**BY ELECTRONIC FILING**

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

**Re: Comments of Digital Alert Systems, Inc. on Proposed EAS Software Rules**

Dear Ms. Dortch:

Digital Alert Systems, Inc. ("DAS") submits the enclosed comments in response the above referenced proceeding, regarding the Commission's inquiry regarding "EAS software."

DAS is submitting two coordinated filings in response to the FNPRM. This filing addresses the proposal to authorize and certify software-based EAS. DAS's companion filing separately addresses measures to improve the security, precision, interoperability, and public usefulness of CAP and legacy EAS alerting.

DAS supports responsible EAS modernization but is concerned that the proposed model could lead to EAS implementations that are insufficiently defined, certifiable, inspectable, secure, or accountable under Part 11. The Commission should defer authorization of EAS software unless and until it establishes a rule framework that treats software as one component of a complete certified EAS system configuration; includes the host environment within the certification boundary; requires disclosure and control of material external dependencies; and preserves a clear line between EAS compliance functions and downstream signal-chain functions.

If the Commission proceeds now, any authorization should be narrow and technology-neutral. Software-based EAS should operate only within an identified, certified system configuration, with the host environment and material dependencies included within the certification boundary. Software, appliance, and hybrid implementations should be subject to equivalent obligations for cybersecurity, reliability, lifecycle, support, inspection, and recovery.

The rules should also require disclosure of proprietary or license-restricted dependencies necessary for the certified configuration, and should make clear that downstream automation, routing, processing, playout, transport, multiplexing, and signal-insertion systems do not become EAS-compliant equipment merely because they carry, route, switch, or insert alert content.

Respectfully submitted,

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

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

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

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

**COMMENTS OF DIGITAL ALERT SYSTEMS, INC.**

**ON THE FURTHER NOTICE OF PROPOSED RULEMAKING**
**PART II: AUTHORIZATION AND CERTIFICATION OF SOFTWARE-BASED EAS**

Contents

# 1 Introduction

Digital Alert Systems, Inc. ("DAS") supports responsible modernization of the Emergency Alert System ("EAS"), including continued examination of software-based implementations. The question before the Commission is not whether software can perform EAS functions. Modern certified EAS equipment already relies extensively on software. The question is whether the Commission can authorize a new implementation model without weakening the reliability, cybersecurity, operational independence, certifiability, accountability, and continuity of operation required of national public-warning infrastructure.

DAS does not contend that the Commission must defer consideration of software-based EAS because the record lacks a complete technical specification for every possible deployment. The Commission may address the policy and technical issues raised by its proposal in this proceeding, while recognizing that the process itself may identify unresolved questions of reliability, cybersecurity, certification, interoperability, or operational performance that warrant additional research, laboratory evaluation, or controlled field trials before final rules are adopted.

DAS's concern is narrower and more fundamental. We observe that the FNPRM's proposed authorization does not yet establish the regulatory object, certification boundary, conditions of authorization, conformity requirements, and accountability relationships necessary to make software-based EAS administrable under Part 11.[1] These matters cannot be left to an application developer, host-platform provider, integration vendor, or EAS Participant to resolve independently after the Commission authorizes the category. The public-safety question is whether the final rules require a software-based EAS implementation to preserve reliability, operational independence, cybersecurity, certifiability, accountability, and continued operation under emergency and degraded conditions. The Commission should not infer that result merely because software can perform individual EAS functions.

DAS's position is informed by direct experience with software-based EAS architecture. Since 2016, DAS has developed and fielded DAS Collector™, a software-based DASDEC implementation designed for defined, supported platform environments. That experience has provided DAS practical grounding in the additional engineering, integration, cybersecurity, lifecycle, support, and recovery responsibilities that arise when EAS functions move beyond a bounded appliance and into a host computing environment.

DAS therefore does not contend that software cannot perform basic EAS functions. Conversely, we do not contend that a software-based solution can perform EAS functions better than a dedicated device-based solution. Rather, DAS's experience demonstrates why software EAS cannot be treated as a simplification in which certification applies only to application code. The host platform, operating system, virtualization environment, interfaces, dependencies, configuration controls, update path, security posture, and responsible support parties can each materially determine whether required EAS functions remain available and compliant. Those elements must be addressed as part of the complete certified EAS Implementation.

