

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

In the Matter of )  
 )  
 ) PS Docket No. 25-224  
Modernizing the Nation’s Alerting Systems )  
 )

**COMMENTS OF DIGITAL ALERT SYSTEMS  
REGARDING THE NOTICE OF PROPOSED RULEMAKING -  
MODERNIZING THE NATION’S ALERTING SYSTEMS**

**Contents**

1	Introduction .....	1
2	Goals and First Principles .....	2
2.1	Goals of the Emergency Alert System .....	3
2.2	A Fuller Framework for the FCC’s Listed Goals .....	4
2.3	Digital Alert Systems’ efforts to achieve these additional objectives .....	6
2.4	Public Warning Objectives, Outcomes, and Metrics .....	9
3	The Paradox of EAS as an Unfunded Public Service Mandate .....	11
3.1	EAS as an Unfunded Mandate .....	11
3.2	The Paradox: Expanding Public Benefits, Expanding Private Burdens .....	11
3.3	Implications for Public Safety and Industry .....	12
3.4	Recommendations .....	12
4	National Level Alerting .....	14
4.1	Core Design Principles for Presidential-Level Alerting .....	15
4.2	Video-Based Alerts: Foundational Considerations .....	15
4.3	Stakeholder and Cost Considerations for Video-Based Alerting .....	16
4.4	Recommendations/Conclusion .....	17
5	The Effectiveness of EAS: State and Local Alerting .....	20
5.1	Where EAS is effective today .....	20
5.2	Where agencies still hit limits .....	21
5.3	Video Alerting for SLTT Agencies .....	21
5.4	Recommendations .....	21
6	Recommendations to Move to an “Enhanced EAS” .....	23
6.1	Near-Term Steps .....	23
6.2	Enhancing Relay/Transmission Capabilities of EAS .....	24
6.3	Maintaining the Focus of EAS .....	26

6.4 Recap and Recommendations for Enhancing EAS.....26

7 Pushing the Boundaries of EAS and WEA .....28

7.1 Maintaining a Line between Emergency Alerting and Emergency Information .....28

7.2 Comparing Scenarios and Tools.....29

7.3 The Role and Value of EAS in an Evolving Landscape.....30

8 Machine-to-Machine (M2M) Alerting.....32

8.1 M2M Communication .....32

8.2 Sensor-to-EAS Automation.....33

8.3 Transparency and Governmental Oversight .....34

9 EAS: Guaranteed Delivery or Best Efforts? .....36

9.1 EAS as a Hybrid: More than Best Efforts, But Less than Guaranteed. ....36

9.2 Enhancing EAS Performance .....37

9.3 Voluntary versus Mandatory Participation.....38

10 The Resilience of EAS Under “All Conditions” .....39

10.1 Resiliency Approaches That Achieve National Objectives .....40

10.2 Conclusion.....42

11 Are there other alternative communications pathways that EAS and WEA can leverage to ensure redundancy?.....43

11.1 Expanding Redundancy in EAS Dissemination. ....43

11.2 Should EAS and WEA both be independently resilient (i.e., having multiple redundant pathways within EAS)?.....45

12 Security of the Nation’s Alerting Systems.....47

12.1 Security Posture.....47

12.2 Securing the Nation’s Alerting Systems: The Role of EAS Device Manufacturers and Standards 49

12.3 Importance of Certified, Standards-Conformant Equipment.....50

12.4 Supply Chain Integrity for Core EAS Equipment .....50

12.5 Precedents for Supply Chain Integrity Policy .....53

12.6 Minimum Cyber Hygiene Checklist for EAS Participants and Devices .....57

13 Modernizing the EAS for Greater Public Impact.....59

13.1 Improving the EAS Textual Display .....59

13.2 Harmonizing the Visual Presentation of EAS .....61

13.3 Enhancing EAS Displays with Symbology .....61

14 Are Traditional EAS Alert Delivery Channels Still Representative of Modern Media Consumption? 63

14.1 Traditional Platforms Retain an Important Role.....63

14.2 The Shift Toward Streaming and Digital Platforms .....63

14.3 Implications for EAS Objectives.....64

14.4 Conclusion.....65

15 Effectiveness of EAS in the Context of Changing Media Habits .....66

15.1 What can the Commission do under its current legal authority? .....66

15.2 Minimum requirements to preserve trust in expanded systems .....67

15.3 Conclusion.....67

16 Evaluating End-User Device–Centric Alerting in the Nation’s Alert and Warning Systems .....68

16.1 Risks and Constraints of End User Device-Centric Design.....69

16.2 The Continuing Key Role of EAS.....69

16.3 A Balanced Path Forward.....70

17 Does EAS Meet the Needs and Expectations of the Public and Alerting Authorities? .....72

17.1 Where EAS Remains Useful and Effective .....72

17.2 Recommendations .....73

17.3 Conclusion: Preserve EAS While Enabling Evolution.....75

18 Testing, Training, and Collaboration on Public Warning .....77

18.1 Recommendations on National / Regional EAS Testing.....78

18.2 An Additional Concept for National Readiness Testing .....79

19 Conclusion .....82

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

In the Matter of	)	
Notice of Proposed Rulemaking - PS Docket	)	PS Docket No. 25-224
Modernizing the Nation's Alerting Systems	)	

**COMMENTS OF DIGITAL ALERT SYSTEMS  
REGARDING NOTICE OF PROPOSED RULEMAKING ON  
MODERNIZING THE NATION'S ALERTING SYSTEMS**

**1 Introduction**

Digital Alert Systems (“DAS”) respectfully submits these comments in response to the Commission’s ongoing inquiry into the future of the Emergency Alert System (EAS). We commend the Commission for its leadership in advancing public alert and warning and share the vision of evolving the EAS into a system that ensures guaranteed delivery, supports video and multimedia alerting, and meets the multilingual and accessibility needs of today’s diverse audiences.

As the leading developer of advanced FCC-certified EAS encoder/decoder platforms, Digital Alert Systems has a unique perspective on both the technical feasibility of these enhancements and the economic realities facing a wide range of EAS participants.

The Commission’s inquiries into modernizing the Emergency Alert System are both timely and commendable. As public expectations evolve and communications technologies advance, it is appropriate to ask how EAS can be made more effective, accessible, and resilient. We support many of these directions—such as the possible incorporation of clear symbology and iconography to improve comprehension across diverse populations, enhancing security, and more precise geographic targeting to reduce over-alerting and increase public trust.

At the same time, some of the questions under consideration raise significant challenges in the current framework. The EAS remains, at its core, an unfunded mandate. It is a system in which private EAS participants bear the costs of regulatory obligations. An often-overlooked issue is that EAS manufacturers also carry significant burdens and risks, as they must rapidly innovate to

meet new regulatory expectations while ensuring affordability, backward compatibility, and reliability in a market that is entirely compliance-driven.

Advancing into some of the complex capabilities raised by the Commission, such as guaranteed delivery, video-based alerting, and multilingual services, risks pushing this alerting ecosystem to the breaking point. Without a funding mechanism, expanding the public mission and capabilities of EAS while leaving both participants and manufacturers to shoulder the weight. The Commission needs to balance what can be realistically approached in an unfunded, voluntary ecosystem.

Yet it is critical to stress that the EAS continues to provide indispensable utility and necessity—fundamentally supporting the nation’s public warning goals, even under the most challenging environments when other systems may fail.

## **2 Goals and First Principles**

The FCC seeks comments on the objectives that effective alert and warning systems should serve. Based on our experience in overseeing requirements for EAS and WEA, the Commission identifies and is seeking comments on what it lists as the following three goals:

- (1) alerting systems should provide authorities with the ability to rapidly notify the public of emergencies that may put the public at risk;
- (2) alerting systems should be capable of delivering instructions that facilitate the protection of life and property; and
- (3) alerting systems should provide a mechanism for government officials to provide additional authoritative communications with the public before, during, and after an emergency.

We would suggest that the above points frame a *mission statement* for the nation’s public warning systems, which flow from a core *first principal* that safeguarding life and property:

*The foremost duty of the nation’s public warning systems is to safeguard human life and protect property by ensuring the reliable, timely, and effective dissemination of emergency information.*

## 2.1 Goals of the Emergency Alert System

In short, those above three goal statements are directionally valid, but in our opinion, do not fully suffice as “core goals.” They capture speed, actionability, and continuity of official communication. To stand as first-principal objectives for EAS (and, by reference, WEA), they should explicitly add precision, ubiquity/accessibility, security/trust, and resilience/interoperability. We respectfully encourage the FCC to consider this reframing in its NPRM.

We suggest a more precise – though expanded - articulation of the goals of the Emergency Alert System might include:

1. **Rapid, reliable, authenticated reach to the right people.** Deliver authenticated alerts quickly to the audience *actually at risk* (precision geo-targeting for WEA; appropriate service contours/FIPS targeting for EAS). The nation’s alerting systems must deliver authenticated warnings with minimal latency to the people who are actually at risk, consistent with each system’s technical capabilities.
2. **Actionable, accessible instructions.** Provide plain-language protective actions, with required informational elements (hazard, location, action, expiry, sender) and support for accessibility/multilingual needs. Alerts must include the key informational elements needed to drive protective action and must be accessible to people with disabilities and those with limited English proficiency.
3. **Lifecycle communication, before, during, after.** Support updates, corrections, cancellations, and all-clear messaging to maintain credibility and drive protective behavior.
4. **Security and trust.** Harden authentication/authorization throughout the system, to prevent spoofing and maintain confidence in alerts. Systems must support updates, corrections, and all-clear messaging to maintain public trust and enable adaptive response.
5. **Resilience and interoperability.** Ensure alerts propagate even under degraded conditions (power/internet loss) and flow seamlessly across EAS/IPAWS pathways (EAS, WEA, NOAA Weather Radio, etc.). The systems carrying these messages must be resilient under degraded conditions, interoperable across IPAWS pathways, and protected against unauthorized use.

6. **Measurable performance.** Track timeliness, delivery/penetration, geo-accuracy, accessibility, false-alert rates, and public opt-out/fatigue to improve outcomes. (The most recent nationwide EAS test data illustrates why measurement matters.)<sup>1</sup>

The three goals in the NPRM are solid but omit attributes (precision, accessibility, security, resilience, measurement) that the Commission itself flags elsewhere in this current NPRM.

## **2.2 A Fuller Framework for the FCC's Listed Goals**

Together, these expand the FCC's three listed goals into a fuller framework that reflects the real-world requirements for protecting life and property, from initial warning to protective action, to safe recovery.

### 1. Precision & Relevance

- **Why:** Over-alerting leads to *alert fatigue*, while under-alerting misses populations at risk.
- **Objective:** Ensure alerts are targeted geographically (e.g., SAME/FIPS alignment for EAS, 0.1-mile overshoot for WEA) and demographically (accessibility, language). More precise alerts increase protective action compliance and reduce the risk of property loss through better resource allocation.

### 2. Accessibility & Availability

- **Why:** Alerts that cannot be seen, heard, or understood leave vulnerable populations unprotected.
- **Objective:** Provide alerts in formats accessible to people with disabilities (visual and auditory parity, vibration/haptic support, text-to-speech) and in multiple languages. Ensures that all segments of the population, particularly those most at risk, can act to protect themselves and their communities.

---

<sup>1</sup> "The Emergency Alert System: Status of Current Funding for Improvements," Congressional Research Service, Updated June 24, 2025 (IF12998)

### 3. Continuity Under Stress (Resilience)

- **Why:** Major disasters impair power, internet, and cellular networks.
- **Objective:** Maintain alerting pathways that function when parts of the communications infrastructure are degraded (e.g., PEP/NPWS AM stations for EAS, NOAA Weather Radio, satellite links). Prevents communities from being left without guidance in the most dangerous moments.

### 4. Credibility & Trustworthiness

- **Why:** False alerts (e.g., Hawaii ballistic missile incident, 2018) can erode trust and cause panic.
- **Objective:** Strengthen authentication, require clear “alert source” labeling, and support quick issuance of corrections or cancellations. Trustworthy alerts drive compliance and protective actions.

### 5. Actionability & Specific Protective Behaviors

- **Why:** Research shows people act more when told *what to do* and *why*.
- **Objective:** Standardize core message elements (hazard, location, timeframe, protective action). Enable rich content (e.g., embedded links, maps, multimedia in next-gen EAS/WEA). Clear instructions reduce loss of life and allow individuals to protect property (e.g., securing belongings, evacuating, sheltering).

### 6. Lifecycle Support (Updates, All-Clears, Recovery)

- **Why:** Emergencies are dynamic, and people need to know when it’s safe to return.
- **Objective:** Require systems to carry updates, corrections, and explicit “all clear” messages. Minimizes risk from re-entry into dangerous zones and reduces property loss by guiding timely recovery efforts.

### 7. Public Awareness & Education

- **Why:** Even well-designed systems are ineffective if people don’t understand them.
- **Objective:** Support consistent public education campaigns and, at a minimum, annual testing so the public knows what alerts mean and how to respond. Informed individuals are more likely to take protective actions immediately when real alerts are issued.

## 8. Performance Measurement & Continuous Improvement

- **Why:** National EAS/WEA test data show variable receipt rates and timeliness.
- **Objective:** Institutionalize measurement of latency, coverage, accessibility, and accuracy, and require corrective actions when standards aren't met. Measurable performance ensures systems consistently achieve their statutory purpose of protecting life and property.

### ***2.3 Digital Alert Systems' efforts to achieve these additional objectives***

Over the past years, Digital Alerts Systems has contributed recommendations to policy and standards bodies and technical innovations in our own alerting solutions, which have been targeted at supporting what we have framed as these additional objectives for the protection of life and property.

#### 1. Precision & Relevance

- **Objective:** Deliver alerts to the populations at risk without over-alerting others.
- **Digital Alert Systems contribution:** We are working with our EAS Participant partners to extend the usage of partial FIPS to further narrow the geographic scope of alerting over broadcast and cable media. The DASDEC includes polygons for enhanced geotargeting in those services that support it, such as ATSC 3.0's optional Advanced Emergency Information service.

#### 2. Accessibility & Availability

- **Objective:** Ensure alerts reach people with disabilities and limited English proficiency.
- **Digital Alert Systems' contribution:** Digital Alert Systems took the lead in pioneering multilingual alert services in EAS, including supporting an extended range of languages with text-to-speech capabilities, and creating a standardized approach and lexicon for conventional EAS "header" alert messages in languages including Spanish, French, German, Italian, Somali, and Hmong. We developed an advanced approach for inserting standard non-English EAS warnings when CAP text did not include the desired language. We developed a methodology for presentation of multiple languages for screen text

crawls, support audio text-to-speech from CAP fields, and pass through multilingual content when provided by originators.<sup>2</sup>

- Digital Alert Systems also took a leading role in developing industry guidance for including symbology in EAS crawls as well as HD radio displays, which has resulted in several fielded deployments.<sup>3</sup> This symbology was based on FEMA/NAPSG elements, refined for use in broadcast environments.

### 3. Continuity Under Stress (Resilience)

- **Objective:** Maintain alerting during degraded network conditions.
- **Digital Alert Systems' contribution:** Digital Alert Systems has pioneered efforts to deploy redundant IPAWS dissemination paths and local relay sources, preserving EAS relay capability if one path fails. As one example, we worked to deploy a digital ATSC data broadcast network across the state of Ohio, which has been reliably operating non-stop for seven years as a parallel distribution system for IPAWS CAP alert messaging to add a continuity layer in the event of Internet failure.<sup>4</sup>

### 4. Credibility & Trustworthiness

- **Objective:** Prevent false alerts and maintain confidence in the system.
- **Digital Alert Systems' contribution:** Digital Alert Systems pioneered the development of a time validation window to ensure only alerts intended to be sent within a specified time frame would be processed. This eliminated many false alerts that may have been derived from previously recorded audios or did not fall within the current time window of the decoding device. CAP/EAS devices validate FEMA-issued digital certificates before

---

<sup>2</sup> See “Digital Alert Systems Introduces Multilingual EAS Translation Software,” TV Technology, May 5, 2015 (<https://www.tvtechnology.com/news/digital-alert-systems-introduces-multilingual-eas-translation-software>); also “First Multilingual National Periodic Emergency Alert System Test Transmitted Today,” PipelinePub, November 18, 2015 (<https://www.pipelinepub.com/news/first-multilingual-national-periodic-emergency-alert-system-test-transmitted-today>).

<sup>3</sup> See for example “NVISA’s New VIDS Practice Makes Emergency Alerts Visually Easy to Grasp By Phil Kurz published February 22, 2021,” TV Technology, February 22, 2021, (<https://www.tvtechnology.com/news/nvisas-new-vids-practice-makes-emergency-alerts-visually-easy-to-grasp>); also “KADO-CD Taps Digital Alert Systems to Add VIDS to KADO-CD EAS,” TV Technology, February 1, 2021 (<https://www.tvtechnology.com/equipment/kado-cd-taps-digital-alert-systems-to-add-vids-to-kado-cd-eas>).

<sup>44</sup> See “Ohio Digital Alerting System Is Active: OEAS Public AlertNet system upgrades the state’s “last-mile” EAS infrastructure,” RadioWorld, May 23, 2017 (<https://www.radioworld.com/news-and-business/ohio-digital-alerting-system-is-active>).

processing alerts, ensuring only authenticated originators are relayed. Logging functions also provide a verifiable record of alert receipt and relay.

- Digital Alert Systems' efforts to enhance security include our efforts to create a process for EAS message validation adjunct to the current EAS header tones. The Textual Data eXchange (TDX) protocol outlines how this could be applied and has been field tested for integrity and inter-platform compatibility.

#### 5. Actionability and Specific Protective Behaviors

- **Objective:** Standardize protective instructions and support richer content/
- **Digital Alert Systems' contribution:** CAP-based EAS alerts carry structured fields (event code, expiration time, protective action text). Digital systems can use those fields to drive consistent crawls, audio, and even links or reference information for NextGen TV integration. The DASDEC can currently receive, aggregate, route, and forward additional media resources (graphics, maps, video) for use by partner systems. The DASDEC can aggregate richer content for presentation in services such as web applications, NextGen TV applications, and more,

#### 6. Lifecycle Support (Updates, All-Clears, Cancellations)

- **Objective:** Carry updates and termination messages.  
**Digital Alert Systems' contribution:** In the ATSC 3.0 AEI environment, the DASDEC can process "Update" and "Cancel" alert messages and automatically override or clear previously running alerts, reducing confusion and quickly restoring normal programming. Digital Alert Systems contributed the specifications for the AEI message functionality, which were adopted into the ATSC 3.0 standard.

