use in CAP and EAS

The CAP identifier should be part of signed CAP content. A later update, correction, or cancellation should carry its own message-instance identity and appropriate references to the earlier message. For legacy EAS, a supplemental packet could include the universal message ID, optional incident ID, message version, CAP reference, originator and relay identifiers, four-digit year, a hash of the canonical legacy header, and authentication data binding those elements together.

For a Local Primary translating CAP to legacy EAS, the same CAP-related identifier should be preserved in the supplemental packet bound to the resulting legacy header. Downstream stations could then determine that the over-the-air relay is the same alert already received through CAP or another monitored source.

4 Including Unique Message ID and Signature in Legacy EAS

Beginning as early as 2004, we suggested to the Commission that supplemental digital data could be associated with a legacy EAS message, using the Textual Data Exchange (TDX™) capability, in a manner that preserves compatibility with existing EAS equipment..[10] This provides a practical means of

[10] "Digital Alert Systems, LLC Comments Concerning the FCC Review of the Emergency Alert System," EB Docket 04-29, filed 18 October 2004 (http://apps.fcc.gov/ecfs/document/view?id=6516743468); Reply Comments of the Digital Alert Systems, LLC , Submitted Dec 13, 2004 (https://www.fcc.gov/ecfs/search/search-filings/filing/5512037379); REPLY COMMENTS OF Digital Alert Systems, LLC, Proceeding EB 04-296, Submitted Dec 28, 2005 (https://www.fcc.gov/ecfs/search/search-filings/filing/5513342546)l; Digital Alert Systems' Ex Parte, EB Docket 04-296, Submitted Oct 26, 2007 https://www.fcc.gov/ecfs/search/search-filings/filing/5514895475); Also see "Monroe Electronics Informally Comments on Revision of the Commissions Part 11 Rules Governing the Emergency Alert System Pending Adoption of the Common Alert Protocol by the Federal Emergency Management Agency," EB Docket No. 04-296; DA 10-500; filed 5/17/2010, at page 2 (https://ecfsapi.fcc.gov/file/7020460142.pdf); "Comments of Monroe Electronics," EB Docket No. 04-296, FCC 14-93, filed 8/14/2014, §4.2 at pp4-5. (https://ecfsapi.fcc.gov/file/7521760420.pdf); "Comments of Monroe Electronics," PS Docket 14-200, filed 12/5/2014, at p.5 (https://ecfsapi.fcc.gov/file/60000990607.pdf) ; "Comments of Monroe Electronics," PS Docket 15-04, filed 5/26/2016. Also see "Comments of Richard Rudman," PS Dockets 15-91 and 15-94, at p4, filed 5/21/2016 (https://ecfsapi.fcc.gov/file/60002084092.pdf).

conveying information not accommodated within the existing EAS header codes without requiring replacement of the legacy EAS protocol or installed base.

To clarify our present proposal, we recommend using the term **EAS Data Extension (EDX)** to refer generically to an open, manufacturer-neutral method for conveying supplemental digital information in association with an EAS message. An EDX data block or EDX mechanism refers to a generic implementation of that concept; TDX™ is Digital Alert Systems' implementation of such a mechanism. As proposed here, EDX would convey a unique message identifier and digital authentication/signature information. The mechanism could be defined through a publicly available, interoperable specification capable of implementation by any EAS equipment manufacturer.

4.1 EDX Provides a Practical Payload Envelope for Message Identification and Authentication

The EDX approach provides a practical means to carry the compact data needed to add persistent message identification and cryptographic authentication to a conventional EAS transmission. EDX should not be understood as the authentication mechanism itself. Rather, it is an additional payload envelope that allows an EAS message to carry a unique message identifier, a key or certificate identifier, and a compact digital signature binding those elements to the associated EAS message.

A EDX authentication payload could contain, at minimum:

1. **A unique alert message identifier.** The identifier would allow EAS equipment to recognize and correlate different copies or representations of the same alert, including CAP and legacy EAS versions received through separate distribution paths. Where the legacy EAS message is derived from CAP, the EDX payload should preserve the originating CAP message identifier, or a standardized compact representation of that identifier, rather than create an unrelated identifier at each relay point.
2. **A key or certificate identifier.** The identifier would tell the receiving EAS device which locally maintained public key, certificate, or trust record is used to validate the signature. The complete public-key certificate or certificate chain need not be transmitted with every alert. Carrying a compact key or certificate reference would substantially reduce the size and duration of the EDX payload while allowing receiving equipment to select the appropriate validation material.
3. **A compact digital signature.** The signature would cryptographically bind the unique message identifier and other defined message elements to an authorized signer. Depending upon the framework ultimately adopted, the signer could be an authorized alert originator, State Relay, Local Primary source, or other entity assigned a defined signing or relay role.

4.2 EDX Should Use Three Compact, CRC-Protected Authentication Frames

The Commission should evaluate EDX as a compact binary envelope for conveying the information needed to identify and authenticate a legacy EAS message. To limit the duration of the added AFSK burst, the EDX frame should include only information that the receiving EAS device cannot derive or maintain independently. It should not carry the complete signing certificate, certificate chain, or a separately transmitted digest of the EAS header.

An illustrative frame could contain:

```
<version/flags | unique message ID | key ID | four-digit year | compact
digital signature | CRC>
```

The unique message identifier would correlate the legacy transmission with the corresponding CAP alert or other representations of the same warning. A compact key identifier would direct the receiving device to the appropriate public key or certificate maintained in its local trust store. The protocol version or identified credential could establish the applicable cryptographic algorithm and the authorized role of the signer, avoiding the need to transmit that information with every alert.

The digital signature should be calculated over a defined canonical representation of the legacy EAS header together with the protocol version, unique message identifier, key identifier, and four-digit year. The receiving device would reconstruct the same signed data from the received EAS header and EDX fields, select the appropriate public key using the key identifier, and validate the signature. Because the receiver can calculate the header digest independently, the digest need not be transmitted as a separate field.