---

[1] See Modernization of the Nation's Alerting Systems; Protecting the Nation's Communications Systems from Cybersecurity Threats; Wireless Emergency Alerts; Amendment of Part 11 of the Commission's Rules Regarding the Emergency Alert System, Report and Order and Further Notice of Proposed Rulemaking, FCC 26-38, ¶¶ 96, 104–09 (2026) ("FNPRM")

DAS therefore urges the Commission to use this proceeding to determine whether it can establish an enforceable technical and operational framework for authorizing defined, certifiable EAS Implementations consistent with applicable Federal requirements and guidelines. The final rules must establish the regulated implementation, the material elements of its certification boundary, the conditions for field conformity, the treatment of material changes, and responsibility for continued compliance. If the Commission concludes that it cannot responsibly establish those requirements based on the proposals before it, it should not adopt a general authorization at this time. It may instead seek additional technical input through a focused further notice, workshop, laboratory evaluation, controlled field trial, waiver process, or public notice seeking detailed certification proposals.

We wish to re-emphasize the following themes from our comments filed on September 25, 2025:

- certified EAS Implementations must remain the system trust anchor;
- software must preserve independent monitoring and fallback operation;
- the full cybersecurity baseline applies to the software and its host environment;
- supply-chain controls must cover hardware, software, development, signing, updates, and ownership; and
- manufacturer sustainability is part of the public-safety ecosystem, not merely a private commercial concern.

These matters are not peripheral implementation details. They determine whether a proposed software-based configuration can function as an identifiable, certifiable, inspectable, and accountable EAS system. An implementation whose host environment, dependencies, configuration state, failure behavior, update path, and responsible party cannot be defined and verified is not merely an imperfect EAS implementation; it is not a sufficiently bounded system for Part 11 certification. The burden should rest on the applicant for a particular EAS software implementation to demonstrate conformity with the Commission's adopted requirements and to show that the defined configuration provides assurance equivalent to or greater than that required of other certified EAS Implementations.

## 2 EAS Is Public-Safety Infrastructure, Not Merely Another Broadcast Application

The Commission's discussion of software-based EAS approaches the issue principally from the perspective of modern broadcast architecture. The FNPRM observes that stand-alone EAS equipment may reside outside the "core processing systems" used by broadcast, cable, and satellite services and asks whether software implementation could more closely integrate EAS into increasingly IP-centric signal chains. Those are legitimate operational considerations, but they do not fully describe the regulatory function performed by EAS.

EAS equipment is not simply another component used to produce or distribute commercial programming. It performs a federally mandated public-warning function.[2] An EAS Implementation receives and evaluates emergency information, monitors designated sources, determines whether alerts satisfy applicable criteria, originates certain alerts, controls retransmission, and provides the mechanism through which emergency information interrupts normal programming. A compromise or failure can therefore affect the authenticity, availability, and delivery of warnings concerning threats to life, property, and national security. EAS is more

[2] Public Alert and Warning System, Exec. Order No. 13,407, § 2(a)(ix), 71 Fed. Reg. 36,975, 36,976 (June 28, 2006).

appropriately understood as public-safety infrastructure deployed within communications facilities, regardless of the particular technology used to implement it.[3]

That distinction is increasingly important as the Commission strengthens EAS cybersecurity and message authentication. The Commission is appropriately seeking greater assurance that emergency messages are authentic, and that EAS systems are protected against compromise.[4] It would be inconsistent with that direction to assume, without further examination, that required EAS functions can simultaneously be absorbed into general-purpose commercial processing environments without preserving equivalent controls over platform integrity, configuration, cybersecurity, testing, recovery, and manufacturer accountability.

The regulatory character of EAS should follow the function, not the form factor or location of the equipment performing it. EAS does not become an ordinary broadcast application merely because its functions can be executed within a broadcast processing platform. Modernization should begin with the security, reliability, and assurance requirements appropriate to a public-warning system and determine what architectures can satisfy those requirements, rather than begin with the architecture of the modern broadcast plant and determine how EAS can be fit shoehorned into it.

## 3 The Regulatory Focus Should Be the Complete EAS Implementation

DAS has long supported EAS modernization. The concern here is not the use of software; it is the separation of certified EAS functions from a known, controlled, and accountable operating environment. The principal advantages claimed for software-based EAS are flexibility, potential integration efficiency, reduced reliance on dedicated hardware, and potentially faster software updates.

Those benefits are possible, but remain largely operational conveniences. The principal advantages of a dedicated EAS device are directly tied to the Commission's public-safety responsibilities: a defined certification boundary, controlled configuration, reduced attack surface, operational independence, failure isolation, inspectability, reproducibility, recovery, and clear manufacturer accountability.