#### 7. Public Awareness & Education

- **Objective:** Familiarize the public with alerting functions through testing.
- **Digital Alert Systems' contribution:** Making Required Monthly Test (RMT) scheduling and reporting, nationwide EAS test reporting (ETRS), by data collection systems like Digital Alert Systems HALO™ and Collector™, thereby making test execution and compliance more transparent.

## 8. Performance Measurement & Continuous Improvement

- **Objective:** Measure latency, coverage, accessibility, and error rates.
- **Digital Alert Systems' contribution:** Systems log alert reception and relay times, errors, and other system information. Digital Alert Systems directly supports the FCC's objectives via solutions like the DASDEC, HALO and the Collector, by creating a future path to enable alert precision beyond SAME/FIPS, facilitating accessible/multilingual content, ensuring resilient multi-path reception, authenticating alerts for trust, investigating means to support lifecycle messaging, and generating logs/metrics for accountability.

### **2.4 Public Warning Objectives, Outcomes, and Metrics**

The Commission seeks comment on whether to articulate objectives not only in terms of the capabilities that EAS and WEA participants must provide (e.g., rapid, authenticated, accessible distribution of alerts), but also in terms of the public-safety outcomes these capabilities are meant to achieve (e.g., ensuring all members of the public actually receive and comprehend alerts and take protective action).

Yes, these objectives should be grounded both in system capabilities as well as public safety outcomes. The objective of ensuring that all participating communications channels distribute emergency messaging is a reasonable goal. Working to ensure that alerts are comprehensible by the public is a reasonable goal.

However, ensuring that all members of the public receive alerts and take protective action is not reasonable. This requires "guarantees" beyond the scope of providers' equipment, networks and services. At a minimum, this is because the user's individual actions – including whether or not to even have a device powered on - are outside of its control.

#### **Service-Capability-Based Objectives**

There are *performance requirements* that the FCC can regulate directly under its Part 11/Part 10 authority. They define what broadcasters, cable/satellite operators, and wireless carriers must do to ensure the system works reliably. These are necessary conditions; they describe what the *system* can do: to transmit alerts, and do so within a defined latency; validate alert authenticity of alert messages (e.g. digital signatures), reject unauthorized inputs, and log events; transmit the alert into relevant geographic areas (CMSPs must geo-target WEA messages to the

defined area with minimal overshoot; broadcast and cable operators must geo-target EAS messages within their respective coverage areas); and so forth.

### **Public-Safety Outcome Objectives**

The statutory purpose of the system is “to provide the President and state and local authorities with the capability to alert the public to emergencies...to protect life and property.” Accordingly, outcome objectives should focus on whether the system is actually protecting people in practice, such as:

- Participating dissemination technologies must be able to reliably relay the alert.
- The language, format, and urgency of the alert message should be clear and actionable for diverse populations.
- Alerts should guide recipients toward the correct protective actions. People must know what to do and feel motivated to take immediate steps that reduce risk and safeguard life and property.
- Members of the public should believe that alerts are authentic, accurate, and relevant. High trust ensures recipients respond appropriately — neither ignoring the message nor overreacting in ways that cause panic or secondary harm.

Together, these conditions represent sufficient criteria for evaluating whether the system is effective in practice. If reach, comprehension, action, and trust are achieved, the system fulfills its intended purpose: protecting lives and property during emergencies.

These are sufficient conditions that describe what the *system should achieve in practice*.

### **Why Both Are Needed**

- If the FCC grounds objectives *only* in capabilities, the system risks being technically compliant but ineffective (e.g., an alert goes out, but people ignore it because it is vague, inaccessible, or mistrusted).
- If the FCC grounds objectives *only* in outcomes, it risks holding EAS participants to goals they cannot fully control (because behavior depends on message originators, public education, and context).

The right framing is to set realistic capability requirements (what EAS and WEA must technically do) and acknowledge outcome objectives as the *ultimate purpose* of the system, and build mechanisms for measuring and reporting them (via national tests, surveys, research partnerships with FEMA/NWS, etc.).

### **3 The Paradox of EAS as an Unfunded Public Service Mandate**

We wish to highlight an important paradox: the Commission is rightly asking whether EAS should advance beyond its “best efforts” design toward more robust capabilities, yet the current framework leaves the burden of this public service mandate entirely with private-sector licensees. This theme will recur throughout certain responses in this document, underscoring that several of the enhanced features or capabilities under consideration extend significantly beyond the reasonable capacity of EAS Participants to support absent supplementary resources (e.g. government funding support), if feasible at all.

#### **3.1 EAS as an Unfunded Mandate**

Since its inception, the EAS has functioned as an unfunded mandate. Every broadcaster, cable operator, and other covered entity is required to purchase, deploy, and maintain FCC-certified EAS equipment (47 C.F.R. § 11.11). Unlike other components of the public safety infrastructure, there are no dedicated federal funding streams to offset these costs.

While this framework may have been adequate when EAS was primarily a “fail-safe” system to ensure presidential access<sup>5</sup>, the Commission’s current inquiry seeks to expand EAS into a front-line, multimedia, and multilingual alerting platform. That vision is laudable, but it magnifies the resource demands on the private entities responsible for compliance.

#### **3.2 The Paradox: Expanding Public Benefits, Expanding Private Burdens**

The Commission is considering enhancements, such as:

- Guaranteed delivery mechanisms with end-to-end monitoring or acknowledgments.
- Video-based alerting, including embedded graphics, ASL interpreters, and other visual content.
- Multilingual capabilities to serve diverse language populations; and
- Accessibility improvements for those with hearing or vision impairments

Each of these enhancements delivers broad public benefits, but they also incur private costs in the form of new equipment purchases, integration, testing, and ongoing operational support.

---

<sup>5</sup> Amendment of Part 73, Subpart G, of the Commission’s Rules Regarding the Emergency Broadcast System, Report and Order, 10 FCC Rcd 1786 (1994)

The paradox is that the Commission's expectations are rising, but the responsibility still falls entirely on private broadcasters and operators who get no public support. This imbalance risks undermining the Commission's goals by creating disparities in adoption—large operators may move ahead quickly, but small-market and rural licensees might find it hard to keep up.

### **3.3 Implications for Public Safety and Industry**

#### **1. Ubiquity and Coverage Gaps**

Smaller broadcasters and translator stations, critical in rural and underserved regions, face significant financial barriers. Uneven adoption jeopardizes the universality of EAS, weakening public safety in precisely the communities most dependent on broadcast and cable alerts.

#### **2. Innovation and Affordability**

Vendors such as Digital Alert Systems are committed to advancing the state of the art—our platforms already support CAP delivery through FEMA IPAWS, multilingual insertion, aggregating multimedia, and advanced distribution options. But unlike many other technology markets, EAS manufacturing is almost entirely compliance-driven. This means manufacturers must invest heavily in R&D, certification, and ongoing support without a broad commercial demand signal, carrying substantial business risk. New regulatory requirements can demand rapid product redesigns, software development, and certification cycles—costs that manufacturers must absorb and recover in a market that expects affordability and backward compatibility.

#### **3. Policy Disconnect**

Absent funding mechanisms, the risk is that the Commission's goals will be delayed, diluted, or unevenly implemented, undermining public confidence in the system. Both participants and manufacturers are left bearing burdens for what is fundamentally a national public safety function.

### **3.4 Recommendations**

Digital Alert Systems respectfully proposes the following actions to reconcile regulatory ambition with practical realities:

- 1. Funding Support:** Establish dedicated federal or state-level funding programs, administered through FEMA's IPAWS office or DHS grant mechanisms, to support purchasing and deploying enhanced EAS equipment. Precedent exists in the Homeland Security Grant Program (HSGP), which funds interoperable communications

- infrastructure, and the Next Generation Warning System (NGWS) Grant Program. Such programs should also recognize the burdens borne by manufacturers, who must invest in research, development, and certification to meet evolving requirements in a compliance-driven market.
2. **Collaborative Standards Development:** Formalize industry-government collaboration through the FEMA IPAWS Subcommittee and the FCC Communications Security, Reliability, and Interoperability Council (CSRIC) to ensure practical, interoperable solutions for multilingual, accessible, and video alerting. And, importantly, we reiterate our long-standing recommendation to reinstate the FCC's National Advisory Committee (NAC), which was focused on emergency alerting, and expand the scope of that committee to include representatives from all relevant stakeholder areas, including active EAS manufacturers. A focused NAC would be more effective than the CSRIC framework.
  3. **Public-Private Partnerships:** Explore cooperative programs in which federal support leverages private-sector innovation. For example, equipment rebates, matching grants, R&D cost offsets, or tax credits could accelerate innovation. We understand that these suggestions are outside the scope of the Commission; however, we note this because, again, the desire to expand the capabilities of the nation's alert systems will require tangible support, not just regulation. Moreover, realistic time needs to be allowed for technical standards to mature and for EAS Participants to budget for necessary upgrades.

## 4 National Level Alerting

A core purpose of EAS is to enable the transmission of an emergency alert from the President or his designee during a national emergency. In furtherance of those objectives, the Commission believes that the nation's alerting systems should be designed to allow the President to both send the public an immediate warning to take protective action and to later provide additional information and reassurance to the public. As we discuss, as relatively short messages, these two functions may readily be accommodated via EAS and WEA. However, lengthier messages or those expected to be delivered with heavier media requirements (i.e. video), are best left to systems and approaches that are separate from, but complementary to, EAS and WEA. That being said, the national EAS has always been designed to accommodate a lengthier audio message in exceptional case of the National Emergency Message (EAN formerly Emergency Action Notification).

The Commission asks how alerting systems should be designed to ensure these capabilities are available and maximally effective during national emergencies. In particular, the question is posed whether it would be most effective for alerting systems to be able to support video messages from the President. Our response to this is cautious, as the idea of additional video requirements for alerting may raise extreme technical and cost impacts on EAS Participants, as we will discuss further below in regard to national alerting, and also in Section 5 in relation to state and local alerting.

In short, EAS functions as a resilient path that can support extended audio messaging, with accompanying standard EAS text, for National Emergency Messages. The introduction of video into the core alerting environment rises to the level of a “moon shot” ambition. It blurs the lines between “emergency alerting” and “emergency public information.” And adding a video component may be contrary to the goal of resilience and survivability of EAS.

Below, we examine the question of implementing a “video-rich” alert system for the United States in terms of core design principles, practical pathways for implementation, and incremental cost considerations, with specific focus on EAS (but referencing WEA where relevant).

#### **4.1 Core Design Principles for Presidential-Level Alerting**

Resilience and redundancy have always been one of the core design principals for Presidential-level alerting. EAS must continue to function when internet and commercial power are compromised (via FEMA’s PEP/NPWS AM stations and broadcast daisy chain). Any new capabilities (e.g., video-rich content) should not displace, distract or deteriorate this hardened baseline. Even with the most current compression standards, video delivery requires several orders of magnitude in bandwidth—read this as more spectrum or bits. When resilient message delivery is the goal, the less bandwidth required, the better.

In this type of scenario, EAS is designed for immediate protective action and follow-up. The system is organized around short, urgent warnings, with the exception of the National Emergency Message which has no specified message time limit.

Longer or media-rich (video) communications from the President or other national authority may not easily fit into EAS or WEA capabilities. The idea of “video-rich” messaging would be better considered a parallel system, so that the hardened baseline of EAS is not adversely impacted.

Other technical considerations that would need to be weighed in looking at video-based alert messaging would include authentication and trust, and the possibility of needing to support persons with vision disabilities and non-English speakers (captioning, audio description, and possibly multilingual streams). If required, these features would significantly increase the cost and technical complexity of any “video-rich” messaging capability.

#### **4.2 Video-Based Alerts: Foundational Considerations**

While the Commission asks for input on how video-based alerting could be implemented, it must recognize that before any implementation details can be reasonably addressed, a necessary prerequisite is the development of requirements and performance objectives.

Because these questions intersect technology, policy, and public safety, the discussion cannot occur in isolation. FEMA, FCC, DHS, EAS Participants, equipment manufacturers, and other core stakeholders must collaborate to define the goals and objectives of the concept of video in alerting. Only with shared requirements in place can industry participants like Digital Alert Systems design equipment and software solutions that are both compliant and practical.

These requirements research and standards-setting processes would be inherently complex and would require interagency coordination to align WHCA/WHMO expectations, FEMA IPAWS program operations and FCC regulatory expectations. Such a concept would also absolutely require cross-industry dialogue including broadcasters, cable operators, and equipment manufacturers.

### ***4.3 Stakeholder and Cost Considerations for Video-Based Alerting***

Any discussion of video-based alerting must start by recognizing that requirements drive costs. Without clear definitions of what video alerts should achieve, how they should be delivered, and what performance standards they must meet, it is premature to estimate equipment changes or project nationwide expenses.

#### **Broadcasters and EAS Participants**

Broadcasters and other video service providers will ultimately bear a significant share of the deployment responsibility, but the scale of required investment depends entirely on agreed standards. For example, firmware upgrades may suffice if video alerts are limited to simple embedded clips or links. By contrast, if “guaranteed delivery” of real-time Presidential video to every outlet is mandated, completely new encoding, playout, and transmission infrastructure may be needed. The cost implications of this could be enormous.

However, the first question is not how much it might cost but what it might require. Only after FEMA and the FCC articulate those desired parameters can industry begin to discuss feasibility. And only then can manufacturers like Digital Alert Systems respond with the design of affordable, phased solutions that minimize burdens on licensees, if that is even possible.

#### **NextGen Broadcast Services**

Next generation broadcast services like ATSC 3.0 already provide optional support for rich emergency information services, including video. However, whether this pathway is the FCC’s desired vehicle for video alerts or simply one of several options must be clarified in policy first. NextGenTV’s Advanced Emergency Information provides this capability but is an optional service within a voluntary standard.

#### **Federal Costs and Responsibilities**

It is equally important to note that federal infrastructure must evolve in tandem with broadcaster obligations. FEMA IPAWS does not currently host or distribute video and multimedia resources,

just as today IPAWS does not host audio resources itself. A video-capable alerting environment would require FEMA to define payload specifications, develop encoding/hosting infrastructure, and maintain secure, redundant distribution. These foundational federal investments must be specified before private-sector costs can be projected.

### **Overall Cost Framework**

Without established requirements, we can only speculate that the overall cost framework could run into the tens or hundreds of millions of dollars. What can be said with confidence is that:

#### **4.4 Recommendations/Conclusion**

The Commission is right that Presidential communication remains paramount. Designing systems for short, immediate warnings plus follow-up reassurance is essential. However, video-rich alerts could entail major broadcast and cable system redesigns, identification of secure/robust distribution systems for the video, and more. The cost implications of such an undertaking would be, as we indicate above, easily in the tens of millions of dollars, more likely into the hundreds of millions.

Further, by adding video, we raise the question of whether this is starting to blur the lines between an emergency "alert" vs. emergency "information", a topic we further discuss in Sections 7 below. There is a risk of "emergency alerts" being blurred with "informational messages." Alerts must be concise, urgent, and guaranteed to break through. Video is better suited for *follow-on information*, not the initial alert message. The "alert" itself should not turn into long-form "information."

- **Emergency Alerts (urgent):** minimal, authenticated, failsafe message that interrupts programming and prompts a protective action (audio + crawl in EAS; short text in WEA). This is squarely within Part 11's purpose, giving the President immediate communications capability.
- **Information (follow-on):** richer context or reassurance that the President (or FEMA) can provide after that initial alert, potentially including video. Treat this as *supplementary content referenced by the alert*, not the alert itself. CAP already allows a resource pointer for rich media; receivers that can render it may do so, while legacy devices still present audio/text.

If video is seriously being contemplated, then the practical approach may be to design the system so that the alert remains short, authenticated, resilient, and universally receivable, and any video

is an optional, follow-on element delivered by paths that can actually carry it. This avoids blurring roles, keeps EAS/EAS dependable under stress, and contains costs.

**Video would require significantly upgraded distribution vs today's IPAWS CAP polling.**

The NPWS/PEP system is organized around EAS, meaning that it is by nature an audio/text system, not itself capable of supporting video. Even if the IPAWS CAP message carries only a pointer (resource URL) to video delivered by an external source, such a system needs to undergo upgrades.

Video resources could be referenced as a link in a CAP message; however CAP message availability is currently served over the public Internet. Resiliency cannot be assured. As the FCC knows, IPAWS OPEN makes CAP available to EAS participants to retrieve over the Internet and relay them via EAS, WEA, etc. It is optimized for compact payloads, not the mass distribution of large binaries.

The IPAWS CAP Profile explicitly supports <resource> marked "EAS Broadcast Content" for audio/video/image intended for EAS. In practice, this is best used as a URL pointer to media hosted on hardened infrastructure (CDN/broadcast), not as a giant embedded payload. If many thousands of EAS devices simultaneously pulled large video files directly from IPAWS, FEMA would need the requisite secure hosting/bandwidth and new operational practices. Such an approach would open yet another potential vulnerability and resilience issue.

If a video resource was to be made available by FEMA IPAWS or other agency, we do note that there are options that could be explored on a voluntary basis. For example, many older and all current DASDEC systems support video outputs in both baseband (NTSC, HDMI) and compressed IP (MPEG-2 Transport Streams & MPEG-DASH), which could be updated to make video resources available as an optional service for systems like newsrooms, station websites, applications, etc.<sup>6</sup>

---

<sup>6</sup> For broadcasters transmitting NextGen TV (ATSC 3.0) there may be optional services to support video. In the case of ATSC 3.0, the DASDEC can support a video resource that could be made available to the optional broadcast ATSC 3.0 Advanced Emergency Information data service.