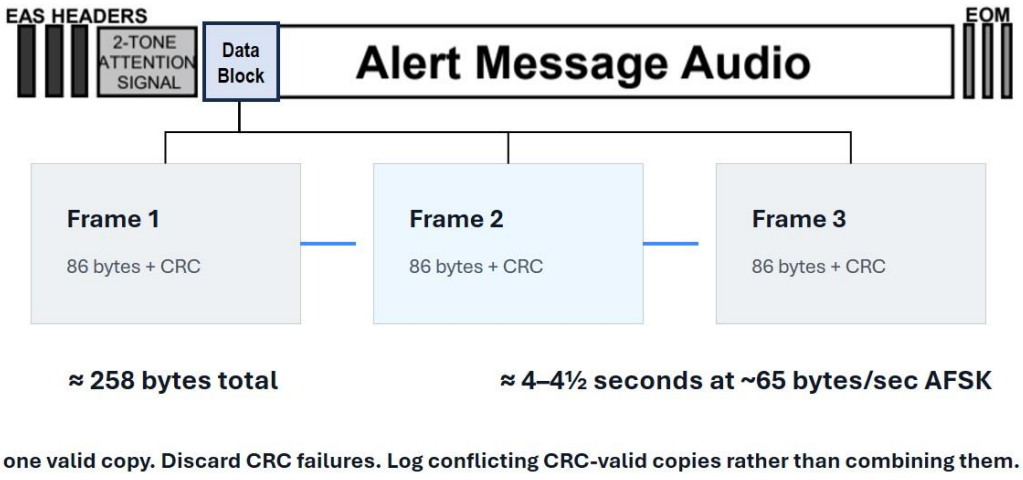
Each EDX frame should include a cyclic redundancy check (CRC) to identify transmission errors before signature validation. The CRC would not provide authentication nor replace the digital signature. Its function would be to enable the receiver to quickly determine whether a particular copy was corrupted during AFSK transmission. A compact CRC-16 would likely be sufficient for this purpose, as the digital-signature verification would provide an additional, and substantially stronger integrity check.

DAS recommends transmitting the complete EDX authentication frame three times. Each copy should be framed separately, and CRC-protected so that any one correctly received copy can be used for validation. The receiving device would accept the authentication object if at least one copy passes both the CRC check and digital-signature validation. Copies that fail the CRC would be discarded. If multiple CRC-valid copies contain conflicting information, the device should log and report the conflict rather than combine the inconsistent frames.

Using compact binary encoding, an individual frame could be approximately 86 bytes:

Field	Definition	Illustrative size
Version and flags	Identifies the EDX authentication-frame version and provides a small set of control bits indicating how the frame should be interpreted, such as message type or optional features.	2 bytes
Unique message identifier	A compact identifier assigned to the alert so the identical alerts can be recognized across CAP, legacy EAS, and other distribution paths, included for duplicate detection and correlation.	12 bytes
Key identifier	A short reference identifying the public key or certificate the receiving EAS device should use to validate the digital signature. This avoids transmitting the full certificate with every alert.	4 bytes
Four-digit year	Supplies the full year associated with the alert, resolving a limitation of the legacy EAS header and helping prevent ambiguity or replaying expired messages that may unknowingly queue devices.	2 bytes
Compact digital signature	A compact cryptographic signature generated using the authorized signer's private key over the defined EAS header and EDX metadata. The receiving device uses the Key ID to select the corresponding public key and verify both the integrity of the signed information and the signer's authority. A fixed-length elliptic-curve signature can provide this function in approximately 64 bytes.	64 bytes
CRC-16	A short cyclic redundancy check used to detect transmission errors in that individual EDX frame. It allows a corrupted copy to be rejected quickly before signature validation and is not used in message authentication.	2 bytes
Total		86 bytes

A complete, three-copy burst would require approximately 258 bytes, plus limited synchronization and framing overhead. At the existing EAS AFSK rate of approximately 65 bytes per second, the complete three-copy authentication burst could likely be transmitted in approximately **four to four-and-one-half seconds**. The precise duration would depend on the final framing and synchronization requirements.



The Commission should therefore pursue a fixed-format EDX authentication frame that uses compact identifiers, a compact digital signature, three complete repetitions, and per-frame CRC protection. This would provide three independent opportunities to receive all information needed for validation while keeping the added AFSK burst within a more operationally acceptable duration.

To optimize transmission efficiency, the EDX payload should carry only the information required for identification and validation. It should not ordinarily include a complete certificate chain, a full CAP message, or other information that receiving equipment can obtain or maintain separately. Compact identifiers, fixed-length digests, binary encoding, and appropriately sized signature mechanisms would minimize the size of the added data and therefore its duration while preserving the necessary security properties.

This approach also allows the message-identification and authentication functions to reinforce each other. A unique message identifier improves correlation and duplicate detection, but an unauthenticated identifier could be copied or deliberately misused to suppress a message improperly. A digital signature, in turn, is more operationally useful when it authenticates a persistent identifier that can be followed across CAP, legacy EAS, relay, and other dissemination paths. EDX provides a common envelope in which those complementary functions can travel together.

The Commission should therefore move to quickly evaluate EDX, not merely as a means of adding text to a legacy EAS transmission, but as a compact metadata and authentication layer. Properly structured, a EDX payload could provide legacy EAS with persistent message identity, signer identification, and cryptographic integrity without carrying large amounts of ancillary content.

4.3 Implementation Requirements and Cost Control

A useful identifier requires operational rules, not merely a new data field. The Commission should address preservation across paths where technically feasible; treatment of updates and cancellations; logging; conflicts, malformed IDs, and missing IDs; testing; and coordination among FEMA, NWS, EAS manufacturers, WEA stakeholders, State Emergency Communications Committees, and alert-origination vendors.