The Commission should be cautious in distinguishing genuine modernization from the mere relocation of critical EAS functions to shared or general-purpose platforms without equivalent assurances of reliability, security, and accountability.

Modern certified EAS equipment already relies extensively on software for monitoring, decoding, encoding, CAP processing, alert handling, logging, configuration, operator interfaces, networking, security updates, and integration with downstream systems. What makes those systems dependable is not the absence of software, but

---

[3] See 47 C.F.R. § 11.1; Exec. Order No. 13,407, § 1, 71 Fed. Reg. at 36,975 (Federal policy for an effective, reliable, integrated, flexible, and comprehensive public alert-and-warning system for war, terrorist attack, natural disaster, and other hazards to public safety and well-being); see also Amendment of Part 11 of the Commission's Rules Regarding the Emergency Alert System, Notice of Proposed Rulemaking, FCC 24-23, ¶ 3 (2024) describing EAS as a national public warning system used to warn the public of emergencies and dangers to life and property.

[4] See also Exec. Order No. 13,407, § 2(a)(ii), (v), 71 Fed. Reg. at 36,975–76 (directing the adoption of protocols and procedures supporting interoperable and secure delivery of coordinated messages, and the protection and restoration of communications capabilities necessary for the public alert-and-warning system).

the combination of identified hardware, controlled host environments, defined interfaces, tested configurations, and singular manufacturer accountability.

The FNPRM sometimes frames the issue as a choice between software and hardware. That framing is too simple. The public-safety question is whether a proposed implementation preserves or improves reliability, operational independence, cybersecurity, certifiability, accountability, and continued operation under emergency and degraded conditions.

DAS itself has offered a software-based DASDEC implementation (the Collector™) for more than a decade. Collector has not been used as the Part 11 compliance device; rather, it is a secondary message processor, that operates after the original message(s) have been vetted. Our experience here gives us good grounding to note the additional support, integration, and cybersecurity responsibilities that arise when EAS functions move beyond a bounded appliance.

### *3.1 A Revised Regulatory Framework Would be Needed*

The Commission should establish a regulatory framework that defines, bounds, and independently certifies the complete system responsible for required EAS functions. Any authorization framework must instead be built around a complete, defined ***"EAS Implementation***" (a specific term we propose in this comment). At a minimum, the framework for EAS Implementations must provide that:

- certification would attach to the defined configuration that performs or directly controls required EAS functions, subject to an FCC-administered or FCC-recognized independent certification and verification process, rather than supplier self-verification;
- the host hardware, operating system, virtualization environment, firmware, interfaces, dependencies, security controls, deployment topology, update process, and recovery model would fall within the certification boundary where they materially affect compliance;
- software-based implementations would preserve required monitoring, CAP processing, independent fallback paths, local alert processing, logging, and continued operation during Internet, host, network, or enterprise-service failures;
- platform identity, software and firmware integrity, authenticated updates, configuration control, access control, audit logging, vulnerability management, and lifecycle support must apply to both the EAS application and its host environment;
- downstream automation, routing, audio or video processing, playout, transport encoding, multiplexing, and payload-generation systems would not become EAS compliance equipment merely because they carry, switch, route, or insert alert content;
- routine code-table updates could receive streamlined treatment, but material changes to required functions, hosts, dependencies, security controls, or deployment topology would remain subject to appropriate certification review; and
- local-operation and cloud restrictions would be treated as operational-readiness requirements, while allowing remote monitoring, administration, support, update distribution, and reporting that do not perform required EAS functions or make local operation dependent on external connectivity.

The Commission should also adopt a coherent regulatory vocabulary distinguishing four related but different concepts: the EAS function being performed; the hardware, software, or hybrid form of the implementation; the complete configuration subject to certification; and the deployed installation at an EAS Participant's facility. The proposed term "EAS software," particularly when it refers to software that "performs and/or manages" EAS requirements, is too broad and could unintentionally encompass monitoring, reporting, maintenance, licensing, or downstream signal-chain applications that do not themselves perform regulated EAS functions.[5]

The Commission should not authorize software-based EAS based on assumed flexibility, presumed cost savings, or assumed equivalence to existing certified systems. For each defined configuration, equivalent assurance should be demonstrated through certification against objective technical, cybersecurity, operational, and accountability requirements applicable to the complete implementation.[6] Any resulting rules must impose genuinely equivalent certification, security, lifecycle, inspection, and support obligations across appliance, software, and hybrid implementations. A framework that certifies only an application while externalizing material responsibilities and costs would weaken public-warning assurance, distort competition, and jeopardize the continued sustainability of the EAS supplier ecosystem.