**Why 24 Months Is Not a Reasonable Timeframe**

For EAS participants, tens of thousands of stations/headends would need equipment upgrades, automation integration, new storage/servers, and staff training, even after equipment is specified/available. And that is after basic requirements have been set.

For WEA, URL-based references to video could result in network congestion and bottlenecks, creating an adverse situation of mobile service unavailability. For CMS Providers to link to video reliably, at a minimum new standards work, handset updates, CMPS architecture and CDN build-out would be needed. True in-band video would take years, requiring costly system re-architecting (true video broadcast over 5G is several years away).

A distribution burden would exist across the ecosystem. FEMA's IPAWS CAP polling mechanism was not designed to directly serve resources such as video. A video host capable of handling secure video distribution at scale would have to be scoped, either by IPAWS or at the expense of individual SLTT agencies. Without secure hosting and distribution infrastructure, video cannot be expected to be ingested at scale, even as an optional resource.

In short, this is not just a "software patch." This concept represents workflow reengineering and infrastructure investment across thousands of facilities and multiple industries. The Commission should maintain a distinction between immediate alerts (short audio/text) and optional/supplementary video information (optional, device-dependent, and phased adoption).

## 5 The Effectiveness of EAS: State and Local Alerting

The Commission is correct that nearly all alerts that the public receives day-to-day originate not from FEMA, but from other agencies at the federal, state, Tribal, territorial, or local level. We believe that EAS remains an effective tool that allows these agencies to achieve their alerting objectives, potentially with additions and modifications.

The short answer is that EAS and WEA often work very well for day-to-day originators (NWS, USGS, AMBER authorities), even though they don't yet let every agency "fully" achieve their objectives. EAS and WEA excel at rapid reach. EAS, however, struggles with precision, accessibility, multilingual parity, and uniform operational readiness.

### 5.1 Where EAS is effective today

- **High national reliability under test.** The 2023 nationwide EAS test showed markedly better reception/retransmission when the alert originated in CAP (rather than over-the-air only), indicating the architecture works when CAP is used as intended.<sup>7</sup>
- **Resilience under stress.** Because it relies on EAS (non-Internet) and CAP (Internet) dissemination, the EAS provides a strong architecture for redundancy and reliability. For national-level messaging, redundant and alternative survivable (non-Internet) dissemination remains essential. The record (FCC Docket 15-94) clearly demonstrated this.
- **Timeliness.** The core purpose of the national EAS is to provide the President of the United States the capability to address the nation within 10 minutes during a national-level emergency.<sup>8</sup> Weather, civil and non-weather EAS/CAP messaging may be relayed up to 15 minutes after time of receipt.<sup>9</sup> In practice, however, the vast majority of EAS Participants retransmit an EAS/CAP message with minimal delay.

---

<sup>7</sup> Federal Communications Commission, "Report: October 4, 2023 Nationwide Emergency Alert Test". June 2024; "Nationwide EAS Test Numbers Improve," RadioWorld, 28 June 2024.

<sup>8</sup> <https://www.fema.gov/emergency-managers/practitioners/integrated-public-alert-warning-system/public/emergency-alert-system> As the Commission is aware, through data collected through its Electronic Test Reporting System (ETRS), the response time by EAS participants to a national EAS message (EAN or NPT) is near-immediate from message reception by radio and TV broadcasters, cable TV, wireless cable systems, and satellite operators.

<sup>9</sup> See 47 CFR § 11.51(n) "EAS Participants may employ a minimum delay feature, not to exceed 15 minutes, for automatic interruption of EAS codes."

## 5.2 *Where agencies still hit limits*

EAS targeting is still coarse. Most legacy EAS activations are county-based (SAME/FIPS) and service-contour dependent, so audiences far from the hazard can be interrupted, fueling alert fatigue. NWS is piloting Partial County Alerting to reduce this, but it is not yet ubiquitous.

Inconsistent or Preferential use of WEA over EAS. Despite the availability of EAS at the local level, many emergency managers rely almost exclusively on Wireless Emergency Alerts (WEA) for critical incidents. This tendency has resulted in underutilization of EAS, even in situations where its broader reach and redundancy could have added significant value.

## 5.3 *Video Alerting for SLTT Agencies*

The Commission has questioned whether SLTT agencies should use video in emergency alerts. As with the previous discussion in Section 5, we raise great concern about overtaxing the public warning system.

Video should not replace the emergency alert, nor should it be entertained in SLTT-originated alerts. Video can add value as *supplementary, optional content*, especially through more capable distribution channels than EAS or WEA.

EAS alerts should remain primarily focused on audio and visual text presentations, though the Commission could look at whether multimedia resources like symbology/iconography and basic images and graphics that may be utilized on an optional basis by appropriate services.

EAS and WEA function effectively, but additional refinements and features could enhance the utility of alert messaging for originators, disseminators, and the general public. Video should not be mandatory or replace the alert. Video is more appropriate for agency-driven communication for emergency *information*, and not requirement for emergency *alerting*. The core alert should remain concise and universally receivable (audio plus text).

## 5.4 *Recommendations*

1. **Scale fine-grained targeting on EAS.** Support further efforts on Partial County Alerting in state EAS plans.
2. **Codify core message templates for all originators.** Use FEMA IPAWS best-practice templates (source, hazard, location, protective action, expiry) to improve clarity and compliance across agencies.

3. **Keep measuring outcomes, not just capability.** Build on the 2023 national test (and RAND's public-reach survey) to track timeliness, geo-accuracy, accessibility, and opt-out rates, then feed results into rule updates and training.

## 6 Recommendations to Move to an “Enhanced EAS”

As the commission recognizes, EAS is an effective tool for most day-to-day originators, but not yet “fully enabling” every agency’s objectives. The record is clear that EAS is effective but not fully optimized for the day-to-day agencies that originate the most alerts (NWS and SLTT originators). The fastest path to “fully” is pursuing optional complementary technologies that enable fine-grained targeting (such as ATSC 3.0’s AEI), paired with consistent accessibility and message-template practices across federal, state, local, tribal, and territorial (SLTT) originators.

The Commission is correct that FEMA, NWS, USGS, and state, local, tribal, and territorial agencies originate the overwhelming majority of alerts the public receives. To ensure these agencies can fully achieve their alerting objectives, the Commission should recognize that improvements fall into two categories: (1) near-term steps achievable within current architectures, and (2) longer-term enhancements requiring further study and investment.

### 6.1 Near-Term Steps

#### Technical Upgrades

- **Expand Dissemination Paths:** Supplement IPAWS EAS and Internet CAP dissemination with redundant IP-based distribution (e.g., FEMA IPAWS over secure broadband/satellite) to avoid single points of failure.
- **Precision Targeting:** Work with EAS manufacturers to investigate how to integrate polygon-based geotargeting (as WEA does) into EAS. This could reduce alert fatigue and make alerts more relevant.
- **Rich Media & Accessibility:** Enable inclusion of maps, graphics, multilingual text/audio, and accessibility features (ASL video, text-to-speech) via ancillary services.
- **Two-way capability:** To improve reliability and auditability, move to enable acknowledgments, diagnostics, and feedback from EAS Participants (i.e., automated from FCC-certified EAS appliances).

### **Policy & Regulatory Changes**

- **Funded mandate:** Transition from unfunded to supported infrastructure. Federal or state grants/subsidies could ensure consistent equipment quality across participants.
- **Uniform participation standards:** Standardize state and local alert obligations (today, they vary widely). This would make reliability less dependent on local plan differences.
- **Accountability and audits:** Beyond log-keeping, establish regular compliance testing, independent audits, and penalties for failure to meet reliability benchmarks.

### **Operational Enhancements**

- **Integrated training and exercises:** Ensure broadcasters and cable operators are regularly trained for real-world scenarios, not just compliance testing.
- **Rapid update/cancel workflows:** Avoid “frozen” alerts that confuse the public. Systems should investigate how to allow dynamic updates and withdrawals in real time (like WEA).
- **Coordination with next-gen systems:** Pair EAS with WEA, for a layered approach where EAS is the universal backbone but not the sole tool.

### **Governance & Funding Model**

- **Shift from “best effort mandate” to “national infrastructure.”** Treat EAS like other critical infrastructure (power grid, 911). Fund modernization via the federal budget, not private broadcasters and cable operators alone. Establish a national coordination body to oversee standards, upgrades, and long-term strategy.

## **6.2 Enhancing Relay/Transmission Capabilities of EAS**

The Commission asks for comments on the alert transmission capabilities that a national public alert and warning system must have to meet its objectives. Digital Alert Systems works with a variety of SLTT and Federal authorities and can provide an overview of the capabilities a national alert & warning system should possess, as well as what alert originators expect in practice when they activate the system.

In terms of the capabilities the system must have:

- **One message, many paths (simultaneous delivery).** Originators expect to compose a single alert that’s authenticated and fanned out at once to WEA (phones), EAS

(radio/TV/cable/sat), and NOAA Weather Radio, via FEMA’s IPAWS OPEN. That “write once, reach many” model is foundational.<sup>10</sup>

- **Geographic precision where the medium supports it.** For phone alerts, originators expect polygon targeting that covers ~100% of the target area with ≤0.1-mile overshoot (FCC rule). For broadcast, originators recognize EAS is area-wide; NWS is promoting Partial County Alerting to better align EAS/NWR with finer risk areas.
- **Resilience under degraded conditions.** Originators expect alerts to propagate even with commercial power or internet failures, hence reliance on the National Public Warning System / Primary Entry Point (PEP) stations as a hardened national backbone for presidential and other critical messaging. Similarly, SLTT authorities should maintain the capability for direct EAS activation, should power or internet failures disrupt communications from alert origination facilities, or disrupt the ability for broadcast and cable operators to receive IPAWS CAP alert reception.

Digital Alert Systems has long recognized that resilience is a critical pillar of public alerting, and the reason we helped implement the Ohio datacast relay system. To operationalize “one message, many paths,” we worked with state agency and broadcast partners to stand up an over-the-air datacast backhaul that delivers authenticated CAP alerts directly into EAS relay endpoints as an alternate to conventional Internet,<sup>11</sup>

The Ohio “OEAS” datacast relay system preserves alert flow when commercial power or internet links are degraded, maintaining statewide distribution to EAS Participants and enabling SLTT authorities to continue direct activation if origination facilities or IP reception paths are impaired.<sup>12</sup> The relay preserves geographic targeting metadata where supported and aligns with the FEMA IPAWS posture and state EAS plan to help ensure that alerts can still propagate even under adverse conditions. In short, the Ohio deployment exemplifies our approach: add

---

<sup>10</sup> <https://www.fema.gov/emergency-managers/practitioners/integrated-public-alert-warning-system>

<sup>11</sup> See “Joint Comments of Digital Alert Systems, Inc. and Ohio Educational Television Stations, Inc. In Response to the Notice of Inquiry” PS Docket 15-94, filed April 11, 2022, also “Joint Comments of Ohio Educational Television Stations, Inc., Monroe Electronics, Inc. and Triveni Digital, Inc. on Improvements to EAS Capabilities,” PS Docket 15-94, filed May 17, 2016.

<sup>12</sup> “Ohio Educational TV Stations to Strengthen Emergency Public Information System,” Government Video, March 25, 2016; “Triveni, DAS Team on Ohio Digital EAS,” TV Technology, March 24, 2016; and “Triveni Digital Teams Up With Ohio Educational TV Stations and Digital Alert Systems to Strengthen Dissemination of Emergency Public Information,” Broadcasting & Cable, March 23, 2016.

redundant, diverse transport paths and seamless failover logic so that EAS remains a dependable backbone for public warning when other systems falter.

In summary, originators expect quick, verified, geo-accurate alerts that reach everyone who needs them, even when infrastructure is compromised, delivered simultaneously via phone, broadcast, and NWR. The current record (FEMA/FCC/USGS/NWS) supports these expectations and highlights areas for further improvement, especially reducing latency for WEA, enhancing geo-targeting precision, CAP-first EAS operations, and strengthening NPWS, which most improve outcomes.

### **6.3 *Maintaining the Focus of EAS***

EAS and WEA function effectively, but additional refinements and features could enhance the utility of alert messaging for originators, disseminators, and the general public.

EAS alerts should remain primarily focused on audio and visual text presentations. The Commission should rather look at steps towards including more modest multimedia resources with alerting. This could consist of further introducing standardized symbology/iconography to accompany EAS and WEA alerts, as well as basic images and graphics that may be carried on an optional basis by appropriate services. Using CAP <resource> pointers, systems like the DASDEC can aggregate such media for use by appropriate systems.

The Commission should take care to maintain the distinction between “alerts” and “public information”. Alerts remain short, authenticated, and universally delivered; via robust and survivable dissemination paths. The investigation of enhancing EAS should be mindful of concepts that are overly burdensome, high-cost/low-return, device-dependent, or likely better fitting the emergency “public information” category than used in conjunction with “emergency alerting”.

### **6.4 *Recap and Recommendations for Enhancing EAS***

EAS is effective but not yet sufficient for all agency needs. With CAP-first, fine-grained targeting, and accessibility improvements, EAS can more fully support NWS, USGS, AMBER coordinators, and others. Video should be treated as an experimental, voluntary, long, supplementary enhancement, not a near-term requirement, given the technical and massive cost

challenges of mandating any form of video support. Further, standards work relating to video would need to be done in coordination with the government.

Conversely, adding multimedia with alerts (such as images and maps) should be seen as a voluntary option, suitable for systems that can easily include this media in their customer-facing displays. For some systems, like ATSC 3.0's Advanced Emergency Information, alert multimedia could be prioritized as a short-term goal. Still, coordination is necessary with government agencies (especially FEMA IPAWS) to determine the types of multimedia needed and to ensure that relevant standards cover these aspects.

## **7 Pushing the Boundaries of EAS and WEA**

The Commission asks whether there are certain kinds of emergencies that EAS and WEA are not designed to adequately support today, and if so, what steps can be taken to better support those emergencies.

EAS and WEA are effective for fast-moving, geographically bounded hazards like tornadoes, earthquakes, AMBER Alerts, and national emergencies, but they are not designed or optimized for many other types of emergencies.

### ***7.1 Maintaining a Line between Emergency Alerting and Emergency Information***

Emergency Alerting refers to the issuance of short, authenticated, and high-urgency messages intended to capture immediate public attention and drive protective action. FEMA describes alerting within IPAWS as a “concise, time-sensitive message delivered through multiple communications pathways to rapidly inform people of imminent threats.”<sup>13</sup> By contrast, Emergency Information encompasses the broader, ongoing communications that follow or accompany alerts.<sup>14</sup> We are concerned that the direction of some of the Commission’s inquiries may inadvertently blur the line between the two.

Both are essential. Alerts trigger protective awareness, while emergency information sustains public understanding and response. The EAS and WEA primarily serve as an alerting mechanism, while partner communications fulfill the information role. A resilient public warning ecosystem requires both elements working together. But this should not mean that EAS or WEA are stretched to accommodate the emergency information role, which could have adverse consequences for system resilience and operations.

Digital Alert Systems’ DASDEC platform functions as a policy-based gateway that supports both emergency alerting and emergency information. For alerting, the DASDEC ensures that authenticated, concise warnings reach broadcast radio, TV, cable, satellite, and IPTV operators as

---

<sup>13</sup> <https://www.fema.gov/emergency-managers/practitioners/integrated-public-alert-warning-system>

<sup>14</sup> See Mileti, D. & Sorensen, J. Communication of Emergency Public Warnings: A Social Science Perspective and State-of-the-Art Assessment, Oak Ridge National Laboratory, 1990.

EAS. Simultaneously for emergency public information, the DASDEC can aggregate, manage, and route richer content—such as informational messages, video, graphics, multilingual text, and metadata—into downstream systems, including ATSC 3.0 Advanced Emergency Information (AEI) services, websites, over-the-top (OTT) apps, and other IP-based platforms. In this way, DASDEC bridges the gap between the alerting function that captures public attention and the information function that sustains public response, reinforcing the full public warning ecosystem.

It is important to emphasize that emergency alerting channels were not originally designed to carry the full weight of emergency information. Alerting systems such as EAS and WEA are optimized for brevity, urgency, and reliability—short messages that seize attention and drive immediate protective action. Asking these same channels to deliver longer, more complex content—such as multimedia files, video streams, or detailed instructions—risks undermining their core purpose. Bandwidth limitations, backward-compatibility issues, and message latency can all compromise the ability of alerts to break through quickly and effectively.

This is why a balanced ecosystem is essential. Alerting channels should retain their role as the “front door,” reliably capturing public attention with concise warnings. Emergency information should then flow through complementary distribution systems that can handle richer, multimedia content. Digital Alert Systems’ DASDEC supports this separation of roles, acting as a policy-based gateway that can both trigger immediate alerts and route extended information into the appropriate downstream services without overburdening the alerting pathway.

## **7.2 Comparing Scenarios and Tools**

For emergencies with broad, urgent impact, EAS offers particular strengths, such as during national emergencies, major storms or weather events, tsunami warnings, and multi-county Amber Alerts. EAS is *intentionally universal*, interrupting all viewers and listeners within a station’s service area. This “everyone hears/see it” approach is suitable when *widespread awareness is necessary*. In such situations, EAS remains essential for these blanket scenarios even with its current capabilities.

However, for emergencies that require precise geographic targeting, EAS has certain limitations. In these situations, EAS struggles because the nature of traditional audio and video distribution systems cannot confine the alert to just the affected FIPS or polygon. Audience members located miles away who are not at risk still receive the alert, but being outside the risk area doesn't necessarily mean they don't want or need the information. However, this geographic overreach

can result in *over-alerting* and alert fatigue, causing audiences to disregard messages when they might still be critical and impactful.

For these hazards, WEA is positioned as a precision tool (polygon targeting to 0.1-mile overshoot). EAS can improve at the margins by providing CAP-to-text crawls that display precise location instructions such as text and audio. ATSC 3.0 Advanced Emergency Information, potentially coupled with EAS, adds both the potential of a precision tool (with polygon targeting to location-aware devices), and goes further by integrating maps, graphics, extended instructions, or even follow-on video in ATSC 3.0 environments where feasible.