To minimize cost and complexity, the identifier should be globally unique, compact, machine-readable, automatically generated, CAP-compatible, version-aware, authenticated, path-agnostic, usable offline, backward-compatible, and independent of proprietary databases. A compact UUID-style, URN-style, or CAP-compatible equivalent could meet these objectives, with the exact format developed through standards work.

4.4 Recommended FCC Approach

DAS recommends a staged approach:

1. Require or encourage CAP-based EAS messages to include a stable message identifier within signed CAP content.
2. Develop a backward-compatible supplemental legacy mechanism, such as EDX, to carry the same identifier without modifying the existing EAS header format.
3. Require updated EAS equipment to log the identifier and use it for alert correlation when available.
4. After testing and transition, use authenticated identifiers as the primary duplicate-correlation mechanism, while retaining the current header-based logic as a fallback.
5. Coordinate preservation of the identifier across EAS, WEA, NOAA Weather Radio, and other public-warning channels whenever technically feasible.

Once properly implemented, a universal identifier would be an important building block for traceable, consistent, and trustworthy multi-path public warning.

5 Securing the Alert Message Is Only Part of Securing EAS

The Commission is appropriately focused on strengthening the authentication of EAS messages, including CAP-based alerts. Authentication is fundamental: an EAS Participant should be able to determine that a message came from an authorized source and has not been altered in transit. But message authentication protects the message payload. It does not, by itself, establish that the EAS system receiving, validating, processing, and transmitting that message is secure.

5.1 The need for a uniform security baseline.

DAS reaches this conclusion from experience. Over more than a decade, DAS has worked through vulnerabilities identified by independent security researchers and addressed in federal cybersecurity advisories, including US-CERT and later CISA processes involving DASDEC products. Public advisories in 2013 and 2022 identified vulnerabilities that required investigation, remediation, software updates, changes in security practices, and continuing customer guidance. DAS has also maintained a vulnerability-disclosure process, credited researchers who responsibly reported issues, issued patches, and repeatedly advised customers to isolate EAS equipment from the public Internet, maintain current software, disable unnecessary services, and use appropriate network protections. Those experiences have reinforced a practical lesson: EAS security cannot stop at verifying the authenticity of the message being received.

The security boundary must extend back to the EAS equipment itself. A properly authenticated alert can still be suppressed, delayed, mishandled, incorrectly routed, or improperly transmitted if the

implementation processing it has been compromised, misconfigured, or altered. Likewise, an EAS Implementation performing encoder functions may itself become a source of unauthorized or false alert activity if its software, firmware, credentials, configuration, interfaces, or update mechanisms are not adequately protected. CISA has specifically warned that exploitation of vulnerabilities in EAS equipment could result in false alerts being issued to connected broadcast or cable facilities. The Commission should therefore treat message authentication and EAS-system security as complementary requirements, not substitutes for one another.

DAS accordingly recommends that certified EAS systems be required to meet a uniform security baseline addressing secure development, authenticated software and firmware updates, configuration integrity, access control, logging, vulnerability management, supply-chain provenance, and applicable cybersecurity standards. Certification should provide assurance not merely that an implementation correctly recognizes and processes an authenticated EAS message, but that the system performing those public-warning functions is itself trustworthy and remains so throughout its operational lifecycle. A trusted alert cannot depend upon an untrusted EAS Implementation.

5.2 Recommendations for a Security Baseline for Certified EAS Solutions

The Commission should translate the principle above into concrete requirements for the systems that receive, validate, originate, process, and transmit EAS messages. DAS does not suggest that Part 11 become a general-purpose cybersecurity code, nor that the Commission prescribe a particular technical architecture. It should, however, establish minimum security expectations appropriate to equipment entrusted with a mandatory public-warning function. DAS has previously recommended secure software and firmware development, authenticated updates, hardened configurations, access controls, audit logging, vulnerability management, supply-chain integrity, and continuing security oversight for EAS systems.[11]

These requirements should attach to the certified EAS implementation, not merely to individual applications or message-processing functions. The objective should be straightforward: the Commission's certification process should provide reasonable assurance that the system entrusted with authenticated emergency messages is itself designed, deployed, maintained, and updated in a manner appropriate to public-safety infrastructure. The requirements should apply consistently to appliance, software, hybrid, or other implementations performing regulated EAS functions.

At a minimum, DAS recommends that the Commission establish the following baseline requirements:

[11] See Comments of Digital Alert Systems, PS Docket No. 25-224, Sept. 25, 2025 (“DAS 2025 Comments”), §§ 12.2–12.6, pp. 49–58.

1. **Secure development and product integrity.** Manufacturers should follow documented secure-development practices appropriate to critical infrastructure. Executable software and firmware should be integrity-protected, and production builds should be traceable to controlled development and release processes. DAS previously recommended controlled build environments, signed binaries, and secure software and firmware development practices.[12]

2. **Authenticated updates and lifecycle control.** EAS Implementations should accept only authenticated software and firmware updates and should reject altered or unauthorized packages. Manufacturers should maintain a defined security-support process, provide timely remediation of significant vulnerabilities, and establish procedures for determining when a material software, firmware, operating-system, or security change requires additional testing or certification review. DAS's earlier comments similarly called for digitally signed updates and continuing cybersecurity reassessment rather than treating certification as a one-time event.[13]

3. **Secure configuration and access control.** Certified implementations should ship in a reasonably secure configuration, avoid universal or default administrative credentials, minimize unnecessary services, protect security-sensitive configuration parameters, and support individual accounts with appropriate privilege separation. Changes affecting alert sources, geographic areas, event filters, authentication, forwarding behavior, network interfaces, or other material EAS functions should be attributable and auditable. These measures are consistent with the configuration and access-control protections DAS previously recommended.[14]

---

[12] DAS 2025 Comments § 12.2, pp. 49–50. Also See National Institute of Standards and Technology (NIST), Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities, NIST SP 800-218, Practices PS.1–PS.3, PW.1 & PW.4 (Feb. 2022) (addressing protection of software from unauthorized access and tampering, verification of software-release integrity, preservation of provenance information, secure software design, and security of third-party software components), doi:10.6028/NIST.SP.800-218; Cybersecurity and Infrastructure Security Agency (CISA) et al., Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software 3–10 (Oct. 2023) (urging technology manufacturers to take ownership of customer security outcomes and make security a core product requirement).