Any authorization should also address national security and supply chain eligibility. The Commission should require transparency regarding ownership, development, signing, updating, remote administration, component provenance, and third parties who can modify an EAS implementation. Products, software, firmware, critical components, and update services controlled by entities presenting an unacceptable national-security risk should not be permitted to enter or remain active in the EAS ecosystem merely because an earlier equipment authorization was granted.

Finally, the Commission should assess the effect of the proposed rules on supplier sustainability and national resilience. The EAS market is small, specialized, concentrated, and driven largely by replacement demand. A compliance pathway that imposes materially different certification, cybersecurity, lifecycle, and support obligations on software and appliance suppliers could advantage certain firms, reduce the revenue supporting continued engineering and field service, increase market concentration, and create common technical or proprietary failure points. Supplier diversity is not simply a commercial interest; it is part of the resilience of the national public-warning system.[7]

---

[5] See FNRPM, FCC 26-38, ¶¶ 96, 104–09 (2026); id. app. B, proposed 47 C.F.R. § 11.2(e) (defining "EAS Software" as software integrated within an EAS Participant's audio and video processing system that "performs and/or manages" specified Part 11 requirements and that may be installed across multiple components).

[6] NIST SP 800-161r1-upd1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (Nov. 2024) (addresses lifecycle-wide supply-chain risk management, system components, provenance, and supplier relationships).

[7] See US Gov't Accountability Office, GAO-10-296, Critical Infrastructure Protection: Update to National Infrastructure Protection Plan Includes Increased Emphasis on Risk Management and Resilience, at 24–25 (2010) (describing Communications Sector resilience as supported by technology, redundancy, and diversity); Exec. Order No. 13,407 § 2(a)(ix), 71 Fed. Reg. 36,975, 36,976 (June 28, 2006) (directing DHS to administer EAS as a critical component of the public-alert-and-warning system).

DAS accordingly urges the Commission to adopt a software-EAS framework that limits authorization to EAS Implementations that are defined, testable, independently certified, secure, locally operable, and accountable. The Commission may properly address the underlying policy issues in this proceeding; it should do so through enforceable certification and operational requirements, rather than through a general authorization that leaves material system boundaries and responsibilities to be determined after deployment.

### *3.2 The Discussion Should be about "EAS Implementation", Rather than "Hardware Vs. Software".*

The comparison is therefore not properly characterized as "hardware versus software." Existing EAS devices already rely extensively on software. The issue is whether the Commission should create a new regulatory category that permits those functions to run on general-purpose hosts or across signal-processing components unless the final rules establish enforceable requirements for cybersecurity, certification, reliability, host control, interoperability, intellectual property, and supplier sustainability.

The meaningful comparison is between a bounded, certified EAS system and a model in which EAS functions may be decoupled from the hardware, operating environment, dependencies, and the parties responsible for their reliable operation. The regulatory question is whether a software-based implementation can preserve equivalent or greater assurance while remaining identifiable, testable, certifiable, inspectable, recoverable, and accountable.

The Commission's proposed definition would cover software "physically integrated within an EAS Participant's audio and video processing system" that "performs and/or manages" specified EAS requirements. It would permit installation on a server, personal computer, or custom-manufactured system component, or "across multiple components within an EAS Participant's signal processing system," while excluding cloud-based EAS functions and third-party cloud EAS services.

That is a significant architectural change. It could move Part 11 compliance functions into ordinary automation systems, routers, audio and video processors, playout systems, transport encoders, multiplexers, importers/exporters, broadcast payload generation systems, or potentially into a generic PC. It is unclear how those configurations would be bounded, certified, secured, supported, or inspected.

Consistent with DAS's prior comments, the complete certified EAS Implementation should satisfy all Part 11, Part 15, CAP, and cybersecurity requirements applicable to the components within its certification boundary; software code considered separately is not itself an intentional or unintentional radiator subject to Part 15.

DAS proposes a practical path forward: continue exploring software-based EAS, while keeping the regulated system defined, testable, and accountable. Innovation should not turn mandatory EAS compliance into a shifting collection of host configurations, proprietary interfaces, and fragmented support responsibilities.

### *3.3 No Core EAS Function Is Unique to Software*

The Commission asks whether EAS software could provide functions not available to EAS hardware devices and particularly beneficial to alert originators. DAS is unaware of any core EAS function that is available only when implemented as stand-alone software on a general-purpose host. Modern EAS appliances are already software-intensive systems. Encoding, decoding, CAP receipt and processing, alert validation, filtering, routing, logging, configuration, monitoring, control, and downstream alert signaling may be implemented in an appliance, a defined software deployment, or a hybrid system. The relevant difference is therefore one of packaging, host environment, and system integration—not the presence of a new EAS function.