For emergencies requiring extended instructions, the local authority must make the decision of what information properly belongs in an “alert” and what belongs in supplemental or follow on “emergency information”. Today’s EAS is primarily an audio and text alert (though Digital Alert Systems has already been experimenting with symbology with its partners), and WEA supports textual messages. On the other hand, a short, targeted alert message is arguably not the optimal place to convey such extended information. EAS and WEA remain best leveraged as a “signal” and not necessarily the platform for detailed step-by-step information.

Finally, some emergencies develop quickly, such as a fast-changing weather event or a chemical plume drift. By design, EAS is designed to be intrusive and limited by linear transmissions that are not ideal for frequent updates, corrections, or cancellations. Ancillary services, such as ATSC 3.0’s supplementary AEI service as one example, are much better suited for rapid updates and cancellations. Similarly, WEA also provides better support for quick updates and cancellations.

EAS should continue to serve as an essential, initial wide-area attention-getter, with WEA and next-generation tools carrying subsequent refinements.

### **7.3 The Role and Value of EAS in an Evolving Landscape**

EAS is not, and may not become, a precision tool. Nor was it designed to be one. By design, once an EAS alert is issued, everyone watching that channel receives it. This approach is appropriate for national emergencies or hazards where widespread awareness is necessary. WEA, combined with EAS, offers a powerful solution.

Improvements for EAS can include additional support and training for alert originators, so that EAS and WEA can consist of precisely worded, understandable, and actionable textual information, even if broadcast universally.

Digital Alert Systems will continue to explore ATSC 3.0 video/multimedia for richer context, and we hope the Commission will as well, but keep the “alert” function simple and universal.

IPAWS is designed with the concept of “use every path you have” in a “system of systems” approach. FEMA’s guidance to Alerting Authorities is to push the same CAP alert over WEA and EAS (and NWR) to maximize reach. EAS catches people without phones, and with TV and radio on, WEA delivers precise polygons. EAS is still a valuable tool at the alert originators’ disposal. The use of EAS helps ensure that a critical threat to life and property is further communicated to those who may not have a cell phone at the ready, may not have a weather radio, or may otherwise find themselves out of touch.

## **8 Machine-to-Machine (M2M) Alerting**

The Commission raises the interesting question of whether accomplishing the nation's alert and warning objectives requires expanding the ability of EAS and WEA to support machine-to-machine alerting (e.g., using networked sensors to trigger automated protective action, such as slowing trains or closing water valves). If so, the Commission asks how EAS and WEA should be redesigned to better support these types of alerts.

### **8.1 M2M Communication**

While the primary role of EAS should remain to serve human users with authenticated public alerts, we are well-equipped to support M2M protective actions. Digital Alert Systems' DASDEC already offers several automated functions. For instance, the DASDEC can monitor an authenticated CAP feed and send signals to secure OT/ICS systems today.

While being careful not to blur human public warning with industrial control systems, we feel there is ample opportunity to extend the role of FCC-certified solutions like the DASDEC in this area. For example, systems like USGS' ShakeAlert could deliver machine-readable, digitally signed CAP messages directly to systems like the DASDEC to interface with downstream machines by physical or IP communication, for functions like digital signage, signaling control systems, interfacing with enterprise warning systems, etc. ShakeAlert could also send those alerts to IPAWS as a redundant path.

To better support an M2M ecosystem for time-critical sensor-based alerts, the current IPAWS CAP polling mechanism would suffice, but adding a low-latency push option directly to the DASDEC is preferable. A resilient, authenticated pub/sub interface to complement IPAWS-OPEN polling would enable the DASDEC to receive alerts quickly enough for automation, without transmitting binaries through public alert channels. Naturally, such a system should adhere to government guidelines on strengthening trust and identity for machines and industrial control systems. Another advantage of this approach is that solutions like the DASDEC already hold FCC certification and have completed the IPAWS conformity assessment process, providing an additional layer of confidence in an M2M ecosystem.

## 8.2 *Sensor-to-EAS Automation*

The concept of sensor-to-EAS automation holds additional promise. For hazards with seconds-to-minutes lead time (earthquakes, tsunamis, missile launches, radiological releases), automation can outpace human decision-making. Sensors can provide immediate, standardized data into CAP (or other formats, for that matter), reducing lag or local discretion.

For example, USGS ShakeAlert already pushes machine-generated CAP messages, which can be received by WEA (earthquake early warning on the West Coast). NOAA NWS automates certain warning issuance (e.g., tornado detection via Doppler radar) into EAS/WEA. The Department of Defense relies heavily on automated detection for specific activities. It would seem a logical step to explore the potential for secure, authenticated sensor-to-EAS automation for particular scenarios.

At the same time, policymakers need to consider issues related to direct sensor-to-public alerts (EAS). The risk of false positives should be evaluated, and relying solely on automation without human review could worsen errors. Similarly, context is crucial, and a human might be the key factor in deciding whether sensor data justifies EAS or WEA activation. An effective authentication process is vital, and all system components must have strong cryptographic identities to ensure EAS devices only trust verified inputs. Maintaining public trust in the nation's warning systems is essential. If the public perceives alerts as being automatically triggered without human judgment, confidence in the system could decline. If a Direct Sensor to EAS Model were considered, it may require a significant redesign of the trust model:

- **IPAWS certification for sensors.** Treating a sensor array (e.g., USGS, DOE radiological monitors) as a vetted “originator” with FEMA-issued digital certificates.
- **Event code constraints.** Limit sensor-originated alerts to a narrow set for a specific mission set relevant for that sensor (TSU, EQW, RHW).
- **Automated pre-scripted templates.** Messages must include pre-cleared, plain-language text and protective action, so the audio/crawl messages are immediately useful. Those automated templates could be stored by the EAS device (audio, text, and even appropriate multimedia) and issued upon being triggered by an authenticated sensor input/message.
- **Fail-safe review.** Where latency allows, require automated alerts to queue at the responsible authority with some form of review window. Where time is of the essence, allow full automation.

- **Robust cancellation.** Systems must support rapid “cancel”/“update” to cover any instance of false triggers, so that they can be quickly reversed.
- Direct sensor-to-EAS device triggering (bypassing IPAWS) should be **avoided** if possible for public warning purposes. It could undermine the uniform trust/authentication model and increase the risk of inconsistent messaging. On the other hand, such sensor-to-EAS triggering could have merit for critically time-sensitive alerts, insofar as a secure zero-trust environment could be maintained from the sensor to the EAS device.

### **8.3 Transparency and Governmental Oversight**

The FCC poses the question of having non-governmental entities transmit safety-related alerts and machine-to-machine alerting, and whether government agencies should be the sole initiators of alerts via the nation's alert and warning systems.

This goes to the heart of public warning system governance and balancing the public trust and accountability that only government authority provides. For this reason, we are reluctant to support direct industry activation of public warning assets such as EAS and WEA.

If utilities or automated systems were allowed to initiate alerts directly, then vetting, credentialing, auditability, oversight, and message consistency must be considered:

- **Federal Vetting and Credentialing:** Any non-government originator (utilities, transport operators, universities, sensors) must be vetted by FEMA/IPAWS and issued digital credentials, similar to those of authorized public agencies. The scope of use should be limited and carefully defined.
- **Auditability:** Each alert, whether triggered manually or automatically, must be recorded by the receiving device (FCC-certified, IPAWS-conformant unit) and IPAWS, creating detailed audit trails accessible to FCC/FEMA for review. Machine-generated alerts should be indicated as such in metadata for clarity.
- **Mandatory Public-Sector Oversight:** Even if a sensor triggers an alert, the system should notify the designated emergency management agency at the SLTT level, as well as FEMA IPAWS, to ensure human awareness and accountability. In situations where seconds count, such as earthquakes, alerts could be triggered automatically, but a post-incident review must be conducted by a public authority. Clear procedures and technical capabilities for message cancellation must be established for false alarms or machine errors, along with defined EAS procedures and processes for issuing follow-up messages.

- **Pre-Scripted Templates and Guardrails:** To prevent confusing, inconsistent, or panic-inducing messages, any automated or non-government alerts must use pre-approved templates with clear protective actions, and those public-facing templates should preferably be stored and maintained on the FCC-certified and IPAWS conformant device.

Again, we prefer an approach of government-sourced alerts over machine- and industry-issued public alerts. Federal, state, Tribal, territorial, and local government agencies have the statutory duty to protect public safety. That role includes responsibilities not shared by private companies or machines. The public views an “official” EAS/WEA alert as credible mainly because it originates from a government agency. Diluting that trust by allowing private actors to issue alerts could weaken that credibility.

Unless speed is the key factor in protecting life and property, government agencies should remain the only ones initiating public-facing EAS/WEA alerts. This preserves accountability and trust. Non-governmental entities and machine sensors can contribute information but not bypass the system. Sensors can send data to SLTT or Federal agencies, which then decide (sometimes automatically, through pre-authorization) whether that data should trigger a public alert. This model maintains speed (since automation and templates can be nearly instant) but preserves legitimacy (because the “final step” is still a public authority pressing “send,” even if automatically delegated under predefined rules).

## 9 EAS: Guaranteed Delivery or Best Efforts?

The commission asks whether the nation's alerting systems should be designed with the purpose of **guaranteeing** delivery of each alert to the intended audience (regardless of the conditions on the ground) versus only a "**best effort**" attempt at delivery and rely on the likelihood that the audience will receive at least one alert from a number of possible sources.

There can be no "guarantee" of per-person delivery under all conditions. As a hybrid voluntary/mandatory EAS system, there can be no reasonable expectation or guarantee of **absolute** delivery by all EAS Participants under all conditions, much less a guarantee of delivery to the intended audience. The nation's system should therefore be designed and regulated for redundant, authenticated, multi-path delivery with measurable performance targets, reserving the strongest obligations for the rarest, highest-consequence alerts (e.g., Presidential). This approach aligns with how FEMA/IPAWS and the Commission already frame the ecosystem.

### 9.1 EAS as a Hybrid: More than Best Efforts, But Less than Guaranteed.

EAS is neither a true "guaranteed service" system or a fully laissez-faire "best effort." It's best described as an "unfunded mandated best effort" system, with core national obligations but inconsistent reliability outside that scope. Today, EAS is a hybrid of sorts.

In practice, EAS is a best-efforts system for state/local alerts and geographic/technical reliability (uneven coverage, no guaranteed precision). At the same time, it is a mandated but still non-guaranteed system because the FCC requires participation, but the government does not provide resources to ensure uniform robustness. EAS is not deterministic because there are no delivery guarantees, no quality-of-service measures, and failure modes exist in the daisy-chain relay system.

The elements of EAS that lean toward a Best-Efforts system include:

- **Unfunded mandate:** Participants are required to comply, but must self-fund equipment and upkeep, leading to uneven implementation quality.
- **Relay-chain dependence for FSK EAS:** Alerts propagate hop-by-hop through monitored stations. A failure upstream can block downstream delivery (no guaranteed redundancy).

- **Singular dependence on conventional Internet for CAP EAS.** EAS Participants maintain EAS gear that polls IPAWS OPEN over the Internet, with all the accompanying potential risks of system outages, last mile interruptions, etc.
- **Limited enforcement of state/local alerts:** Beyond national alerts, participation varies by state plan, meaning coverage consistency isn't guaranteed.
- **Equipment variability:** Variations due to different vendors, configuration differences, and potential inconsistencies in results.

At the same time, EAS is not purely a Best-Effort:

- **Mandatory national alerting:** Presidential/National alerts must be relayed by all Participants, which is a strict requirement and not optional. Additionally, FEMA's NPWS/PEP network offers a secure broadcast backbone for national messaging. These rules establish capability guarantees (architecture, obligations) but do not guarantee that every individual will receive the message.
- **Testing regime:** Regular RWTs/RMTs ensure at least a readiness baseline.
- **Regulatory oversight:** FCC inspections, logs, and fines for noncompliance create a stronger obligation than "we'll try if we can."
- **Performance is high but not perfect, consistent with a "best-effort plus redundancy" design.** In the 2023 nationwide test, 96.6% of EAS participants received the message, and 93.6% retransmitted it, revealing a strong, but not absolute or guaranteed system.

## 9.2 Enhancing EAS Performance

The current FCC proceeding explicitly asks whether to shift from "best efforts" to some form of guaranteed delivery for certain messages (e.g., Presidential), and whether voluntariness influences originator confidence. Without additional support from the government—such as moving EAS from an unfunded mandate to a formal government-run program—the goal might be more appropriately focused on guaranteed *capabilities* and reliable, high-probability (though not guaranteed) delivery through multiple resilient paths.

There are indeed certain types of alerts, such as alerts sent by the President, for which delivery must be consistently guaranteed for the objectives of the alerting system to be satisfied. "National Alerts" (President/FEMA/President's designee) may warrant the strongest, nearly guaranteed obligations, while most other alerts should aim for high probability through redundant, multi-path delivery rather than an impossible per-person guarantee. Today's rules already reflect this

tiering: EAS carriage of national alerts is mandatory, and participating WEA carriers must immediately and with the highest priority transmit National Alerts; by contrast, state and local EAS carriage and carrier participation in WEA are voluntary.

For *national* alerts, the Commission can reasonably expect and require architecture and operational responsibilities that aim for reliability to be “must-not-fail,” while recognizing that true per-person guarantees are impossible (power off, out of coverage, device limitations).

### **9.3 Voluntary versus Mandatory Participation**

The question is whether voluntary, rather than mandatory, participation in the nation's alerting systems reduces alert originators' confidence that their alert will reach their targeted audience. Again, based on our direct experience working with SLTT alert originators, the short answer is a qualified “yes”. This, for example, is one reason that some SLTT originators rely solely on WEA more than broadcast EAS.

Certainly, the FCC Rules allow EAS Participants discretion in transmitting alerts at the state and local levels (i.e., carriage is not mandatory, which reduces the likelihood that a local alert will interrupt programming everywhere). Additionally, FCC Rules give EAS Participants an extra window of up to 15 minutes to transmit non-national emergency alerts. In our experience, the broadcasters we work with are responsible and diligent about promptly transmitting emergency alerts related to threats to life and property. However, a disparity remains in the mechanisms and requirements between EAS and WEA alert transmission.

Voluntary participation partly aligns with the goals of the nation's alert and warning systems. The objective is to safeguard life and property through redundant, authenticated, multi-path alerting. While voluntary participation has achieved broad coverage, it still leaves gaps that are significant for coverage, availability, and confidence.

## 10 The Resilience of EAS Under “All Conditions”

We agree with the Commission that it is reasonable to expect alerts will be successfully transmitted by EAS Participants during blue-sky conditions, but alerting systems should also incorporate resilience to common causes of disruption to communications, such as power outages and physical damage to infrastructure, to accommodate “gray-sky” conditions.

Below, we offer suggestions on approaches to improve the resilience of the national EAS and better achieve the objectives of the nation's alert and warning systems. This is a fundamental question, and the Commission is correct to emphasize that resiliency is not a “nice-to-have”; it is the purpose of EAS. To address this question, we need to consider it in terms of “blue-sky” versus “gray-sky” performance.

- **Blue-sky (normal conditions):** At least for national EAS activations, it is reasonable to expect near-universal, timely delivery of alerts to all targeted members of the public. The 2023 national test results showed strong performance of both EAS and WEA when networks were up, which aligns with originators’ expectations.
- **Gray-sky (regionally or temporarily disrupted conditions):** The system must assume loss of commercial power, internet, and related services in affected areas. In these conditions, redundant, independent alerting channels are not just desirable but *essential* to protect life and property.

However, an important differentiation between EAS and other public warning capabilities is the intended resilience and continued operation during even more severe conditions:

- **Black-sky (catastrophic disruption):** This would be a low-probability, high-impact event that causes longer-duration, widespread failures of critical infrastructures simultaneously—such as extended grid-down scenarios, geomagnetic disturbances, coordinated cyberattacks, nuclear detonation (EMP), or extreme natural disasters.

Under “black-sky” conditions, the assumption is that most or all conventional communications and power systems may be unavailable for extended periods. In this scenario, even redundant channels may not suffice unless they are hardened and sustained independently of commercial lifelines. Alerting objectives shift from timely delivery to any delivery at all, prioritizing hardened, off-grid, survivable pathways (e.g., EAS via broadcast radio, satellite, or other pre-positioned systems). The discussion of modernizing the nation’s EAS must factor in this level of

resilience and survivability. We emphasize that EAS remains very relevant and essential to keep as a backup dissemination method, ensuring availability when other communication channels – including the Internet – are not working.

### ***10.1 Resiliency Approaches That Achieve National Objectives***

The effectiveness of the nation’s alert and warning systems depends not only on their performance under normal “blue-sky” conditions but also on their resilience during times of crisis, when power, communications, and network infrastructure might be disrupted. Resilience must therefore be addressed on two separate levels: the public-facing delivery of alerts to the public and the dissemination of alerts to EAS Participants themselves.

On the public-facing side, the Commission should continue to rely on a multi-path architecture that ensures alerts are received even when one or more pathways are impaired. EAS provides a resilient broadcast backbone, WEA delivers precise, geo-targeted alerts directly to individuals, and NOAA Weather Radio offers a separate layer. These are further reinforced by emerging pathways, though these may well lack the resilience of EAS. No single system can guarantee universal receipt, but a diversified ecosystem greatly increases the likelihood that members of the public will receive life-saving alerts under degraded conditions. The backbone and fallback for even a diversified ecosystem is EAS.

On the dissemination side, resiliency begins with how alerts are delivered to EAS Participants. The Commission should encourage and support a multi-path dissemination model that combines IPAWS CAP internet delivery, traditional broadcast relay, and supplemental broadcast data distribution (such as the Ohio OEAS project). CAP-first configurations with triggered polling ensure that EAS Participants use the richest version of the alert when available while falling back to broadcast relay if IP delivery fails. Supplemental broadcast-based CAP dissemination adds a further resilient channel that is not dependent on local connectivity. Together, these approaches ensure that EAS Participants can always ingest alerts reliably, regardless of the conditions on the ground.