[13] DAS 2025 Comments §§ 12.2–12.4, pp. 49–53. See Modernization of the Nation's Alerting Systems et al., Report and Order and Further Notice of Proposed Rulemaking, FCC 26-38, paras. 13–22 (2026) (requiring EAS Participants to test and install manufacturer-provided security patches, software updates, and firmware updates promptly and observing that this requirement is consistent with CISA cybersecurity guidance); CISA, Cross-Sector Cybersecurity Performance Goals, CPG 2.B, "Mitigate Known Vulnerabilities" (recommending a vulnerability-management program to patch and mitigate vulnerable or misconfigured software in a timely manner); NIST, Security and Privacy Controls for Information Systems and Organizations, SP 800-53 Rev. 5, controls SI-2, Flaw Remediation, and SI-7, Software, Firmware, and Information Integrity (Sept. 2020, updated Aug. 2025), doi:10.6028/NIST.SP.800-53r5; NIST, Platform Firmware Resiliency Guidelines, SP 800-193 (May 2018), doi:10.6028/NIST.SP.800-193.

[14] DAS 2025 Comments § 12.2, pp. 49–50. See Modernization of the Nation's Alerting Systems et al., FCC 26-38, paras. 13–22 (2026) (requiring EAS Participants to change default passwords and use strong passwords for EAS

4. **Logging and accountability.** An EAS Implementation should maintain protected records sufficient to determine when alerts were received, generated, validated, rejected, retransmitted, or suppressed, as well as significant administrative access and configuration changes. Logs should support both regulatory compliance and cybersecurity investigation. This is particularly important because an attack on EAS may appear first as an anomalous configuration change or unexpected alert-processing event rather than a conventional equipment failure.[15]

5. **Vulnerability management and coordinated disclosure.** Manufacturers should maintain an accessible process for receiving vulnerability reports from researchers, customers, CISA, and other responsible parties; evaluate reported vulnerabilities promptly; communicate material risks to affected users; and provide remediation when appropriate. DAS's own experience with independent researchers and federal cybersecurity processes demonstrates that vulnerabilities will be found over the life of a product. The regulatory objective should be to ensure that manufacturers have the capability and obligation to respond when that occurs. DAS previously recommended formal vulnerability-disclosure and timely patching practices.[16]

6. **Network and interface security.** EAS equipment should not be designed or deployed on the assumption that an internal broadcast network is inherently trusted. The Commission should require manufacturers to provide secure deployment guidance and should reinforce existing practices involving network segmentation, restricted remote administration, protection against unnecessary Internet exposure, and secure communications for sensitive functions. DAS

---

equipment and certain related systems); CISA, Cross-Sector Cybersecurity Performance Goals, CPG 3.A, "Changing Default Passwords"; NIST, Security and Privacy Controls for Information Systems and Organizations, SP 800-53 Rev. 5, controls AC-2, Account Management, AC-6, Least Privilege, CM-6, Configuration Settings, and CM-7, Least Functionality (Sept. 2020, updated Aug. 2025), doi:10.6028/NIST.SP.800-53r5.

[15] DAS 2025 Comments §§ 12.1–12.2, pp. 47–50; § 12.6, pp. 57–58. See NIST, Security and Privacy Controls for Information Systems and Organizations, SP 800-53 Rev. 5, controls AU-2, Event Logging, AU-3, Content of Audit Records, AU-6, Audit Record Review, Analysis, and Reporting, AU-9, Protection of Audit Information, and AU-12, Audit Record Generation (Sept. 2020, updated Aug. 2025), doi:10.6028/NIST.SP.800-53r5; CISA et al., Enhanced Visibility and Hardening Guidance for Communications Infrastructure (Dec. 3, 2024) (recommending secure centralized logging of authentication, authorization, and accounting information, configuration tracking and auditing, and enhanced monitoring of communications infrastructure).

[16] DAS 2025 Comments § 12.2, p. 50; § 12.6, pp. 57–58. See NIST, Recommendations for Federal Vulnerability Disclosure Guidelines, SP 800-216 (May 2023) (recommending formal processes to receive, assess, manage, and communicate remediation of reported vulnerabilities), doi:10.6028/NIST.SP.800-216; NIST, Secure Software Development Framework (SSDF) Version 1.1, SP 800-218, Practices RV.1–RV.3 (Feb. 2022) (addressing identification, analysis, remediation, and disclosure of vulnerabilities), doi:10.6028/NIST.SP.800-218; CISA et al., Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software (Oct. 2023) (calling for manufacturer transparency and accountability concerning product vulnerabilities).

previously identified direct Internet exposure, weak credentials, and inadequate segmentation as continuing EAS security concerns.[17]

7. **Supply-chain transparency and integrity.** Certification should address the provenance and integrity of security-relevant hardware, firmware, software, libraries, and update mechanisms. Manufacturers should maintain sufficient component and supplier information to identify exposure when a component or supplier is later determined to present a vulnerability or national-security risk. DAS previously recommended SBOMs, component traceability, authenticated update mechanisms, disclosure of relevant manufacturing and software-development sources, and identification of components obtained from government-designated high-risk vendors.[18]

8. **Independent verification and continuing oversight.** Security requirements have limited value if compliance is established only through manufacturer assertion. The Commission should develop objective conformity criteria and require appropriate independent testing or verification as part of certification, with additional review following material changes and periodic reassessment where necessary to address evolving threats. DAS previously recommended third-party conformance testing and continuing recertification for security-sensitive EAS equipment.[19]