To the extent the Commission has in mind browser-based workflows, enterprise integration, application-programming interfaces, centralized management, or similar conveniences, those may be useful ancillary capabilities, but they are not unique to software-based EAS and do not require that the Part 11 compliance function be removed from a certified appliance. An appliance may provide such capabilities directly or through defined companion applications and interfaces. Moreover, software that merely monitors, reports on, administers, or exchanges information with a certified EAS system should not itself become regulated EAS software unless it performs or directly controls a required Part 11 function.

We suggest that a dedicated EAS appliance may provide public-safety-relevant capabilities that software alone cannot furnish. For example, DASDEC systems incorporate internal radio monitoring and storage capability to facilitate input auditing, along with native video slate generation. A purported software-only implementation can provide comparable functions only by relying on external RF receivers, hardware-based audio and video interfaces, processing resources, storage, among other hardware and service dependencies. Once those elements are necessary to receive, process, log, or transmit alerts, they are not incidental to the system; they are part of the complete EAS Implementation that must be identified, tested, secured, and certified. The Commission should therefore not assume that "software" expands EAS functionality. It may instead redistribute functions and dependencies that existing appliances already provide within a defined and accountable system boundary.

## 4 The Commission Must First Establish a Certifiable and Administrable Model

The Commission should not assume that appliance-based EAS sits outside modern broadcast and cable systems or requires those systems to conform to obsolete interfaces. At a contemporary broadcast station, cable headend, or centralized distribution facility, the EAS device is ordinarily integrated at multiple points in the operating workflow: it exchanges status, control, and alarm information with facility-management and automation systems; and delivers the required alert audio, video, text, triggering, and metadata to downstream routing, playout, encoding, multiplexing, and distribution systems.[8]

The fact that the EAS device retains a discrete form factor does not make it external to, or incompatible with, the modern air chain. It serves as a purpose-built, interoperable control point within that chain, one that can accommodate IP-based and conventional inputs, networked digital-audio environments, automation systems, routing and playout infrastructure, and multiple downstream distribution paths. The distinction is that these integrations occur through defined and supportable interfaces, while the functions required by Part 11 remain within a known, testable, and independently certifiable EAS boundary.

The relevant question is therefore not whether an EAS function is embodied in software or in an appliance, but whether the complete implementation can reliably perform required functions, withstand failures and compromise, and remain identifiable, inspectable, and accountable throughout its operating life.

[8] See, the Future TV (Nov. 19, 2024), https://www.thefuture.tv/2024/11/23/digital-alert-systems-v5-4-software-supports-full-aoip-air-chain-and-boosts-security-with-sso/; Digital Alert Systems, Optional Software, https://www.digitalalertsystems.com/software. DASDEC supports CAP processing; TCP/IP transport of EAS audio, data, and control triggers; optional AES67/Livewire+ audio-over-IP; interfaces with automation, master-control, cable, and video platforms; MPEG transport-stream output; multi-station operation; and remote monitoring. These capabilities enable a purpose-built EAS device to operate as an integrated, locally operable control point within modern IP, automation, routing, playout, and distribution workflows, rather than as a disconnected peripheral..

### *4.1 Product-Specific Integration Limitations Do Not Justify a New Regulatory Model*

In the prior inquiry, many comments appear to reflect integration issues associated with particular equipment in particular radio architectures, especially facilities using streamed monitoring sources, AES67, or other networked audio environments. Where a device lacks native support for those interfaces, gateways or conversion may be required. That is a legitimate but product-specific issue, not an inherent limitation of dedicated EAS equipment as a class, and not of the Digital Alert Systems' DASDEC in particular.

Another EAS manufacturer has previously stated that software-only EAS would operate "within the system, rather than trying to force the existing system to accommodate EAS." In context, that observation appears directed principally to the use of streamed monitoring sources and networked digital-audio environments. But the asserted integration concern is not inherent to appliance-based EAS, nor does it establish that a certified EAS device cannot operate effectively within modern broadcast and cable architectures. DAS has separately described to the Commission how current DASDEC systems integrate with IP-based monitoring, digital-audio, automation, routing, and downstream distribution environments.