#### **Broadcast Backstop (EAS/NPWS/PEP) is still necessary.**

EAS was designed to operate when other communications fail, via independently powered broadcast facilities, AM/FM radio, and NPWS/PEP (Primary Entry Point) stations hardened with backup power, fuel, and satellite links. FEMA’s National Public Warning System maintains approximately 77 PEP stations with hardened facilities designed to cover more 90% of the U.S.

population even in severe disruptions. EAS relay at the state and local level provides alert relay when Internet access to IPAWS is unavailable to alert originators, EAS Participants, or both.

Broadcast backhaul remains relevant today. Broadcast does not depend on local towers or internet backhaul; a battery-powered AM/FM radio can still receive alerts. During extended power/cell outages (wildfires, hurricanes), broadcast has demonstrated its role as a lifeline.

The broadcast EAS backbone is still *necessary*, though it should be modernized. We offer recommendations on modernization of the EAS backbone elsewhere in our comments.

### **Cellular Resiliency (WEA)**

In blue-sky conditions WEA now reaches more than 91% of adults with functioning phones. To accommodate gray-sky scenarios, carriers maintain backup power at certain sites, but cell networks are still vulnerable to extended outages (wildfires, hurricanes, earthquakes). While mobile alerting via WEA is now nearly ubiquitous, the need for multipath redundancy is clear – including the need for broadcast EAS.

### **Multi-Path Redundancy**

IPAWS’s core design (“one alert, many paths”) should be reinforced:

- EAS (broadcast/cable/satellite)
- WEA
- NOAA Weather Radio (VHF, independently powered, covers 95% of population)
- Emerging technologies, like ATSC 3.0 for richer data delivery

The expectation is that no *one* system guarantees delivery, but redundant systems compensate for each other when infrastructure is impaired.

### **Does the Traditional EAS Resiliency Model Remain Necessary?**

In short, yes. Even though most Americans rely on mobile phones, EAS’s broadcast-based, independently powered backbone remains the most resilient layer when power grids or networks fail. WEA cannot fully replace it because cell sites and devices depend on local power and backhaul. While NPWS/PEP is a “system of last resort” to reach the entire nation during catastrophic failures, state and local EAS continue to play a crucial role in keeping citizens informed during local emergencies. However, there is still significant room for EAS to improve without losing its hardened broadcast core.

## **10.2 Conclusion**

It is wholly reasonable to expect full delivery in blue-sky conditions, and the system must be resilient against gray-sky disruptions. The traditional broadcast-based resiliency of EAS (via NPWS/PEP) remains necessary today. It is the only layer not dependent on local power or IP infrastructure. Resiliency is best achieved through redundancy: hardening WEA, sustaining EAS/NPWS, maintaining NOAA Weather Radio, and educating the public on backup receivers.

EAS broadcast resiliency remains crucial today - it is the only layer capable of functioning when local power, internet, and cellular networks are disrupted. The Commission should reaffirm that the broadcast-based resiliency of the Emergency Alert System, anchored by FEMA's National Public Warning System and its network of hardened Primary Entry Point stations, remain vital to the nation's alerting objectives. Unlike IP- and cellular-based systems, broadcast radio and television can continue operating during widespread power outages and network failures, and battery-powered receivers help ensure the public can still receive life-saving information during catastrophic events. While modernization of WEA and deployment of targeted transmission technologies other media architectures will improve accuracy and detail, broadcast resiliency remains a unique and indispensable safeguard in the nation's multi-layered alerting framework.

Below is a table contrasting resiliency strengths/weaknesses of EAS, WEA and NWR, illustrating the essential complementary of these systems.

## **11 Are there other alternative communications pathways that EAS and WEA can leverage to ensure redundancy?**

We believe that there are other alternative pathways that EAS can leverage to ensure redundancy, and this is a place where the record is strong: EAS and WEA should not be the only pipes, but part of a redundant “one message, many paths” ecosystem. FEMA and the FCC have already stressed this, and FEMA’s IPAWS is architected to fan out a single CAP message across multiple delivery mechanisms.

To achieve the nation’s alerting objectives, the Commission should continue using a multi-path, redundant architecture for public alerts. EAS provides the most reliable backbone through broadcast facilities that work even during large-scale outages; WEA sends targeted alerts directly to individuals; and NOAA Weather Radio provides an independently powered national layer. These are further supported by new channels like ATSC 3.0, internet apps, connected vehicles, and smart devices. No single system can ensure everyone gets alerts, but a diverse system increases the chances that the public will receive life-saving alerts even during adverse conditions.

### **11.1 Expanding Redundancy in EAS Dissemination.**

The Commission has traditionally concentrated on redundancy in the *public-facing* parts of the nation’s alert and warning systems, making sure that the public can receive alerts through multiple channels, like EAS, WEA, and NOAA Weather Radio. Equally as critical is resilience in the dissemination of alerts to EAS Participants. If EAS Participants cannot reliably receive alerts in the first instance, then public-facing redundancy cannot be achieved.

The Commission should recognize that resilience in the nation’s alerting systems starts with how alerts are delivered to EAS Participants. A multi-path dissemination approach, combining IPAWS CAP internet delivery, traditional broadcast relay, and additional broadcast data distribution (such as Ohio’s OEAS project), makes sure that EAS Participants always have at least one reliable way to get alerts, even during widespread power outages or network disruptions. CAP-first setups with triggered polling should be emphasized as best practice, supported by redundant broadcast-based CAP distribution to enhance both accuracy and resilience.

### **Current IPAWS Dissemination Model**

Historically, the EAS architecture has relied on a broadcast relay model: designated stations receive alerts via AM, FM, or NOAA Weather Radio, and retransmit them down a daisy chain of monitored sources. This approach remains essential for resiliency because it leverages independently powered broadcast facilities capable of operating during power outages and internet failures. However, it can introduce latency, duplication, or failure propagation when upstream stations experience disruptions.

Common Alerting Protocol delivery offers significant improvements in clarity, accessibility, multilingual support, and lifecycle management (updates and cancellations). The Commission has already taken important steps to mandate CAP monitoring and use, and CAP should continue to be the preferred method for alert dissemination whenever possible.

Updated EAS devices feature a “CAP-first” design that uses triggered CAP polling to ensure high resilience. Digital Alert Systems first introduced this approach in 2018 and are grateful the Commission later required all EAS devices to adopt it. Under this method, EAS equipment continues to monitor traditional broadcast relay sources, but when an EAS header is detected, the device immediately queries IPAWS to determine whether a CAP version of the alert is available. If it is, the CAP message is used; if not, the device falls back to the EAS FSK broadcast relay copy. This approach guarantees that the system delivers the richest form of the alert during normal operation while maintaining a reliable fallback if internet connectivity is impaired.

While this approach is effective, we have long believed that the current dissemination model is incomplete or only a partial solution. Therefore, Digital Alert Systems has been working to enhance the Internet-based IPAWS OPEN polling mechanism by adding wireless data broadcast relay of the IPAWS OPEN feed.

### **Digital Alert Systems: Working on Supplemental Dissemination Innovations**

Redundant dissemination is further enhanced by initiatives like the Ohio OEAS project discussed in Section 8, which uses ATSC broadcast data channels to send IPAWS CAP messages to EAS Participants statewide. This method combines the reliability of broadcast with the accuracy and information-rich messaging of CAP:

- Does not depend on local internet access at any of the receive stations.
- Full CAP content, including rich text, accessibility options and multilingual content.

- Offers a broad coverage area, ensuring EAS devices across the state can receive alerts even if IP networks are down.

The Commission should recognize that resiliency must be ensured at both the dissemination and public delivery layers of the nation’s alerting architecture. Specifically, the Commission should:

1. Reaffirm CAP-first configuration for all EAS Participants.
2. Support broadcast-based CAP distribution pilots (such as Ohio OEAS) as a complementary dissemination path that enhances resiliency against cyber incidents, local power outages, or IP network failures.
3. Emphasize the need for multiple ingestion paths, IP delivery, traditional radio relay, and broadcast data distribution, so that EAS Participants can reliably acquire alerts under degraded conditions.

Resiliency begins not only with how alerts are presented to the public, but with how they are delivered to EAS Participants. By strengthening and diversifying dissemination pathways, the Commission can ensure that EAS Participants always have at least one reliable method to acquire alerts, regardless of the conditions on the ground. This multi-path dissemination model, combining IPAWS CAP delivery, broadcast relay, and broadcast data supplements, provides the strongest assurance that alerts will propagate quickly, accurately, and resiliently throughout the national system.

### ***11.2 Should EAS and WEA both be independently resilient (i.e., having multiple redundant pathways within EAS)?***

Ideally, each system should have independent resiliency within its own stack and should enhance cross-system redundancy so one can take over if the other fails. This means (a) EAS must still function if IP and cellular services are down; (b) WEA must remain reliable on operational cellular networks; and (c) IPAWS should continually issue authenticated CAP messages across *all* available paths simultaneously.

EAS and WEA should each be independently resilient. Disasters often disable an entire family of infrastructure (e.g., cellular), while broadcast continues to operate, and vice versa. FEMA’s NPWS/PEP broadcast backbone exists specifically for “grid/backhaul down” scenarios; it should be maintained and modernized (CAP-first, multiple ingest paths). Meanwhile, WEA remains the

precise, per-device path when cellular is functional. You don't want either system to rely on the other to operate at all.

Cross-system redundancy (EAS covers WEA, and vice versa) is necessary but not sufficient. IPAWS's "one alert, many paths" design is the correct overlay, but each path must still operate independently when others fail. In practice, originators expect a single CAP alert to be authenticated and delivered simultaneously to WEA, EAS, and NWR, so the loss of any one path does not prevent the message from getting through.

Our recommendation is to continue building independent resilience within EAS and WEA, *and* use IPAWS to deliver the same authenticated CAP message through multiple, diverse paths. Explore additional voluntary technologies as future layers, but don't rely on them yet. This layered approach best meets the system's life-and-property objectives under both ideal and degraded conditions.

## 12 Security of the Nation's Alerting Systems

Digital Alert Systems firmly supports the Commission's view that the nation's alerting systems must be secure against cyberattacks from our nation's adversaries. Maintaining trust in these systems is vital for both national security and achieving the nation's alerting goals. As a manufacturer of EAS encoder/decoders and provider of CAP/EAS origination systems, Digital Alert Systems has firsthand insight into the security challenges and opportunities facing the alerting ecosystem. We offer the following perspectives on the importance of security in EAS/CAP devices, based on practical, real-world experience:

- **Trust and legitimacy:** A single cyber-compromised alert, especially one carrying false or malicious content, can erode public confidence and lead to real-world harms (panic, mistrust, non-compliance with future alerts).
- **Critical infrastructure status:** EAS and CAP origination systems are considered vital parts of national critical infrastructure. If adversaries gain control of these systems, they could disrupt emergency messaging or spread disinformation on a large scale.
- **Attack surface:** Encoders/decoders, CAP servers, and dissemination paths all operate on IP-based networks, so they are vulnerable to the same classes of attacks, such as credential theft, denial-of-service, spoofing, and supply chain tampering, that adversaries have used against other public-safety systems, enterprises and critical infrastructure.

### 12.1 Security Posture

Digital Alert Systems is striving to maintain a strong security posture, leveraging current mitigations already in place:

- **Digital signatures in CAP/IPAWS:** FEMA's IPAWS requires authentication and digital signatures on CAP messages, allowing devices to reject unauthenticated or tampered alerts. However, we believe the FCC's rules should be amended to require authentication and digital signatures of every CAP message received by an EAS CAP device, not just those received from FEMA IPAWS.
- **Firmware and software updates:** Digital Alert Systems provides regular security patches; our devices support authenticated, signed updates to ensure integrity.

- **Network segmentation guidance:** FEMA and FCC recommend isolating EAS devices from general-purpose business networks to reduce lateral attack opportunities. Digital Alert Systems has actively worked to educate EAS participants on this matter and to reinforce this message by making separate network interfaces available.
- **Logging and audit trails:** CAP/EAS devices maintain logs that allow after-action review and anomaly detection. Digital Alert Systems developed and deployed the HALO™ system to further facilitate remote monitoring, maintenance, and anomaly detection.

However, there are ongoing vulnerabilities and challenges.

- **Legacy EAS relay chain:** The over-the-air daisy chain relies on unauthenticated analog header tones, making them inherently spoofable. Several security researchers have claimed the ability to spoof legacy EAS via various techniques and scenarios.
- **Device exposure:** Despite industry and FEMA guidance, a small handful of encoder/decoder units remain directly accessible from the open Internet, creating unnecessary entry points for adversaries.
- **Operator practices:** Weak passwords, shared accounts, and failure to apply software updates continue to pose systemic risks.
- **Gray market sales:** Gray-market EAS encoders/decoders (i.e., used equipment sold on auction websites) can ship with outdated firmware and unremoved configurations or credentials, allowing attackers to exploit known vulnerabilities or use retained settings to impersonate sources and inject false alerts. Buying outside trusted supply chains also breaks provenance and tamper controls, increasing the risk that compromised or counterfeit hardware—preloaded with malware or altered settings—enters live alerting paths.
- **Supply chain risk:** As with any hardware or software, adversaries may attempt to exploit vulnerabilities in the manufacturing or distribution chain. Digital Alert Systems maintains a highly controlled supply chain, focused on the US manufacture of its public warning products in its own factory.

Securing the nation's alerting systems requires both technological safeguards and operational discipline. IPAWS authentication, multi-path redundancy, secure EAS appliances, and robust cyber hygiene together form the foundation. Federal standards and Commission rules can help ensure consistent implementation across thousands of EAS Participants, preventing weakest-link vulnerabilities.

A resilient, secure, and trusted alerting system depends on treating every EAS encoder/decoder in the field as part of critical infrastructure, ensuring they are regularly updated, operated according to best practices, and supported by Commission rules that uphold these requirements.

## ***12.2 Securing the Nation's Alerting Systems: The Role of EAS Device Manufacturers and Standards***

Digital Alert Systems agrees that securing the nation's alerting systems is essential to both national security and public safety. As a manufacturer of EAS encoder/decoders and CAP origination systems, we see daily the risks posed by cyber threats, as well as the critical importance of designing, building, and maintaining equipment that is resilient to attack.

EAS device manufacturers are a foundational part of the national alerting ecosystem. Security cannot be an afterthought; it must be embedded in design, testing, and lifecycle support. From our perspective, manufacturers should be expected to follow the following practices:

- Secure Software and Firmware Development:
  - Follow secure coding practices and conduct static and dynamic code analysis.
  - Apply supply chain integrity protections (e.g., signed binaries, controlled build environments).
- Authenticated Updates:
  - Provide digitally signed firmware/software updates to prevent tampering.
  - Ensure devices reject unsigned or altered update packages.
- Configuration Security:
  - Ship devices with hardened default settings (no default passwords, forced credential changes at setup).
  - Minimize exposed services and disable insecure legacy protocols.
  - Tightly controlled, maintained and updated operating systems.
- Access Controls:
  - Support role-based access control for operators and administrators.
  - Provide audit logging of configuration changes and alert activity.
- Secure Deployment Guidance:
  - Publish baseline security hardening guidance for broadcasters and cable operators.
  - Provide tools for monitoring device health and integrity in real time.

- Vulnerability Management:
  - Maintain a public process for vulnerability disclosure and response.
  - Commit to timely patches for critical vulnerabilities and communicate remediation clearly to customers.

### ***12.3 Importance of Certified, Standards-Conformant Equipment***

The public alerting system is only as secure as its weakest component. Equipment should not be left to inconsistent vendor practices or uneven user implementation. Instead, government certification and standards conformance are essential.

- **Conformance Testing:** All EAS equipment should be subject to third-party conformance testing against FCC Part 11 rules, FEMA IPAWS CAP profiles, and NIST cybersecurity standards. This ensures consistent implementation across thousands of EAS Participants.
- **Federal Certification:** Devices should be required to demonstrate expanded compliance with:
  - FCC Part 11 and Part 15 requirements (functional and performance).
  - FEMA IPAWS CAP profile for message authentication and validation.
  - NIST Cybersecurity Framework controls appropriate for critical infrastructure.
- **Secure Supply Chain Certification:** Manufacturers should be required to demonstrate secure supply chain practices, including hardware integrity protections and component traceability.
- **Continuous Recertification:** Certification should not be a one-time test. Regular (e.g., biennial) recertification, including penetration testing, should be required to ensure devices remain secure against evolving threats.

### ***12.4 Supply Chain Integrity for Core EAS Equipment***

The Commission aims to ensure that the nation's alerting systems stay secure, resilient, and trustworthy. In this context, supply chain integrity for key alerting equipment, including certified EAS/CAP appliances, encoders/decoders, and gateway software, is a matter of national security. These devices – and any hardware or software associated with carrying out EAS functionality – acts as the trust anchors of the Emergency Alert System, providing essential functions like cryptographic validation, alert routing, policy enforcement, and deterministic insertion into broadcast and cable programming chains.

Because of this central role, any compromise of these systems, whether through malicious hardware components, unvetted software libraries, or compromised firmware update pipelines, could directly undermine the reliability and authenticity of public alerts. Since EAS Participants are themselves designated as part of the nation's critical infrastructure, the Commission should recognize the supply chain security of EAS appliances as essential to the nation's public safety posture.

Our recommendations in this area include:

1. **Certification Requirement:** The Commission, in coordination with FEMA and DHS/CISA, should establish a certification program for all EAS appliances and software that verifies:
  - Compliance with FCC Part 11 and CAP standards.
  - Implementation of secure boot, signed firmware, and cryptographic trust-anchor management.
  - Maintenance of Software Bills of Materials (SBOMs) and adherence to coordinated vulnerability disclosure practices.
  - Use of secure, authenticated channels for software and firmware updates.
2. **Trusted Manufacturing and Assembly:** The Commission should require that the final assembly, firmware signing, and certification of EAS systems, including both the software and hardware elements, occur within the United States or trusted-trade jurisdictions subject to U.S. regulatory oversight. While recognizing that many components (e.g., semiconductors, boards) are globally sourced, the point of integration, software deployment, firmware deployment, and device certification should be under trusted U.S. or allied control.
3. **Supply Chain Transparency:** Vendors of EAS appliances should be required to provide supply chain transparency documentation, including:
  - Identification of primary manufacturing and assembly locations.
  - Identification of software programming sources and locations.
  - Secure handling practices for firmware and cryptographic keys.
  - Attestations regarding the absence of known high-risk vendors identified by U.S. government supply chain security reviews.
4. **Ongoing Oversight:** Certification should not be a one-time requirement. Vendors should be subject to recertification at defined intervals, particularly when hardware platforms, operating systems, or cryptographic modules are updated.