---

[17] See Modernization of the Nation's Alerting Systems et al., FCC 26-38, paras. 13–22 (2026) (requiring EAS Participants to place EAS equipment and specified remotely managed systems behind a properly configured firewall or use comparable network segmentation and identifying such segmentation as an established cybersecurity best practice); CISA, Cross-Sector Cybersecurity Performance Goals, CPG 3.S, "Secure Internet Facing Devices"; NIST, Security and Privacy Controls for Information Systems and Organizations, NIST SP 800-53 Rev. 5, controls SC-7, Boundary Protection, AC-17, Remote Access, and CM-7, Least Functionality (Sept. 2020, updated Aug. 2025), doi:10.6028/NIST.SP.800-53r5; CISA et al., Enhanced Visibility and Hardening Guidance for Communications Infrastructure (Dec. 3, 2024) (recommending strong network segmentation, default-deny access controls, trusted management networks, elimination of unnecessary Internet-facing services, and restrictions on Internet-based device management). *Also see DAS 2025 Comments § 12.1, pp. 47–48; § 12.6, pp. 57–58.*

[18] See DAS 2025 Comments §§ 12.4–12.5, pp. 50–56. *See* NIST, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, SP 800-161 Rev. 1, Update 1 (Nov. 2024) (addressing risks from malicious functionality, counterfeit components, vulnerable products, inadequate development and manufacturing practices, and limited visibility into technology supply chains), doi:10.6028/NIST.SP.800-161r1-upd1; NIST, Secure Software Development Framework (SSDF) Version 1.1, SP 800-218, Practices PS.3 and PW.4 (Feb. 2022) (addressing software provenance and security of acquired and third-party software components), doi:10.6028/NIST.SP.800-218. *See also* 47 C.F.R. § 2.907(c) (requiring equipment produced by an entity identified on the FCC's Covered List that otherwise would qualify for Supplier's Declaration of Conformity or exemption to obtain authorization through the certification process).

[19] See NIST, Assessing Security and Privacy Controls in Information Systems and Organizations, NIST SP 800-53A Rev. 5 (Jan. 2022, updated Aug. 2025) (establishing methodologies and procedures for assessing whether security controls are implemented correctly, operating as intended, and producing the desired security outcomes), doi:10.6028/NIST.SP.800-53Ar5; NIST, Security and Privacy Controls for Information Systems and Organizations, NIST SP 800-53 Rev. 5, control CA-2, Control Assessments, including CA-2(1), Independent Assessors (Sept. 2020,

The Commission does need to specify the particular technical means by which every manufacturer satisfies these requirements. Secure boot, hardware roots of trust, cryptographic signing, protected key storage, attestation, or other controls may be appropriate depending upon the implementation. The regulatory requirement should instead establish the security outcome: a certified EAS Implementation must have an identifiable security boundary, resist unauthorized modification and access, provide evidence of material activity and changes, support secure remediation, and remain accountable to a manufacturer throughout its supported lifecycle.

Most importantly, these requirements should be incorporated into the certification of the EAS Implementation rather than left solely to deployment recommendations for EAS Participants. Broadcasters and cable operators certainly have responsibilities for securing their facilities, but the security of a federally required public-warning system cannot depend on thousands of individual Participants independently assembling the protections necessary to make the underlying EAS product trustworthy. The Commission is strengthening authentication so that EAS equipment can trust the message. It should take the complementary step of ensuring that the public, EAS Participants, and the government can trust the equipment that acts on it.

DAS supports the proposal to permit, but not require, EAS Participants to use detailed geographic information in CAP messages, including circles and polygons, when deciding whether and how to transmit state and local EAS alerts.[20]

6 Geographic Naming

6.1 Use of Familiar and Understandable Names for EAS Alert Areas

Digital Alert Systems supports the Commission's proposal to permit EAS location codes to correspond to geographic names that are meaningful and readily recognizable to the communities receiving an alert. The effectiveness of an emergency warning depends not merely upon identifying the correct geographic area, but upon communicating that area in terms the public can immediately understand. As the FCC rightly observes, a technically accurate description such as "Southwest Monroe County" may provide little useful information to a person who knows the affected community as "Key West." The Commission

updated Aug. 2025), doi:10.6028/NIST.SP.800-53r5; 47 C.F.R. §§ 2.907(a), 2.960(a) (providing for FCC equipment certification based on representations and test data and requiring recognized TCBs to satisfy applicable ISO/IEC 17065 accreditation requirements, demonstrate technical testing competence, and demonstrate impartiality). See also 47 C.F.R. § 2.909(a) (providing that the grantee of an equipment certification is responsible for the equipment's compliance with applicable technical and other requirements). See DAS 2025 Comments § 12.3, p. 50; § 12.4, pp. 51–53; § 12.6, pp. 57–58

[20] FCC 26-38, paras. 70-72.

appropriately recognizes that such ambiguity can leave recipients uncertain whether an alert applies to them.

This proposal should be understood primarily as an improvement in EAS message presentation and intelligibility, rather than as a new form of EAS geofencing. The existing EAS location-code mechanism provides a standardized means of identifying geographic areas; associating additional codes with familiar community names would permit EAS equipment and downstream systems to render those locations in more useful, understandable terms. For DAS, adjusting the text correlating with a location code could be accomplished simply by software update.

The Commission's proposal appropriately builds upon the existing legacy EAS location-code architecture while addressing a significant limitation of the current partial-county construct. Existing PSSCCC geocodes can identify a county or one of nine generally directional subdivisions, but those descriptions do not necessarily correspond to the names by which communities understand themselves. Permitting additional EAS location codes to identify familiar localities, such as "Key West," would allow the geographic description carried through legacy EAS to correspond more closely to the terminology understood by the public. This is not polygon-based geofencing; rather, it is an improvement to the geographic vocabulary available within the EAS protocol. Any such codes should be standardized, publicly documented, and implemented consistently across EAS equipment so that alert originators, Participants, and downstream presentation systems interpret them identically.