The assertion by that manufacturer should not be mistaken for a showing that the claimed limitation is inherent in certified EAS devices generally, rather than in the design choices of a particular product or implementation. At most, that observation may describe the capabilities or integration choices associated with one particular product implementation. It does not support a general conclusion that software-based EAS is necessary to accommodate modern air-chain requirements, or that device-based EAS must be "forced" into those environments. The relevant policy question is whether a proposed EAS implementation—whether appliance, software, or hybrid—can meet Part 11's operational, security, certification, and accountability requirements as a complete system.

Other certified appliance-based systems, including DASDEC, already integrate directly with automation and playout platforms, audio-over-IP (AoIP) networks, master-control systems, multiplexers, cable headends, transport-stream systems, and related infrastructure. Hybrid and edge-based architectures can likewise exchange EAS audio, control information, and alert data with centralized or virtualized air chains. A well-designed appliance can adapt to the Participant's architecture rather than require the architecture to adapt to it.

The Commission should also not assume that software-based EAS will necessarily cost less or be easier to operate. Software may reduce rack space or simplify some deployments, but a fair comparison must include host infrastructure, integration, cybersecurity, redundancy, operating-system maintenance, regression testing, configuration control, licensing, and responsibility for failures involving both the application and its host. Software may redistribute cost and complexity rather than remove them.

The relevant inquiry is not whether a particular product requires an interface converter or additional integration step. It is whether an appliance-based, virtualized, distributed, or hybrid architecture can demonstrate the reliability, interoperability, cybersecurity, continuity of operation, certifiability, and lifecycle support required by Part 11. Product-specific inconvenience does not establish a defect in the existing certification model, much less justify replacing it with one in which the regulated system, certification boundary, and responsible party may be less clearly defined. Part 11 should be modernized without treating the limitations of a particular product or deployment as limitations of appliance-based EAS as a whole.

### *4.2 The Proposal Does Not Define the Regulatory Object Required for Certification*

DAS previously explained that the FCC-certified EAS system serves as the trust anchor for authentication, alert processing, policy enforcement, routing, logging, and program insertion. That position is functional rather than

chassis-specific. Whether implemented as an appliance, software, or a hybrid architecture, the regulated EAS Implementation must remain an identified, certified, secure, inspectable, and accountable trust anchor.

The threshold question is whether the proposed software-EAS model provides a sufficiently well-defined regulatory object for Part 11 certification, independent verification, and enforcement. Before authorizing such a model, the Commission must be able to determine what constitutes the EAS Implementation; which hardware, software, operating-system, virtualization, security, interface, and dependency elements fall within its certification boundary; how conformity with the certified configuration will be independently verified in the field; which changes require additional review or authorization; and which party remains responsible when required functions fail.

That process cannot be reduced to self-verification by the software developer, host vendor, or EAS Participant. EAS is a mandatory public-warning function, and its failure, compromise, or misconfiguration can result in false, altered, delayed, or unavailable alerts. Those risks extend beyond the individual implementer to downstream participants, public-safety authorities, and the public. The Commission must therefore preserve an FCC-administered or FCC-recognized independent process for certification and verification of EAS solutions against defined technical and operational requirements. A vendor's assertion that software code conforms to Part 11 cannot establish that the complete deployed implementation, including its host, dependencies, interfaces, security controls, and update mechanisms, will perform reliably or remain compliant over time.

The problem is not merely an absence of additional information in the record. The proposed authorization does not specify how a software implementation running on a general-purpose computer or across multiple signal-processing components becomes a defined regulatory object for certification, independent verification, and enforcement. A final rule authorizing such an implementation must enable the Commission to identify the complete system being certified, reproduce the configuration that was tested, determine whether a deployed installation conforms to that configuration, and assign responsibility for maintaining the required EAS functions. Unless the adopted framework does so, the authorization would not be certifiable, independently verifiable, or administrable under Part 11.

Software-based EAS may be workable in defined circumstances and within carefully defined configurations. The relevant question is not whether software can perform individual EAS functions, but whether the authorization requires the complete implementation to be bounded, tested, independently certified or verified, installed, inspected, updated, restored, and supported as a coherent public-safety system.

### *4.3 EAS Participants Operate Public-Safety Functions at Critical-Infrastructure Sites*

EAS is not an ordinary broadcast workflow application. It is mandatory public-safety infrastructure that must operate during emergencies and degraded conditions at facilities with widely varying levels of engineering support, cybersecurity maturity, redundancy, staffing, and vendor resources.[9] Part 11 applies across broadcast, cable, wireline video, DBS, SDARS, and other participating services.