By establishing supply chain requirements for EAS appliances, the Commission can help ensure that the core elements of the nation's alerting infrastructure remain trustworthy and resilient. Such a requirement does not preclude global sourcing of components but ensures that the devices responsible for validating and forwarding public alerts are assembled, signed, and certified under U.S. jurisdiction.

This approach reinforces public trust, reduces systemic cyber risk, and aligns EAS supply chain policy with broader national security measures already in place for other sectors of critical infrastructure. We would go so far as to suggest that 47 C.F.R. Part 11 be amended to add new subsection 11.56 on "Supply Chain Integrity of EAS Equipment.

Such a new § 11.56 for the Supply Chain Integrity of EAS Equipment could cover the following elements:

- **Certification Requirement.** All EAS solutions, including EAS encoders/decoders, must be certified by the Commission, in coordination with FEMA, to ensure compliance with applicable security and interoperability standards.
- **Trusted Manufacturing and Assembly.** Final assembly, firmware signing, and certification of EAS solutions must occur within the United States or in jurisdictions designated by the Commission as trusted for supply chain security purposes.
- **Software and Firmware Integrity.** Certified EAS solutions must:
  - Implement secure boot and cryptographically signed firmware;
  - Maintain a Software Bill of Materials (SBOM) identifying all included software components;
  - Provide for secure, authenticated firmware and software update mechanisms; and
  - Comply with coordinated vulnerability disclosure requirements as specified by the Commission.
  - Require disclosure of country of origin for all software components and any associated development activities, to enhance transparency and enable risk assessment of the software supply chain; and
  - Require production and development of critical software elements be conducted within the United States, ensuring greater oversight, security assurance, and protection against foreign influence.
- **Supply Chain Transparency.** Manufacturers of certified EAS solutions must disclose:
  - The location of primary manufacturing and assembly;

- Supply chain risk mitigation practices, including secure handling of cryptographic keys; and
- Identification of any hardware or software components sourced from vendors determined by the United States Government to pose a national security risk.
- **Ongoing Oversight.** We recommend that Certification for the above requirements should remain valid for a period of not more than three (3) years. Recertification would be required upon any hardware, software, or cryptographic module changes, or upon expiration of the certification period.

### ***12.5 Precedents for Supply Chain Integrity Policy***

The Emergency Alert System remains a cornerstone of the United States' public alert and warning architecture. Its core functions—validating, authenticating, and distributing emergency alerts to broadcasters, cable systems, and other EAS Participants—rely on specialized EAS/CAP devices. These devices act as trust anchors in the alerting process, ensuring that authenticated alerts are integrated into programming streams even during degraded communication conditions.

Unlike consumer devices or downstream presentation platforms, EAS appliances operate at the plant and headend level, where they perform cryptographic validation of CAP messages, enforce CAP-first requirements, manage redundancy across multiple delivery paths, and provide secure logging and audit functions. Because of this unique role, any compromise of these devices would directly weaken the authenticity, reliability, and credibility of the nation's alerting system.

The Commission has already recognized the national security implications of supply chain integrity in the nation's communications networks:

- In FCC Docket 19-351 (Protecting Against National Security Threats to the Communications Supply Chain), the Commission prohibited the use of equipment from Huawei, ZTE, and other entities deemed security risks. The related Secure and Trusted Communications Networks Reimbursement Program underscores the importance of ensuring that critical communications infrastructure is sourced from trusted vendors.
- In FCC Docket 21-68 (Improving the Emergency Alert System and Wireless Emergency Alerts), the Commission sought comment on improving the security posture of EAS and WEA, including device-level protections and resilience against cyber threats.
- DHS CISA and NIST have issued repeated guidance emphasizing supply chain risk management (SCRM) as a fundamental principle for securing critical infrastructure. The

White House's Executive Order 14028 (Improving the Nation's Cybersecurity, 2021) explicitly directs agencies to adopt measures such as SBOMs and secure update pipelines to strengthen software and firmware integrity.

The Commission's work on these dockets demonstrates a consistent recognition that the supply chain itself is a security vector. EAS appliances act as the policy enforcement gateway between IPAWS and broadcast/cable delivery. Since EAS Participants are designated as critical infrastructure, EAS solutions used at these sites should meet the same supply chain integrity standards applied to other sectors like telecom, energy, and transportation.

The benefits of a supply chain requirement are multiple:

1. **National Security:** Requiring final assembly, firmware signing, and certification in the U.S. or trusted jurisdictions prevents adversarial manipulation of alerting gateways.
2. **Resilience:** Ensures continuity of parts, assembly, and technical support during crises, independent of geopolitical disruptions.
3. **Transparency:** SBOMs and supply chain documentation improve visibility for both regulators and operators.
4. **Accountability:** U.S.-based certification ensures that patch cycles, vulnerability disclosure, and firmware management occur under U.S. legal and regulatory oversight.
5. **Alignment with FCC Precedent:** Builds directly upon supply chain restrictions in Docket 19-351 and cybersecurity measures under consideration in Docket 21-68, extending them logically to the core trust anchors of EAS.

The Commission should adopt supply chain integrity requirements for EAS appliances and gateway software, ensuring that these devices are assembled, certified, and signed within trusted jurisdictions and subject to FCC/FEMA certification. This action would bring EAS policy into alignment with the Commission's broader supply chain security measures, reduce systemic cyber risk, and reinforce public trust in national alerting.

By anchoring this proposal in the Commission's ongoing dockets (19-351, 21-68) and in cross-agency guidance (CISA, NIST, EO 14028), the Commission can strengthen the alerting infrastructure while leveraging existing policy frameworks.

**Crosswalk: FCC Supply Chain and Cybersecurity Precedents Applied to EAS Devices**

<b>Policy Area / Precedent</b>	<b>Relevant FCC Docket / Policy Action</b>	<b>Key Requirements / Findings</b>	<b>Application to EAS Appliances (Proposed)</b>
<b>Supply Chain Security in Telecom Networks</b>	Docket 19-351 – Protecting Against National Security Threats to the Communications Supply Chain	FCC prohibited use of equipment from Huawei, ZTE, and other covered companies; established the Secure and Trusted Communications Networks Reimbursement Program.	Apply the same principle to EAS appliances, requiring that final assembly, firmware signing, and certification occur in the U.S. or trusted jurisdictions, with exclusion of high-risk vendors from the EAS supply chain.
<b>Cybersecurity of EAS/WEA Systems</b>	Docket 21-68 – Improving the Emergency Alert System and Wireless Emergency Alerts	FCC sought comment on measures to strengthen EAS device security, including patching practices, authentication, and resilience to cyberattacks.	Extend these requirements into a formal certification process for EAS devices, covering secure boot, signed firmware, SBOMs, authenticated updates, and periodic recertification.
<b>Critical Infrastructure Risk Management</b>	DHS CISA / NIST SCRM Guidance; White House EO 14028 (2021)	Emphasizes software supply chain integrity, SBOMs, secure update pipelines, and vulnerability disclosure.	Require EAS vendors to provide SBOMs, disclose supply chain practices, and adhere to coordinated vulnerability disclosure, ensuring transparency and resilience.
<b>FCC / USG Recognition of Broadcast / Cable / EAS as Critical Infrastructure</b>	Presidential Policy Directive 21 (PPD-21); Executive Order 13873; Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA); Secure and Trusted Communications Networks Act of 2019; DHS CISA “Critical Infrastructure Sectors” list; National Infrastructure Protection Plan (NIPP); and FCC ET Docket No. 21-232 and EA Docket No. 21-233; FCC 22-84	EAS Participants (broadcasters, cable operators) designated as part of critical communications infrastructure, including supply chain requirements.	Require core EAS appliances to meet supply chain and cybersecurity standards equivalent to those applied to other critical communications infrastructure.

This proposal is a logical extension of FCC precedent. Docket 19-351 establishes that supply chain integrity is a communications security issue. Docket 21-68 establishes that EAS device security is already on the FCC's radar. EO 14028 and CISA/NIST SCRM guidance provide federal policy backing for supply chain and software integrity requirements. As a manufacturer of advanced public warning systems, we believe these principles must apply directly to the core trust anchors of the EAS (FCC certified EAS/CAP devices) to ensure public trust in national alerting.

The Emergency Alert System depends on certified EAS appliances, like the DASDEC, which sit at the plant or headend as the trust anchors of our national alerting architecture. These devices validate, authenticate, and insert alerts into programming, and if they were ever compromised through a weak supply chain, the entire public alerting system could be undermined.

The FCC has already acted on telecom supply chain risks in Docket 19-351 and on EAS cybersecurity in Docket 21-68. We recommend that the Commission extend those protections to the core elements of EAS, by requiring that EAS appliances be assembled, signed, and certified under U.S. or trusted jurisdiction oversight, with SBOMs and secure update practices. This is a modest step, but one that would ensure the nation's alerting backbone remains secure, resilient, and trusted.

Digital Alert Systems has developed several advanced features in the DASDEC and the HALO system that further strengthen EAS resilience, security, and utility. Our HALO system provides secure device management and monitoring, remote software and patch updating, and other functions. In the future, we look to automate HALO reporting into ETRS so that users can replace burdensome manual filings.

Cybersecurity is a foundational requirement for digital trust. From the manufacturer's perspective, EAS devices must be designed, certified, and maintained as trusted components of critical infrastructure. Government certification and standards conformance provide the necessary assurance that every encoder/decoder and CAP origination system deployed in the field can withstand adversarial threats. The Commission can strengthen this by updating Part 11 to include cyber requirements, mandating the use of certified devices, and assisting broadcasters in deploying secure, standards-compliant equipment.

By holding manufacturers and operators to a uniform cybersecurity baseline, the Commission can ensure that the public continues to trust the alerting systems on which national security and public safety depend.

## **12.6 Minimum Cyber Hygiene Checklist for EAS Participants and Devices**

To keep the nation's alerting systems secure against adversaries, all EAS encoder/decoders, EAS solutions, CAP origination systems should follow the baseline cybersecurity practices outlined here. These recommendations align with NIST Cybersecurity Framework (CSF), NIST SP 800-53/171 controls, and DHS CISA "Cross-Sector Cybersecurity Performance Goals (CPGs)" for critical infrastructure.

### 1. Device and Software Security

- **Authenticated Updates:** All firmware/software updates must be digitally signed by the manufacturer. Devices must reject unsigned or tampered updates.
- **Patch Management:** Manufacturers must provide timely security updates; EAS Participants must apply them within a reasonable window (e.g., 30 days for critical patches).
- **Secure Configurations:** No default passwords and require credential change at setup, both practices already enforced by the DASDEC. Disable unnecessary services and ports.
- **Role-Based Access Control (RBAC):** Devices must support unique user accounts with tiered permissions (e.g., admin vs. operator).
- **Logging and Monitoring:** Devices must generate tamper-proof audit logs of system access, configuration changes, and alert origination. Logs should be retained for at least 12 months.

### 2. Network and Infrastructure Security

- **Segmentation:** EAS devices must be isolated from business and corporate IT networks. Place devices behind firewalls or in DMZs with least-privilege access rules.
- **No Open Internet Exposure:** Direct exposure of EAS devices to the open internet is prohibited. Remote management must be done through secure VPNs or equivalent encrypted tunnels.
- **Encryption:** All CAP/IPAWS traffic must be encrypted and authenticated (TLS 1.2 or higher, FIPS-validated ciphers).

### 3. Vulnerability Management and Disclosure

- **Vulnerability Disclosure Policy (VDP):** Manufacturers must maintain a public process for researchers to report vulnerabilities.
- **Penetration Testing:** Devices should undergo third-party penetration testing and recertification at least every 24 months.
- **Incident Response:** EAS Participants must have an incident response plan aligned with NIST CSF “Respond” function and CISA CPG 2.0 guidance.’

### 4. Supply Chain Security

- **Secure Build Process:** Manufacturers must follow secure development lifecycle (SDL) practices, including controlled build environments and signed binaries.
- **Component Traceability:** Maintain documentation of hardware/software components and provenance.
- **Counterfeit Prevention:** Validate authenticity of hardware modules and integrated circuits.

### 5. Government Certification and Oversight

- **Certification Requirement:** Only FCC/FEMA-certified, NIST- and CISA-conformant devices should be eligible for deployment in the EAS.
- **Periodic Recertification:** Equipment should be re-certified for cybersecurity compliance every 24-36 months or following significant firmware changes.
- **Critical Infrastructure Alignment:** Broadcasters, cable operators, and other EAS Participants are already classified as critical infrastructure under DHS CISA guidance, with reporting obligations for major cyber incidents.

By codifying a uniform cyber hygiene checklist aligned with NIST and CISA standards, the Commission can ensure that every EAS Participant, large or small, operates equipment that is resilient to cyber threats. This approach not only reduces risk of compromise but also reinforces public trust that national, state, and local alerts are authentic, secure, and reliable even under adversarial conditions.

### **13 Modernizing the EAS for Greater Public Impact**

The Commission inquires how to modernize the Emergency Alert System (EAS) for greater public impact. It examines approaches to EAS design that could maximize the relevance of information to recipients; evaluates whether additional content types or modes—such as static graphics or video—should be supported to improve effectiveness; and considers how alerting systems can better serve communities by delivering messages in languages they understand. Building on prior multilingual efforts, it also explores whether further steps are warranted to ensure alerts effectively reach non-English-speaking populations and how multilingual capabilities should inform EAS architecture and show the *relevant* geography, even when broadcast is universal.

#### **13.1 Improving the EAS Textual Display**

Alerts are most effective when they (1) are *specific to the person and place at risk*, (2) contain a *plain-language protective action with a time box*, and (3) preserve *authenticity and accessibility* across languages and disabilities. Commission rules should require their consistent use and presentation.

We agree that originators should include the key elements of an alert in their messages. However, the EAS header sentence can be refined by adjusting the order of presentation. The Commission could encourage or require originators to use CAP templates that map to: *Hazard + Location + Time window + Protective action + Source*. NWS, FEMA, and the FCC already publish guidance and examples (including Spanish WEA and 360-character fields).

In our 2022 Comments, we proposed that alert messages (i.e. the “standards” EAS header text message) should be modified to make the more concise, readable and readily translatable.<sup>15</sup> This would generally fit the above suggestion by the Commission. As we noted then, while the FCC currently identifies what header elements should be used in an EAS header text message, it does not definitively prescribe how to construct the alert text output. As a result, there are minor variations across various EAS manufacturers’ implementations, and hence minor variation in what the public sees. Our suggestion then, which again fits the Commission's current discussion

---

<sup>15</sup> Digital Alert Systems, “Comments of Digital Alert Systems, Inc.” PS 15-94, filed March 10, 2022 at §6. (<https://www.fcc.gov/ecfs/search/search-filings/filing/10310606016624>).

of *Hazard + Location + Time window + Protective action + Source*, is a specific EAS message construct to deliver the most critical information clearly and upfront. Such an approach may make EAS visual messages more understandable and actionable, more quickly read, and potentially more consistent with the text approach of public warning messages delivered via WEA.

Taking both approaches together, a revised alert text format would be as outlined below for a CAP EAS message:

```
A [Hazard / EEE] for [Location / PSSCCC] was issued at [Time
window / JJHHMMM] until [End Time window / JJHHMMM+TTTT].
[Protective action / Description+Instruction from CAP text].
Message from [Source / ORG].
```

For a message received via EAS only, there would be general consistency:

```
A [Hazard / EEE] for [Location / PSSCCC] was issued at [Time
window / JJHHMMM] until [End Time window / JJHHMMM+TTTT].
Message from [Source / ORG].
```

In addition, this approach could foster greater consistency between EAS and WEA messaging/ Digital Alert Systems has also proposed other solutions to insert additional textual information and metadata into the EAS system, to further harmonize it with the CAP version of the message. For example, we have long presented a flexible approach to add ancillary data to the EAS message without modifying the EAS protocol itself. Textual information added via an ancillary data frame could include a message ID corresponding to a CAP message, potentially along with a short textual message to expand upon the brief standard EAS message created by the EAS encoder/decoder by utilizing header information.<sup>16</sup>

---

<sup>16</sup> See, Digital Alert Systems, “Comments of Digital Alert Systems, Inc. on the Notice of Inquiry,” PS 15-94, filed April 11, 2022 (<https://www.fcc.gov/ecfs/search/search-filings/filing/10411876725249>). Initial presentation of the concept can be found in Digital Alert Systems, “Notice of Ex Parte,” date posted October 26, 2007.

### **13.2 Harmonizing the Visual Presentation of EAS**

As the Commission considers modernization, one area deserving attention is the visual presentation of EAS alerts. Currently, EAS Participants use a variety of fonts, colors, layouts, and crawl behaviors, resulting in inconsistent experiences for viewers. This inconsistency risks confusing the public, diluting the impact of alerts, and reducing trust in the system. A harmonized approach—ensuring a recognizable and authoritative “look and feel”—would help establish EAS alerts as distinct and credible, separate from ordinary programming graphics or station branding.

The NVISA industry group has issued a voluntary specification that provides an important reference point for such harmonization. VIDS addresses the overall visual design and presentation framework of alerting content, including placement, contrast, readability, and layout.<sup>17</sup> Adoption of common visual standards across EAS participants would create consistency for audiences, whether receiving an alert via broadcast television, cable, or IPTV. Just as the EAS audio tones are instantly recognizable, a unified visual identity would improve comprehension, accessibility, and trust in the system.

Digital Alert Systems strongly supports continued exploration of harmonized visual standards, building on NVISA’s work and in collaboration with FEMA IPAWS, the FCC, industry stakeholders, and accessibility advocates. By ensuring a common design framework, the Commission can help reduce confusion, improve accessibility for vulnerable populations, and reinforce the authority of EAS messages across all platforms.