6.2 Implementation Considerations

From an EAS equipment perspective, the first approach should be particularly straightforward. The DASDEC can readily support additional recognized PSSCCC location codes through a routine software update. Much of the functionality involved is fundamentally table-driven: a particular EAS geographic code is associated with a defined geographic area and a corresponding human-readable name. The same new code can likewise be recognized in CAP processing and encoded or decoded in legacy EAS. Thus, the Commission can substantially improve the usefulness of alert-area descriptions without introducing the complexity associated with polygon-based targeting.

Expanding the existing PSSCCC mechanism may also be technically feasible but deserves somewhat greater consideration because the existing protocol defines the subdivision character as a numeric value. In particular, the Commission should preserve a clear path for eventual National Weather Service implementation. NWS and EAS presently share the SAME/EAS location-code structure, and NWS-originated warnings remain an important source of EAS messages.

The Commission therefore should not design a new locality-identification mechanism solely around what current EAS encoder/decoder equipment can readily accommodate. Rather, any new mechanism should be standardized and implemented so that NWS can subsequently adopt and originate messages using the same codes when it is operationally prepared to do so. This need not delay useful

improvements to EAS, but it does counsel in favor of an architecture that maintains compatibility and avoids creating separate or competing geographic vocabularies for EAS and NWS.

7 EAS Geofencing and Geotargeting

DAS generally supports the concept to permit, but not require, EAS Participants to consider more detailed geographic information in CAP messages (including circles and polygons)hen deciding whether, and through which outputs, to relay state and local EAS alerts.[21] Used appropriately, such information could make the upstream relay decision more geographically informed than county-based FIPS filtering alone.

At the same time, conventional broadcast EAS has inherent geographic limitations. EAS devices ordinarily filter alerts using FIPS codes, which generally correspond to counties or county-equivalent areas; the legacy EAS Protocol permits no more than 31 location codes in an alert.[22] Once a radio or television station transmits an EAS message, however, that message is carried to all receivers tuned to the service within the station's transmission area. The message cannot be limited to receivers located within a CAP polygon. The same practical limitation applies to a cable system throughout the area served by the affected channel or system.

A polygon therefore could be used only to improve the decision whether a particular station, transmitter, cable system, or other EAS output should relay an alert, not to target the resulting broadcast to particular receivers. To do so reliably, an EAS implementation would need to compare the CAP geometry with an established geographic representation of the relevant output's coverage or service area, and apply a defined relay policy. That entails maintaining and validating coverage profiles; accounting for multiple transmitters, translators, multicast streams, and nonstandard service areas; establishing conservative rules for marginal or uncertain overlap; and retaining sufficient logging to explain the resulting decision.

These functions are technically achievable, but they are not costless or self-executing. The Commission should carefully consider the development, data-maintenance, configuration, support, and ongoing compliance burdens on both EAS Participants and EAS system providers, as well as the need for interoperable implementation rules. In light of the fact that a conventional EAS transmission will still reach the entire service area once initiated, the Commission should determine whether the incremental benefit of polygon-based relay selection warrants those additional burdens in particular use cases.

---

[21] ibid.

[22] 47 C.F.R. § 11.31(c).

7.1 Distinct Forms of Geotargeting

The Commission should distinguish among three functions:

- **Transmit-decision geotargeting.** An EAS Participant uses CAP geometry to determine whether an alert is sufficiently relevant to its service area to warrant transmission.
- **Distribution path geotargeting.** A cable, IPTV, ATSC 3.0, HD Radio, or other digital platform uses geometry to route or present alert information through specific services, zones, streams, or data paths.
- **Receiver-level geofencing.** A location-aware receiver or application presents alert information only when it determines it is within or near the affected area.

Legacy EAS can support the first function. Some digital distribution platforms can support the second. Services like ATSC 3.0's Advanced Emergency Information can support more refined receiver- or application-level presentation where broadcaster and receiver implementations provide the necessary capabilities.

7.2 CAP Geometry and the Legacy EAS Path

CAP polygons and circles can improve relay decisions, ATSC 3.0 AEI generation, logging, and correlation. The full geometry should generally remain in CAP or another higher-capacity data environment. It should not be inserted into the legacy FSK header stream or treated as ordinary payload for a compact supplemental packet. Complex polygon data can be too large for the constrained legacy audio path, potentially adding delay and reducing robustness.

A supplemental packet should instead carry compact metadata, such as a universal message ID, CAP identifier, geometry hash, canonical legacy-header hash, signer or relay identifier, or an indication that an authorized node evaluated the CAP geometry. A compact bounding box, centroid and radius, or predefined state zone may also be useful in limited cases.

For a Local Primary relay, the device could evaluate the authenticated CAP polygon, generate the legacy alert, and create a relay attestation binding the legacy header to the CAP message and its geometry. Downstream devices could correlate the relay with the full CAP alert through the message ID, CAP identifier, or geometry hash, without forcing the legacy path to carry the polygon itself.

7.3 ATSC 3.0 Advanced Emergency Information

ATSC 3.0 provides a technically suitable broadcast television path for richer emergency information. The ATSC Advanced Emergency Information implementation framework is complementary to, not a

replacement for, required EAS compliance. It supports features such as wake-up signaling, geotargeting, personalization, rich media, accessibility, broadcaster applications, and companion-device delivery.[23]

A broadcaster could receive a CAP alert containing circles or polygons, perform the required EAS processing, and generate AEI content that contains geometry, identifiers, text, audio, maps, multilingual material, and other supplemental information. A location-aware receiver or broadcaster application could then make a more refined presentation decision. The Commission should recognize this capability without requiring every ATSC 3.0 broadcaster to implement AEI on a common timetable.

7.4 HD Radio and Other Digital Audio Paths

Digital radio can also support richer alert information than analog legacy EAS. NRSC guidance describes an HD Radio Emergency Alerts workflow in which an alert processor receives CAP or legacy content, converts it to the HD Radio alert format, and provides information that compatible receivers can present. This does not mean every receiver or station can perform polygon geofencing today, but it supports continued development of more relevant digital-radio alert presentation.[24]

The Commission should avoid rules that freeze EAS geotargeting around legacy county codes when newer broadcast and application technologies can use CAP geometry more effectively.