The Commission identifies several potential benefits of software-based EAS, but those benefits remain prospective and should not be assumed merely from a change in implementation. Claimed gains in efficiency, integration,

[9] EAS devices and/the application must continuously monitor multiple audio inputs, network inputs (IPAWS) and make specific logic choices based on those inputs. Moreover, the outputs are also dynamically modulated from live events like an EAN and NPT, down to mundane events like RMT or RWT. Each input can have a varied response and output based on the input(s) and individual user-defined configurations.

flexibility, or cost should be evaluated against their actual effects on reliability, resilience, cybersecurity, and operational accountability, particularly where required EAS functions are distributed across multiple signal-processing components. Before authorizing software-based EAS broadly, the Commission should determine whether those benefits are demonstrable and whether they can be achieved without diminishing the protections expected of certified EAS systems.

Any final regulatory framework must specify the certification boundary, acceptable host environments, treatment of distributed architectures, required cybersecurity controls, behavior during host or network failures, effects of software and platform changes, proprietary dependencies, long-term support obligations, field-verification methods, and responsibility for restoring required EAS functions. The Commission identifies several potential benefits of software-based EAS, but those benefits remain prospective and should not be assumed merely from a change in implementation. Claimed gains should be evaluated against their actual effects on reliability, resilience, cybersecurity, and operational accountability, particularly where required EAS functions are distributed across multiple signal-processing components.

The Commission should determine whether those benefits are demonstrable and whether they can be achieved without diminishing the protections that are expected of certified EAS systems. Any final regulatory framework must specify the certification boundary, acceptable host environments, treatment of distributed architectures, required cybersecurity controls, behavior during host or network failures, effects of software and platform changes, proprietary dependencies, long-term support obligations, field-verification methods, and responsibility for restoring required EAS functions.

These are not secondary implementation details that may safely be delegated to individual Participants, integration vendors, certification laboratories, or future software releases. They determine whether the EAS Implementation will remain available, inspectable, and accountable during the conditions in which it is most needed. The Commission should prescribe the governing certification and operational framework in its rules and authorization process, rather than permit it to emerge piecemeal through individual certifications and deployments.

## 5 The Proposal Must Be Reconciled with the Proceeding's Cybersecurity Objectives

This proceeding is focused in substantial part on EAS cybersecurity, including the risk that compromised EAS or related systems could generate false alerts, hijack programming, or interfere with legitimate warnings. The Commission's discussion extends to EAS equipment, studio-transmitter-link equipment, and remotely managed systems that route, process, or insert programming content.

That security objective points toward tighter platform control, stronger authentication, controlled updates, hardened configurations, reduced attack surfaces, network segmentation, and clear accountability.

A broad EAS software framework could potentially move in the opposite direction. Allowing certified functions to run on a server, personal computer, custom component, or several signal-processing components may expand the attack surface unless the rule also defines and controls the host environment.

A dedicated certified EAS device has a defined boundaries for hardware, software, firmware, interfaces, and support. Software that is relegated to run on a general-purpose server, virtual machine, automation computer, processor, router, or playout system inherits the host's unrelated workloads, remote-access tools, third-party dependencies, patch variability, credentials, network exposure, storage, logging, and configuration drift.

DAS has consistently moved toward more tightly controlled hardware and software platforms, stronger update processes, fewer unnecessary services, improved authentication and logging, and tighter binding of software to authorized hardware. The reason is straightforward: software security cannot be evaluated apart from the platform on which the software runs – including the operating system, any supervisory applications (such as hypervisors), and the physical platform itself.

The Commission asks whether software-based EAS would require more technical and cybersecurity expertise than stand-alone equipment. For many smaller broadcasters and cable systems, the answer may be yes. A rule that assumes around-the-clock broadcast IT and cybersecurity support could increase the risk of misconfiguration, delayed patching, insecure remote access, incomplete logging, and degraded alert performance.

The Commission should not tighten EAS cybersecurity requirements while loosening the environment in which certified EAS functions operate.

### *5.1 Federal Cybersecurity Guidance Supports a System-Level Trust Model*

Modern EAS equipment is already software intensive. The relevant question is not whether software can perform EAS functions, but whether certified functions should operate as portable code separated from a known, authorized, and integrity-verified platform.

The Commission's June 25, 2026 Public Notice describes software implementation as a way to remove outdated hardware requirements while also emphasizing protection against cybercriminals and foreign adversaries. Those goals can be reconciled only if software-based EAS implementations are treated as a complete trusted system rather than an application that can be moved among arbitrary or unmanaged hosts.