### **13.3 Enhancing EAS Displays with Symbology**

To maximize relevance, EAS modernization should include supplemental lightweight visuals, such as static graphics, such as the VIDS iconography, which add clarity.<sup>18</sup> Static VIDS graphics and symbology offer the greatest increase in relevance for the least additional expense. Video has a role but should only serve as a supplementary layer, and only where infrastructure can support it

---

<sup>17</sup> NextGen Video Information Systems Alliance, Visually Integrated Display Symbology (VIDS), WG-1 RECOMMENDED PRACTICES (NVISA-WG-1-001.01 REVISION 1.2) 1/12/2021 ([https://www.nvisa.org/files/ugd/0ddb93\\_d8a48ce7679442038238ecdd869852e7.pdf](https://www.nvisa.org/files/ugd/0ddb93_d8a48ce7679442038238ecdd869852e7.pdf)); also see Reply “Comments of Digital Alert Systems to the Notice of Inquiry”, PS Docket 15-94, filed May 10, 2022, at §8.

<sup>18</sup> Ibid. Also see NVISA, Visually Integrated Display Symbology (VIDS) Symbology Graphics Bundle, [https://www.nvisa.org/files/archives/0ddb93\\_a5a3a2100dac4c0aa9b44cae496e5d24.zip?dn=VIDS%20Graphics%20-%20R1.0%2011-19-2020.zip](https://www.nvisa.org/files/archives/0ddb93_a5a3a2100dac4c0aa9b44cae496e5d24.zip?dn=VIDS%20Graphics%20-%20R1.0%2011-19-2020.zip)

without compromising resiliency. Digital Alert Systems' experience demonstrates that these enhancements are technically feasible; DASDEC devices already aggregate media and support symbology. However, the Commission must balance public safety goals with the technical and economic impacts on broadcasters and cable operators.

It is important to understand that the use of standardized symbols can be displayed on modern radio screens, replacing album art with an appropriate graphic alert. Additionally, these graphic elements can be easily understood without requiring specific language knowledge – people can see a picture and quickly grasp its meaning. Therefore, the adoption of symbology on platforms that support any type of visual output should be included in Part 11 rules.

The Common Alerting Protocol natively supports essential alert elements: structured hazard metadata, precise areas (such as polygons, circles, FIPS codes), time frames, clear protective actions, multiple languages within a single alert, and links to additional resources like maps, images, and audio/video. The Commission has already taken the initial step by adopting a prioritized CAP approach to ingest, validate, and present the CAP version whenever available.

## **14 Are Traditional EAS Alert Delivery Channels Still Representative of Modern Media Consumption?**

The Commission requests feedback on whether the current services that transmit EAS alerts, radio and television broadcasting, cable service, wireline video services, and certain satellite services still reflect how the public consumes video and audio content today. We agree that this question is timely, considering the significant changes in consumer media habits.

### ***14.1 Traditional Platforms Retain an Important Role***

Despite well-documented declines in audience share, broadcast television, cable, and radio continue to serve as vital pathways for reaching a significant portion of the public.

- As of mid-2025, approximately 44% of households still subscribe to cable or satellite television services, and 20% of television viewing continues to occur via broadcast over-the-air channels.
- Radio also retains a strong footprint, with 68% of U.S. households having access to a radio receiver, and AM/FM stations continue to provide resilient local service, particularly during power outages or when broadband networks are impaired.

These figures remind us that, while diminished relative to historic highs, traditional EAS platforms still serve millions of Americans, including populations who may be less connected to streaming or broadband ecosystems (e.g., rural households, older demographics). Maintaining these channels as part of the nation’s alerting fabric remains essential to achieving universal coverage.

### ***14.2 The Shift Toward Streaming and Digital Platforms***

At the same time, the evidence is clear that media consumption has shifted away from traditional broadcast and cable and toward digital and streaming platforms.

- In June 2025, streaming accounted for 44.8% of all U.S. television viewing, surpassing both cable (24.1%) and broadcast television (20.1%) for the first time.
- By 2025, only 11% of households reported reliance on broadcast TV or cable alone, while nearly half (49%) identified as “streaming-only.”
- The shift is even starker among younger audiences: 41% of adults under the age of 30 report that they do not usually watch live TV.

- Audio consumption is following a similar trend, with daily listening increasingly dominated by digital streaming services, podcasts, and other platforms rather than traditional AM/FM radio.

This data suggests that if EAS remains bound only to its legacy distribution mechanisms, it risks failing to reach a growing portion of the population, particularly younger demographics, urban dwellers, and cord-cutting households.

### **14.3 Implications for EAS Objectives**

The statutory purpose of EAS is to provide widespread, timely notification to the public during emergencies. As consumer habits shift, there is a risk that reliance solely on legacy broadcast and cable channels will frustrate this objective, leaving unserved those who consume content primarily through:

- Streaming services (e.g., Netflix, Hulu, YouTube, Disney+).
- Smart devices (tablets without cellular service, wearable technology, smart speakers).
- Social and interactive platforms (social media, gaming consoles, live-streaming platforms).

The Commission has recognized this challenge: the public increasingly engages with media “that are not equipped to interrupt content to provide emergency messages,” thereby undermining the reach of today’s EAS.

It is therefore important to maintain balance in policy considerations:

- **Legacy platforms (broadcast, cable, radio) remain essential** for resilience, redundancy, and for reaching certain audiences who still depend on them.
- **New platforms must be integrated** into the alerting ecosystem if EAS is to remain representative of how Americans consume media today. In particular, the Commission should explore mechanisms for IPAWS CAP integration with streaming services, web browsers, smart speakers, and connected devices, ensuring authenticated, secure, and consistent delivery of alerts.

## **14.4 Conclusion**

Traditional EAS pathways remain necessary but no longer sufficient. The majority of younger and increasingly large portions of the general public consume media outside broadcast and cable environments. If the nation's alerting systems are to achieve their objective of widespread notification, it would make sense to incorporate the platforms where people now spend their time, even if those platforms perform a supplemental role. At the same time, ongoing support must be given to the broadcast and cable services that provide unmatched resiliency under conditions of network disruption.

Digital Alert Systems agrees with the Commission's assessment that the nation's alerting system must evolve as consumer media habits shift toward streaming, smart devices, and social platforms. At the same time, modernization efforts should build on the resilient, standards-based backbone that EAS and IPAWS-CAP provide today. Below are proposed policy directions that balance public safety objectives with the technical and operational realities faced by broadcasters, cable operators, and device manufacturers.

FEMA's Integrated Public Alert and Warning System (IPAWS) already distributes authenticated CAP messages that are digitally signed and profile-conformant. This should remain the authoritative "source of truth" for both legacy EAS and emerging platforms. *Streaming platforms, smart devices, and third-party aggregators* could leverage certified alert gateways (e.g., EAS appliances) at centralized locations to feed downstream consumer systems. Extending the same trust model to streaming services and smart device feeds can avoid creating parallel, fragmented alert feeds.

But while expanding alerts to new platforms, the Commission should reaffirm that broadcast radio and TV remain the resilient backbone, especially during power outages, broadband disruptions, or cyberattacks. The FCC must ensure that multi-path dissemination (CAP polling and daisy-chain relay) are not only maintained but also expanded through additional mechanisms, such as the statewide broadcast-data system in Ohio that today serves as a critical fail-safe layer.

Modernization should not mean replacing EAS; it should mean expanding its reach. By building on IPAWS-CAP, piloting streaming and smart device integration, standardizing graphics, symbology, and media, ensuring multilingual delivery, and supporting certification and funding, the Commission can extend emergency alerts to where the public is *today* without undermining the resilient infrastructure that has served the nation for decades. Digital Alert Systems stands ready to support this evolution.

## **15 Effectiveness of EAS in the Context of Changing Media Habits**

EAS remains an effective tool because significant segments of the public still rely on broadcast television, cable, satellite, and radio. As noted, these platforms continue to serve millions of daily users, especially older Americans, rural communities, and households with limited broadband access. Additionally, broadcast radio and TV offer unmatched resilience during power and broadband outages, making them vital in national emergencies.

At the same time, EAS alone no longer ensures universal reach. With nearly half of U.S. households now “streaming-only,” and 41% of adults under 30 reporting they do not usually watch live TV, relying solely on EAS delivery channels risks missing younger and digitally native populations. Therefore, EAS remains necessary but not sufficient by itself to meet national alerting goals.

### **15.1 What can the Commission do under its current legal authority?**

The Commission’s authority centers on broadcast, cable, satellite, and CMS providers. Within that scope, several practical steps can help EAS “follow the public’s eyes and ears”:

- **Encourage voluntary adoption by new platforms:** The Commission could establish a framework for voluntary participation by streaming and smart device platforms (e.g., apps, browsers, smart speakers) in IPAWS/EAS alerting. Even in the absence of statutory authority to mandate, the FCC can convene industry groups, set interoperability standards, and recognize voluntary adopters.
- **Expand accessibility and multilingual support:** Codify CAP <info> blocks (multiple languages) requirements to ensure alerts are understandable to diverse communities.
- **Encourage symbology and graphics:** Promote adoption of standardized alert symbology (e.g. VIDS) and lightweight CAP-linked graphics to make alerts more straightforward, even if video is not feasible.
- **Encourage new services to adopt certified alert approaches:** As next-generation broadcast and communication technologies expand, enhanced alert tools for richer, targeted notifications (with maps, multilingual text, and accessibility overlays) should be delivered through trusted FCC-certified IPAWS-conformant emergency alert gateways.
- **Certification and cybersecurity:** Expand equipment certification to include cybersecurity compliance (aligned with NIST/CISA CPGs), multilingual parsing,

and CAP resource handling. This ensures that any new pathways introduced maintain public trust.

### **15.2 Minimum requirements to preserve trust in expanded systems**

For any alerting pathway, whether legacy EAS or new digital platforms, the minimum requirements should include:

1. **Authentication and authorization:** All alerts must originate from validated government authorities through IPAWS (digital signatures).
2. **Consistency across channels:** The same CAP message should drive both EAS and WEA alerts, ensuring accuracy and uniformity.
3. **Multilingual and accessible presentation:** Alerts must be understandable across languages, and support text, audio, and visual modalities.
4. **Cybersecurity compliance:** Devices and platforms carrying alerts must comply with baseline NIST/CISA cyber hygiene standards.
5. **Auditability and accountability:** Logs, reporting, and oversight must ensure originators and distributors are accountable for accuracy and timeliness.

### **15.3 Conclusion**

EAS remains effective within its historic footprint but is increasingly limited as Americans migrate to new platforms. The Commission should pursue a dual approach:

- **Sustain and modernize EAS** (through CAP-first implementation, multilingual delivery, graphics/symbology, next gen technology pilots, and equipment certification).
- **In parallel, extend IPAWS-CAP alert delivery to emerging platforms** (streaming, smart devices, social media) through voluntary partnerships, standards-setting, and recognition programs.

This balanced approach recognizes the ongoing importance of EAS in resilience and national security, while also making sure emergency alerts continue to “follow the eyes and ears” of the American public. EAS modernization keeps the legacy system resilient, multilingual, accessible, and cyber-secure. Extending to new platforms ensures alerts “follow the public’s eyes and ears” into streaming services, smart devices, and interactive platforms where younger and digitally native audiences are increasingly present. Together, these parallel efforts maintain the resilience and authority of EAS while also adapting to the realities of modern media consumption.

## 16 Evaluating End-User Device–Centric Alerting in the Nation’s Alert and Warning Systems

The Commission seeks comment on whether the nation’s alert and warning systems would be more effective if their design placed greater emphasis on the capabilities of end-user devices that receive and present alerts, rather than focusing primarily on the communications pathways that transmit them. Specifically, the Commission asks whether EAS would be more effective if consumer “smart” devices connected to the internet, such as televisions, radios, or other video displays, could directly receive EAS messages regardless of the user’s chosen programming at the time an alert is issued.

This is an important and timely inquiry. Emerging device ecosystems hold the potential for more personalized, accessible, and engaging emergency messaging. However, an end-user device-centric approach raises significant concerns regarding **security, reliability, and interoperability**, and it must be evaluated in the context of EAS’s original goal: to provide a secure, redundant, and survivable alerting backbone.

End-user devices like smart TVs, streaming platforms, and connected speakers present clear opportunities. They can customize presentation of alerts based on user language and accessibility preferences, display standardized hazard symbols or maps, and match modern media habits, thereby enhancing relevance and understanding.

However, a device-centric architecture also introduces material risks. Consumer electronics are very diverse, often lack security support over time, and rely on broadband and local power sources. Extending alert authentication and processing across millions of endpoints would increase the attack surface and could lead to inconsistent, confusing user experiences. In short, EAS remains vital as the foundation for survivability and trust. Expanding alerts to new platforms should happen simultaneously and under strong governance to ensure that modernization improves, rather than undermines, the resilience of the nation’s alerting system.

### **16.1 Risks and Constraints of End User Device-Centric Design**

While end-user devices are positioned to add value to public alerting, the idea of placing the burden of alert ingestion and authentication primarily on consumer devices creates significant challenges:

- **Security.** The attack surface expands dramatically when millions of heterogeneous, internet-connected devices become alert endpoints. Key management (e.g., distributing and updating trust anchors), patching vulnerabilities, and revoking compromised devices at scale become far more difficult. Consumer devices frequently run outdated software and may never receive security updates, making them ill-suited to be the authoritative edge of the nation's alerting system.
- **Reliability.** Most consumer devices rely on broadband connectivity and local power. By contrast, traditional EAS functions even during broadband disruptions, with broadcast facilities operating on backup power. Smart devices typically lack store-and-forward capability or the ability to ingest over-the-air fallback signals (FSK/SAME from AM/FM or NOAA Weather Radio).
- **Interoperability.** Without strong governance, device manufacturers will implement alert rendering inconsistently. Some devices may interrupt programming; others may only show a badge or banner. This heterogeneity risks confusing the public and undermining trust. Consistent user experience has long been recognized as a requirement for effective public alerting.

In short, moving core authentication and processing to consumer endpoints risks weakening the trust boundary that exists through IPAWS, digitally signed CAP messages, and FCC/FEMA-certified EAS equipment.

### **16.2 The Continuing Key Role of EAS**

A more resilient design recognizes that certified EAS devices must remain at the core of the architecture. These devices perform several functions that consumer endpoints cannot reliably replicate:

- **Multi-path ingestion.** Certified EAS equipment can receive alerts via CAP/IPAWS over IP, FSK/SAME over AM/FM, and NOAA Weather Radio, as well as emerging broadcast-data feeds. This diversity ensures alerts can still be processed when one pathway is impaired.

- **Authentication and policy enforcement.** EAS devices validate digital signatures, apply CAP-first rules (as required by Part 11), deduplicate multiple inputs, and log events for audit and accountability.
- **Resilience.** When broadband connectivity fails, certified devices continue to receive data via over-the-air relay, ensuring ongoing operations and alert availability for broadcast and cable distribution.

For these reasons, the FCC-certified, IPAWS conformant EAS device must remain the central processor, router, and security appliance in the nation’s alerting ecosystem, regardless of whether alerts are also extended to new endpoints.

### ***16.3 A Balanced Path Forward***

The most effective approach is a layered architecture where certified EAS devices serve as the trust anchor, and end-user devices function as an optional presentation layer.

- **Gateway-plus-endpoints.** Rather than pulling alerts directly from the internet, consumer devices should render alerts through a secure, authenticated feed from a certified EAS device and trusted distribution service. This preserves the integrity of authentication while allowing smart TVs, streaming devices, and others to display alerts in a standardized way.
- **Standardized presentation profile.** Collaborating with FEMA and industry, the Commission could create a certifiable “Alert Presentation Profile” for end-user devices, and for rendered alerts in program streams.
- **Cybersecurity baselines.** Any device or platform that renders official alerts should meet minimum cyber hygiene standards: secure update channels, vulnerability disclosure programs, SBOM availability, and fail-safe behavior in the event of authentication failures.

While consumer devices provide new opportunities for customization, accessibility, and alignment with contemporary media habits, they cannot replace the reliability and trust of the existing EAS backbone. End-user alerting should be viewed as a potential supplementary layer built on the secure, multi-path ingestion and processing carried out by certified EAS equipment.

A balanced approach therefore maintains traditional EAS as the essential fallback, while extending alert rendering to smart and streaming devices through standards-based, secure, and

certifiable mechanisms. In this way, the nation's alerting system can serve the "eyes and ears" of the public while preserving the resilience, security, and public trust on which its effectiveness ultimately depends.

## 17 Does EAS Meet the Needs and Expectations of the Public and Alerting Authorities?

The Commission seeks feedback on whether the Emergency Alert System (EAS) continues to meet the needs and expectations of both the public and alerting authorities. From the perspective of Digital Alert Systems (DAS), the answer is *yes*: EAS remains highly useful and relevant. At the same time, there are areas where its utility is diminished, particularly considering shifting media consumption habits and technical limitations that affect precision and clarity.

### 17.1 Where EAS Remains Useful and Effective

Despite changes in media consumption, tens of millions of Americans continue to watch broadcast and cable television every day. As of mid-2025, 44% of U.S. households still subscribe to cable or satellite services, and broadcast television accounts for approximately 20% of all television viewing.<sup>19</sup> Importantly, these audiences are not evenly distributed. Broadcast and cable consumption remain higher among rural households and lower-income demographics, which may lack access to broadband or streaming platforms. This demographic distribution underscores the ongoing equalizing role of EAS, ensuring alerts reach households who may otherwise be underserved.

- **Proven Resilience During Disruptions.** Unlike mobile broadband or streaming services, broadcast radio and television can keep operating during prolonged power outages and network disruptions by using backup generators and transmitters. This was demonstrated during recent hurricanes and wildfires when cellular networks failed, but local broadcasters continued providing live updates and emergency alerts. The original design of EAS, to work when other communication systems are down, remains a vital national safety asset.
- **Unique National-Level Alerting Role.** EAS remains the only system mandated to carry Presidential alerts during a national emergency. This distinctive statutory role guarantees that the President or FEMA can reach the entire country, even if commercial mobile services or IP-based systems are impaired. There is no other real-time response method available.