8 Promoting the Use of Symbols for Alerts

DAS supports the Commission's inquiry into standardized symbology for EAS and WEA. Well-designed visual symbols can improve rapid recognition, assist people with limited English proficiency, support accessibility, and reduce reliance on text alone. Symbols should supplement alert text and audio, not replace them.[25]

DAS recommends a voluntary, standards-based approach at this stage. The Commission should encourage a harmonized symbol framework, preloaded symbol libraries, compact identifiers, and technology-appropriate implementation, while avoiding a near-term requirement that every EAS Participant or Participating CMS Provider display symbols in an identical manner.

8.1 VIDS and NAPSG as Reference Frameworks

The NAPSG public alert and warning symbol library provides an important foundation. The NVISA Visually Integrated Display Symbology (VIDS) Recommended Practices add a broadcast and video

---

[23] Advanced Television Systems Committee, ATSC 3.0 Advanced Emergency Information System Implementation Guide (Feb. 22, 2019); FCC 26-38, paras. 70-72.

[24] National Radio Systems Committee, NRSC-G300-C, Radio Data System (RDS) Usage Guideline, § 8.3 (2020).

[25] FCC 26-38, paras. 78-82.

presentation layer, including event grouping, high-contrast banners, symbol placement, display duration, and optional persistence for high-impact alerts.[26]

For EAS and other video services, the implementation layer matters as much as the symbol itself. The Commission should seek harmonization among NAPSG, FEMA, NWS, VIDS, accessibility stakeholders, WEA stakeholders, ATSC participants, broadcasters, Commercial Mobile Service providers, and equipment manufacturers, rather than endorsing conflicting symbols for the same hazard.

DAS supports the Commission's consideration of FEMA/NAPSG public alert and warning symbols. The FEMA/NAPSG work provides a valuable foundation because it is publicly available, federally supported, and grounded in public-safety GIS and incident-management practice. It offers a common starting point for emergency symbols. However, the FEMA/NAPSG library should not be treated as a complete EAS or video-alert display framework. It was developed principally for incident mapping, GIS displays, emergency operations centers, and related public-safety uses. Those settings typically include labels, legends, map layers, trained users, and other supporting context.

Public-facing EAS and video displays present a different problem. A viewer may see an alert symbol briefly, at a distance, under stress, and in combination with moving or time-limited text. In that environment, the symbol set must be complete, visually distinct, legible on screen, and tied to practical display rules. This is where NVISA's Visually Integrated Display Symbology, or VIDS, adds important value. VIDS is a publicly available, vendor-neutral, industry-consortium recommended practice for integrating emergency-alert symbols with text in video and display environments.

NVISA's VIDS approach builds on the FEMA/NAPSG library. VIDS expressly derives from the NAPSG public alert and warning symbols but adapts that foundation for display systems that combine graphics and text, including EAS, ATSC 3.0 Advanced Emergency Information, digital signage, web apps and similar video-based alerting systems. FEMA's own IPAWS Tip 36 recognizes this relationship, noting that VIDS incorporates the IPAWS symbol set "with some minor adjustments" to enhance emergency-alert accessibility.[27]

In NVISA's review, the FEMA/NAPSG set lacks distinct symbols for several EAS-relevant event types and, in some cases, uses the same symbol for materially different alerts. That may be workable in a GIS environment where the user has labels, map context, and professional training. It is less suitable for

[26] National Alliance for Public Safety GIS Foundation, Symbol Library; FEMA, IPAWS TIP 36: The IPAWS Symbol Set (Apr. 2021); NextGen Video Information Systems Alliance (NVISA), Visually Integrated Display Symbology (VIDS): WG-1 Recommended Practices, NVISA-WG-1-001.01, rev. 1.2, (Jan. 12, 2021) https://www.nvisa.org/documents.
[27] TIP 36: The IPAWS Symbol Set (April 30, 2021), https://www.fema.gov/sites/default/files/documents/fema_tip-36-symbology.pdf

public-facing video alerting, where repeated symbols can blur distinctions between different hazards and missing symbols can force manufacturers or broadcasters to improvise.

VIDS addresses those limitations by filling symbol gaps, reducing repeated-symbol ambiguity, and modifying several symbols to make them more legible, approachable, and understandable on screen. These changes are not a competing symbol universe. They are an application profile: the FEMA/NAPSG vocabulary refined for EAS and video presentation.

The distinction can be stated simply that FEMA/NAPSG supplies the federally supported public-alert symbol vocabulary, and NVISA VIDS supplies the EAS/video presentation profile. That model resolves the existence of two related symbol sets without fragmenting public-warning iconography. It allows the Commission to rely on the FEMA/NAPSG foundation while recognizing that VIDS is better suited to the actual EAS/video implementation problem.

VIDS also provides a critical element that a raw symbol library does not – it provides display grammar. It addresses how symbols appear with alert text, how alerts are grouped by urgency, how symbols are positioned, how large they should be, how they relate to banners and crawls, and when a symbol may persist after text has disappeared. Those issues are central to EAS, cable, ATSC 3.0 AEI, digital signage, and other public-facing video environments.

Accordingly, DAS recommends that the Commission recognize FEMA/NAPSG as the appropriate source vocabulary, while recognizing NVISA VIDS as the preferred EAS/video application profile because it:

1. builds from the FEMA/NAPSG foundation;
2. fills gaps where FEMA/NAPSG lacks symbols for EAS-relevant event types;
3. reduces ambiguity where FEMA/NAPSG uses the same symbol for different alerts;
4. modifies symbols for clearer on-screen recognition;
5. provides display guidance for text, icon placement, size, color, persistence, and severity grouping; and
6. is specifically directed to systems such as EAS, ATSC 3.0 Advanced Emergency Information, digital signage, cable displays, and other video-based alerting environments.