---

<sup>19</sup> Reuters, June 17, 2025; Pew Research Center, July 1, 2025

- **Trust and Familiarity.** Decades of use have made the EAS tones, crawls, and banners instantly recognizable to the public. While not perfect, this consistency builds trust that an EAS interruption indicates an urgent situation requiring attention.

Overall, the evidence indicates that EAS offers significant value, and even though it cannot on its own meet all desired alerting requirements, EAS does remain the most resilient, reliable, and survivable form of public warning in a true gray-sky situation.

- **Strengths:** EAS remains indispensable as a reliable, universally recognized, and equitable alerting system, especially for rural, lower-income, and older populations, as well as during large-scale emergencies that disrupt IP-based services. Its role in national-level alerting continues to be unmatched.
- **Weaknesses:** EAS is less effective for precise alert targeting, accessibility, multilingual communication, and reaching younger or streaming-only populations. Expanded adoption and integration with CAP features, next gen broadcast capabilities, and supplemental platforms (streaming, smart devices) is necessary in these areas.

## **17.2 Recommendations**

From our perspective, EAS remains useful and necessary for alerting authorities and the public. It has repeatedly proven its worth in crises and serves demographics otherwise underserved by modern, IP-based alerting systems. However, EAS also faces limitations that must be acknowledged and addressed.

The way forward is not to replace EAS, but to modernize and supplement it. EAS can be improved by enhancing message delivery accuracy, supporting multiple languages, and adding graphics for both TV and HD radio. By expanding IPAWS alerts to new platforms alongside traditional media, we can ensure that the nation's alerting systems reflect current media consumption habits.

As a leading provider of EAS encoder/decoder and CAP origination systems, Digital Alert Systems (DAS) strongly supports the Commission's efforts to assess whether EAS continues to meet the expectations of the public and alerting authorities. Based on our experience, EAS remains indispensable. At the same time, modernization is necessary to ensure that alerts stay effective amid changing consumer media habits. Below, we outline recommendations that both reinforce EAS as the nation's resilient backbone and expand its relevance into new markets and delivery pathways.

## 1. Reinforce and Modernize the Core EAS Role

- **Maintain EAS as the backbone:** The resilience of broadcast and cable-based EAS must not be diminished. The Commission should reaffirm the essential role of broadcast, cable, and radio as fallback alerting mechanisms during IP outages and disasters.
- **Standardize symbology and graphics:** The Commission should establish rules for using standardized hazard symbols (e.g., the VIDS specification) and lightweight CAP-linked graphics. Digital Alert Systems has already shown and implemented symbology integrations with companies like ChyTV for TV systems and Nautel for HD Radio, illustrating a practical path forward.<sup>20</sup>
- **Certification and security:** Digital Alert Systems supports the concept of an enhanced FCC/FEMA certification framework, including cybersecurity compliance, CAP media handling, and accessibility features. This ensures that EAS equipment is trusted infrastructure aligned with NIST and CISA guidelines for critical systems.

## 2. Extend EAS/CAP Capabilities into New Platforms

- **Gateway to new media ecosystems:** EAS equipment should serve not only broadcasters and cable operators, but also as a secure gateway for emerging platforms (streaming providers, smart TVs, gaming consoles, smart speakers). In this role, DASDEC-class systems can ingest authenticated IPAWS CAP feeds and distribute them to local apps and devices in standardized formats.
- **IoT, vehicles, and signage:** As machine-to-machine (M2M) alerting expands, solutions such as those provided by Digital Alert Systems can act as a secure gateway and local policy enforcement and authentication node, bridging national IPAWS alerts to local endpoints like connected cars, road signage, or industrial safety systems.
- **Enterprise and institutional markets:** Schools, hospitals, utilities, and other critical facilities can leverage CAP/EAS infrastructure for site-wide safety communications. Digital Alert Systems devices can securely ingest IPAWS CAP and redistribute it into IP-based paging, signage, or alerting systems.

---

<sup>20</sup> DigIt Signage Technologies, “ChyTV EAS VIDS Demonstration,” (<https://www.youtube.com/watch?v=rlyXLn5WxK4>); and “Digital Alert Systems' New VIDS, DASDEC Gear on the Way,” TV Technology, March 18, 2020 (<https://www.tvtechnology.com/equipment/digital-alert-systems-new-vids-dasdec-gear-coming-to-2020-nab-show>)

### 3. Address Consumer Experience Without Undermining Universality

- **Balance customization with consistency:** Consumers should be able to adjust presentation features (language, text size, contrast, haptic alerts), but not disable or suppress imminent threat or national alerts. Digital Alert Systems equipment ensures consistent ingestion and processing rules while allowing downstream platforms to personalize presentation in user-appropriate ways.
- **Clarity in presentation:** The Commission should encourage adoption of structured alert presentation rules (“Hazard + Location + Protective Action + Expiration”) across all platforms. Digital Alert Systems’ products already preserve CAP field fidelity and make this information available downstream. We have previously made recommendations on refining the standard EAS message in this area.

### 4. Encourage Funding and Support for Broadcaster Upgrades

- **Small-market burden:** Many small broadcasters and cable operators operate on thin margins, making equipment upgrades challenging. Digital Alert Systems recommends that the Commission coordinate with FEMA/NTIA to provide targeted funding or grant programs to support required equipment modernization.
- **Leverage modularity:** DASDEC systems are designed to be modular, enabling broadcasters to add features such as graphics, symbology, security upgrades, and a large array of interfaces through software updates instead of replacing entire hardware units. This offers a more efficient and cost-effective way to achieve compliance and foster innovation.

### ***17.3 Conclusion: Preserve EAS While Enabling Evolution***

From DAS’s perspective, the nation’s alerting architecture must remain layered and resilient. EAS, distributed through broadcasters, cable operators, and satellite, continues to be the foundation. But EAS equipment should also develop into a secure intermediary for new platforms, delivering the same authenticated, trusted, and redundant alert content to streaming, IoT, enterprise, and institutional ecosystems.

By reinforcing trust in EAS and extending its reach through modern interfaces, the Commission can ensure that emergency alerts preserve their resilience and follow the public’s “eyes and ears” into the platforms they use most today.

EAS does not require a complete redesign. It needs targeted, standards-based modifications that (a) strengthen security, (b) improve dissemination resilience (multi-path ingestion, including broadcast-data pathways), (c) boost media clarity through CAP-linked visuals and standardized symbols, and (d) broaden interoperability so authenticated alerts can appear in new media environments—both paid and free advertising-supported television (FAST) streaming services—without compromising the broadcast infrastructure.

The existing CAP/IPAWS trust model works and is mandated (CAP-first). Part 11 already requires “triggered CAP polling” after a legacy header, ensuring authenticated, richer CAP content when available. What’s needed is consistent implementation and certification, not a new architecture.

- **Maintain EAS as the resilient backbone.** No new path should reduce the primacy of authenticated CAP or the survivability of broadcast EAS dissemination.
- **Gateway-centric trust:** Treat certified EAS devices as security gateways that ingest via multiple paths (CAP/IP, OTA relay, broadcast-data), verify signatures, apply policy, and expose a signed, minimal feed to downstream apps/players, rather than pushing auth/processing to every consumer endpoint. From a security perspective, this builds on IPAWS CAP signatures and concentrates authentication in certified EAS device gateways, and layers NIST/CISA-aligned hygiene to reduce compromise risk.
- **Performance-based, tech-neutral rules:** Specify outcomes (timeliness, multilingual parity, accessibility, lifecycle handling) without prescribing a single transport beyond CAP/IPAWS and Part 11.

## 18 Testing, Training, and Collaboration on Public Warning

EAS continues to meet essential public safety needs, but training, education, and collaboration vary across jurisdictions. The Commission—in partnership with its sister agencies—can significantly improve outcomes by: (1) standardizing and expanding alert-originator training linked to IPAWS/CAP best practices; (2) funding and coordinating public education so people understand what alerts mean and how to respond; (3) formalizing cooperation among FEMA, FCC, SECCs, manufacturers, broadcasters/MVPDs, and CMS Providers; and (4) establishing a consistent schedule of regional and national tests, with transparent metrics, to address ongoing performance issues gaps.

- **Originator practices vary widely.** Authorization alone does not guarantee message quality. Many originators infrequently receive training on CAP structure (polygons, <info> blocks, updates/cancels), multilingual content, or how to coordinate EAS and WEA. FEMA coursework exists, but participation, currency, and hands-on practice are inconsistent, especially for small jurisdictions. The Commission could encourage monthly originator exercises in the IPAWS TSSF (or vendor testbeds) to rehearse template use, geotargeting, and update/cancel timing without causing on-air disruption.
- **Limited public education.** Many people do not understand how alerts are delivered, what different tones or codes mean, or what actions to take (such as the difference between a test and a real event). National tests highlight this knowledge gap.
- **Irregular exercises below the national level.** While national tests occur, regional and scenario-based drills are not consistently conducted or measured, despite FEMA encouraging regular lab and field testing.
- **Fragmented best-practice adoption.** CSRIC and FCC resources exist but are not consistently implemented in local SOPs, such as message templates, multilingual workflows, and alert lifecycle management. Efforts should be made to assist state and regional alerting coalitions (originators, broadcasters/MVPDs, CMS providers, equipment vendors) in sharing after-action data and coordinating training and test schedules.

Consistent, realistic exercises with shared metrics and after-action review, are the quickest way to align originator practices, distribution performance, and public understanding. FEMA's

coursework and IPAWS Lab provide the necessary framework. The Commission’s role should be to establish a regular rhythm, transparency, and accountability for that work so that training and testing become routine.

Digital Alert Systems supports a training-first, test-often posture. With the Commission’s leadership on cadence and metrics, and FEMA’s continued investment in training and lab capacity, the alerting community can close the remaining gaps and ensure EAS and related systems achieve their life- and property-saving objectives.

### ***18.1 Recommendations on National / Regional EAS Testing***

Ensuring the reliability and resilience of the Emergency Alert System (EAS) requires a structured approach to testing that balances technical rigor, operator readiness, and public perception. The following recommendations outline a framework for increasing the frequency and effectiveness of both national and regional EAS tests.

The Commission should establish a predictable cadence of at least one National Periodic Test (NPT) per year, with the option of additional regional variations coordinated through State Emergency Communications Committees (SECCs). Importantly, NPTs should be distinguished from National Emergency Messages (EANs). While the EAN must remain reserved for true national emergencies, the NPT should serve as the system’s primary training and readiness tool. By framing NPTs as routine drills—both operationally and in public communication—the system can maintain preparedness without generating undue alarm.

#### **Regularizing and Enhancing NPT Testing**

At present, EAS Participants must complete three separate filings in the EAS Test Reporting System (ETRS): Form One (pre-test configuration), Form Two (day-of participation), and then Form Three (detailed post-test report).

This process is duplicative and unnecessarily burdensome. A more efficient framework would consolidate reporting into two steps:

- 1) **Pre-test configuration (Form One):** Filed once annually rather than before every test.
- 2) **Post-test summary (combined Form Two/Three):** A single report filed within a defined period (e.g., 7 days) after the test, with automated population of configuration data from Form One.

This streamlined process would preserve accountability and data quality while reducing participant frustration.

While tests should be less disruptive to the public, they must continue to serve as a full technical exercise for EAS Participants. Consistent test schedules would also allow equipment vendors to provide timely support, updates, and diagnostics to participants.

In addition to national testing, regional tests provide valuable opportunities for state and local emergency management agencies to practice message origination and for broadcasters and cable operators to validate reception paths. They also enable public outreach in a less disruptive format, particularly if aligned with hazard-prone seasons such as hurricane preparedness campaigns.

From Digital Alert Systems' perspective, more consistent and well-structured testing is vital for ensuring resilience, improving operator readiness, and building public trust in the EAS. However, the intrusive nature and administrative burdens of current national tests may deter participation and cause confusion among the public.

The Commission can strike a balance by:

- Mandating at least one national NPT annually, reserving the EAN for true emergencies.
- Streamlining ETRS reporting from three forms to two.
- Supporting regional NPTs as intermediate, lower-impact exercises.

This framework ensures that EAS Participants remain well-trained, the public is informed rather than alarmed, and the system continues to fulfill its life- and property-saving mission effectively and efficiently.

### ***18.2 An Additional Concept for National Readiness Testing***

The Commission seeks comment on how to expand testing of the Emergency Alert System (EAS) at the national and regional levels. Digital Alert Systems supports increasing the cadence of testing but also recognizes that frequent use of the National Emergency Message (EAN) or even the National Periodic Test (NPT) codes can create unnecessary public disruption and administrative burden.

To address this, we recommend that the Commission, in coordination with FEMA, consider adopting a new "silent" national or regional test event code. This code would be designed to exercise the entire alert distribution chain from IPAWS to EAS participants but would not be transmitted by the receiving systems. Instead, EAS devices would decode, process, and log the alert locally, similar to the current Required Weekly Test (RWT). This approach would allow FEMA to validate national-level alerting pathways without causing confusion or alarm among the

public, while maintaining the effectiveness of annual public-facing NPTs for end-to-end validation.

To be blunt, the current testing process for the national EAS, whether using the NPT or EAS code, involves too much preparation, extensive reporting burdens, public disturbance, and advance notification of EAS Participants (the latter of which likely skews the results).

Additionally, the Commission should modernize how such tests are reported. Currently, EAS Participants are required to submit three separate reports in the Electronic Test Reporting System (ETRS) for each NPT. This process has proven burdensome, particularly for smaller broadcasters and cable operators. A more efficient approach would be to combine these reports into a single, automated submission. Specifically, EAS devices should be able to automatically log the receipt of the silent test code and send a straightforward status report to FEMA or FCC systems through a secure, authenticated channel. This report would only confirm technical receipt, without including any personally identifiable information or remote access capabilities, thereby maintaining security and privacy.

This combination of a silent national test code and automated reporting would significantly reduce the administrative and operational burdens on EAS Participants while providing FEMA and the FCC with continuous insight into system health. Importantly, this model would also strengthen the role of certified EAS devices as the secure, monitored gateways of the nation's alerting architecture, ensuring resiliency without imposing unnecessary disruption on the public.

47 C.F.R. Part 11 (Emergency Alert System) could be amended as follows to incorporate what we suggest for the sake of discussion as a Silent National Test (SNT) code:

1. Addition of a Silent National Test Event Code

- Amend § 11.31(e) (EAS protocol) to include a new event code, "SNT" (Silent National Test), defined as follows:
  - "The SNT event code is used by FEMA or other authorized national authorities to conduct silent national or regional EAS tests. EAS Participants must configure their equipment to receive, log, and report receipt of SNT messages. EAS Participants must not transmit SNT messages to the public."

## 2. Silent Test Logging and Reporting

- Amend § 11.61 (Tests of EAS procedures) to include:
  - “In addition to existing weekly and monthly test requirements, EAS Participants shall receive and log all Silent National Test (SNT) messages. Such logs must be maintained consistent with § 11.35 and made available to the Commission upon request. EAS Participants may satisfy reporting requirements for SNT messages through automatic device reporting, where such functionality is provided by certified equipment.”

## 3. Streamlined Reporting via ETRS

- Amend § 11.61(a)(3) to add:
  - “The Commission shall provide for automated reporting of receipt of Silent National Test (SNT) messages via the Electronic Test Reporting System (ETRS). EAS Participants equipped with devices capable of secure automated reporting may rely on such reporting in lieu of manual filings. The Commission may aggregate such reports for the purpose of system readiness assessments.”

This approach would allow authorities to more frequently conduct simulated national system testing, without unnecessary disruption. It would provide FEMA and the FCC with better visibility into actual EAS readiness. This approach would also reduce administrative burdens on EAS Participants.

## 19 Conclusion

The Commission’s objective should be to strengthen, update, and expand EAS, not to reinvent it. The certified EAS/CAP device is the cornerstone of this system, acting as the secure, resilient, and policy-compliant gateway that ensures alerts are delivered reliably, intelligibly, and across multiple platforms.

By strengthening appliance security baselines, codifying multipath ingest protocols, expanding symbology and accessibility options, setting gateway-to-app standards, and standardizing silent testing with automated reports, the Commission can improve the effectiveness of EAS while easing the burden on EAS Participants. These measures would maintain the proven strengths of broadcast alerting while allowing secure integration with the platforms where the public increasingly consumes information. The outcome is a layered, gateway-focused architecture that keeps the nation’s alerting systems resilient, trusted, and effective, now and in the future.

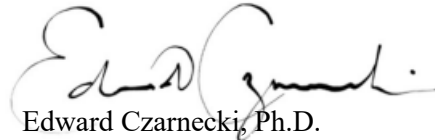
The Emergency Alert System has served the nation well for decades, and it continues to provide indispensable utility as a resilient, last-line safeguard for public warning—even under the most challenging conditions. As the Commission explores modernization, we commend the goal of expanding EAS to meet the needs of today’s diverse and technologically sophisticated audiences. Enhancements such as symbology, improved targeting, accessibility, and multilingual alerting can greatly increase effectiveness and public trust.

At the same time, modernization must be pursued with clear-eyed recognition of the system’s foundation as an unfunded mandate. Broadcasters and cable operators bear the full cost of regulatory compliance, and manufacturers carry significant burdens in advancing innovation within a compliance-driven market. To ask both groups to shoulder the added weight of “guaranteed delivery,” video-based alerting, or other resource-intensive capabilities without federal support creates a paradox that risks slowing adoption, deepening inequities, and weakening the very system modernization is intended to strengthen.

Digital Alert Systems hopes the Commission will align its regulatory vision with practical funding and implementation mechanisms. By fostering collaboration among FEMA, the FCC, industry stakeholders, and public safety agencies, and by ensuring resources are available to both participants and manufacturers, the Commission can chart a path toward a modernized EAS that is effective, equitable, and sustainable.

We stand ready to work with the Commission and our partners to ensure that EAS continues to evolve as a vital component of the nation's integrated public alert and warning system, safeguarding all Americans in times of crisis.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Edward Czarnecki". The signature is fluid and cursive, with a large initial "E" and "C".

Edward Czarnecki, Ph.D.  
Vice President, Government and  
International  
*Digital Alert Systems, Inc.*

25 September 2025