The Commission should therefore avoid endorsing only a raw symbol library and leaving each manufacturer, broadcaster, cable operator, and display system to determine how those symbols should appear. That would risk fragmentation under the banner of standardization. Rather, FEMA/NAPSG provides the government-supported symbol foundation, while VIDS adapts and completes that foundation for public-facing EAS and video alert presentation. VIDS is best understood as a publicly available, vendor-neutral recommended practice, not a proprietary product and not merely a symbol

library. It is an EAS/video presentation profile that adapts the FEMA/NAPSG symbol vocabulary for public-facing alert displays.

8.2 Preloaded Libraries and Reliable Delivery

Symbols should be preloaded wherever feasible. Transmitting full image files with every alert could increase latency, bandwidth, reliability, and compatibility burdens. A better approach is to transmit an event code, symbol identifier, or compact reference and allow the EAS device, mobile operating system, ATSC 3.0 application, or downstream graphics system to render the corresponding local asset.

Alert delivery must remain primary. If a device lacks the symbol library or receives an unknown identifier, it should still present the alert through required text, audio, attention signals, vibration, or other supported mechanisms. Legacy EAS should not be required to carry raster images in the FSK or audio path; downstream equipment should generate symbols locally.

8.3 Voluntary, Phased Implementation

EAS and WEA have different technical chains and user interfaces. EAS may involve an encoder/decoder, CAP polling, automation, character generation, media keying, cable insertion, ATSC 1.0 or 3.0 workflows, and compliance logging. WEA involves carrier networks, device manufacturers, mobile operating systems, notification interfaces, and accessibility settings. A single mandatory presentation rule is unlikely to fit both systems well.

The Commission can nevertheless advance deployment by recognizing approved symbol sets, encouraging manufacturers to support preloaded libraries and identifiers, supporting standards work, and providing a safe harbor for implementations that follow recognized practices. Voluntary requirements should be reconsidered only after additional testing and deployment experience.

8.4 Public Comprehension and Accessibility Testing

The Commission notes that a prior study involving 16 people who were Deaf and primarily used American Sign Language found that NAPSG symbology did not improve understanding of the event or recommended protective action. That limited result should be taken seriously, but it does not justify abandoning symbology. It supports further testing, consistent pairing of symbols with text, and repeated public exposure.[28]

An alternative conclusion is that symbols must be tested, paired with text, integrated into consistent presentation, and repeatedly exposed to the public over time. A symbol that is unfamiliar to a participant in a research setting may not instantly improve comprehension. But a well-designed,

[28] FCC 26-38, para. 80 and nn.263-64 (describing the Rehabilitation Engineering Research Center for Wireless Inclusive Technologies study).

consistently used symbol can become more meaningful through repeated public exposure, just as traffic signs, weather icons, and warning labels gain meaning through familiarity.

Testing should include people with disabilities, people with limited English proficiency, Deaf and hard-of-hearing users, older adults, children, and users responding under stressful conditions. The objective should be semantic clarity and accessibility, not the assumption that an unfamiliar icon will be self-explanatory on first exposure.

8.5 Persistence and Multiple Simultaneous Alerts

Persistent display may be useful for high-urgency or high-impact events because it can alert viewers who tune in after the crawl has ended. Persistence should remain optional and should not apply indiscriminately to every watch, advisory, informational message, or test.

When multiple alerts are active, systems should use a priority-based approach. The highest urgency symbol may take precedence; other alerts may be rotated, placed in a limited icon tray, or indicated a summary where technology permits. Full details should remain available through the crawl, AEI, an application, or another supplemental path, and logs should retain each alert independently.

8.6 EAS and WEA Implementation

A practical EAS workflow would map the EAS event code, CAP event type, CAP parameter, or future symbol identifier to a preloaded asset and instruct the character generator, media keyer, automation system, or AEI generator to display it with the alert text. DASDEC systems already aggregate alert-related media and support symbology workflows, demonstrating that the capability can be implemented without transmitting a complete image file with each alert.

For WEA, symbols should be rendered by the device or operating system using standardized metadata, without reducing text legibility or interfering with screen readers, font scaling, high-contrast, or other accessibility settings. The Commission should define the public-safety objective but avoid prescribing detailed mobile user interface behavior that is better handled by platform and device designers.

8.7 Standards and Recommended FCC Approach

Standards work should address a symbol identifier registry, event-code mapping, CAP parameter guidance, interfaces between EAS devices and downstream display systems, ATSC 3.0 AEI presentation, WEA rendering, accessibility, persistence, simultaneous alerts, logging, and fallback behavior. The Commission need not place every technical detail in Part 11; it can recognize external standards and recommended practices while preserving regulatory flexibility.

DAS recommends that the Commission:

1. endorse standardized emergency alert symbology and a harmonized reference framework;
2. encourage voluntary, phased implementation using preloaded libraries and compact identifiers;

3. require that symbols remain supplemental and never delay or prevent delivery of the underlying alert;
4. support accessibility and comprehension testing across diverse populations;
5. avoid requiring transmission of image files through constrained legacy alert paths; and
6. revisit mandatory display requirements only after standards development and meaningful deployment experience.

9 Conclusion

The Commission's proposals address a common objective: improving the trustworthiness, precision, consistency, and usability of public warning without weakening the reliability of the existing EAS architecture. DAS supports closing the unsigned-CAP gap, developing role-based authentication for legacy alerts, creating an authenticated universal alert identifier, permitting CAP geometry to improve relay decisions, and advancing standardized symbology through a voluntary and standards-driven process.

These initiatives should be implemented with clear certification boundaries, backward compatibility, offline operability where necessary, disciplined testing, and coordination among FEMA, NWS, state and local alerting authorities, State Emergency Communications Committees, EAS Participants, manufacturers, standards bodies, and accessibility stakeholders. Properly structured, the proposals can strengthen both legacy EAS and the richer alerting systems developing around it.