NIST and CISA guidance generally treats platform identity and integrity as part of the security problem. Hardware-backed identity, secure or measured boot, cryptographic integrity verification, controlled updates, asset inventory, and attestation are mechanisms for establishing that software is running on an expected and authorized platform.

At a minimum, an EAS Participant should be able to associate each software instance with a specific hardware platform, firmware and software versions, configuration, network role, physical location, and operational function. That is consistent with zero-trust principles that evaluate both the user and the device before granting access or authority.

For public-warning functions, the software, host platform, cryptographic identity, update path, logs, and operational interfaces must be evaluated as one system. A certification model that considers only the application would leave the most important platform risks outside the scope of authorization.

### *5.2 Relevant CISA and NIST Guidance*

DAS has developed its products in line with the broader federal direction for critical-infrastructure systems: known platforms, protected configurations, authenticated software and firmware, hardware-supported roots of trust where appropriate, secure update mechanisms, device identity, and manageable asset inventories.

That guidance does not treat a critical workload as unchanged when it moves across host environments. The risk profile changes with the platform, configuration, update path, and operational dependencies. The Commission should therefore define the trust boundary around any host that performs certified EAS functions.

DAS notes the cybersecurity baseline proposed in our earlier comments, including authenticated updates, secure configurations, role-based access controls, audit logging, network segmentation, vulnerability disclosure, component transparency, and appropriate reevaluation following material platform changes.[10] Those controls apply equally to software EAS and to the host, operating system, dependencies, and update infrastructure on which certified EAS functions depend.

Applied to EAS, the common principle is that the software, host platform, cryptographic identity, configuration state, update mechanism, logging, operational interfaces, and recovery process should be treated as a single trusted system. The following Federal guidance is particularly relevant to that system-level approach:

| Guideline / Recommendation | Relevance to Software-Based EAS |
|---|---|
| NIST SP 800-193, Platform Firmware Resiliency Guidelines | Addresses protection, detection, and recovery for platform firmware, treating trusted boot and platform-firmware integrity as foundations for higher-level software assurance. |
| NIST SP 800-53 Rev. 5 | Security controls relevant to device identification, software and firmware integrity, components, cryptographic key management, access control, and supply-chain risk. |
| NIST IR 8320, Hardware-Enabled Security | Describes the physical platform as the first layer of a layered security approach and discusses TPMs, trusted execution environments, HSMs, secure enclaves, and other hardware-enabled controls. |
| NIST IR 8320A / 8320B / 8320C | Addresses hardware roots of trust, machine identity, asset tagging, remote attestation, workload protection, and verification of platform trust status. |
| NIST SP 800-207, Zero Trust Architecture | Rejects implicit trust based on network location or ownership and requires authentication and authorization of both users and devices. This supports use of authorized, posture-verified hosts for critical functions. |
| NIST SP 800-161 Rev. 1, Cybersecurity Supply Chain Risk Management | Addresses supplier, component, software, firmware, and lifecycle risks that arise when critical workloads depend on third-party platforms, dependencies, and update paths. |
| CISA Cross-Sector Cybersecurity Performance Goals | Provides baseline critical-infrastructure practices for secure configuration, access control, vulnerability management, logging, segmentation, and resilience. |
| CISA OT Asset Inventory Guidance | Emphasizes current inventories of hardware and software so operators know what must be secured, maintained, and recovered. This supports a documented association between software instances and host platforms. |
| CISA Secure by Design | Supports secure defaults and placing the primary security burden on manufacturers rather than requiring customers to assemble critical controls after deployment. |

[10] Comments of Digital Alert Systems.

### *5.3 Suggested Minimum Conditions for a Software-EAS*

Any authorization for an EAS software Implementation should require the certification applicant to demonstrate, and the certification grant to identify the following conditions:

1. **Authorized host platform.** The certification grant must identify the authorized and supportable host environment and prevent operation on an arbitrary server, virtual machine, clone, backup image, or repurposed workstation.

2. **Protected machine identity.** The implementation must use protected credentials or an equivalent mechanism that prevents operational authority from being copied solely through software, credentials, license files, or a virtual machine image.

3. **Secure or measured boot.** The implementation must verify the integrity of the material firmware, boot loader, operating-system, runtime, and application elements before certified functions are enabled.

4. **Platform verification.** The implementation must provide attestation or another method to confirm that the platform remains in an approved state, where appropriate for the certified architecture.

5. **Update integrity.** Material software, firmware, configuration, and dependency updates must be authenticated, logged, tested, protected against unauthorized rollback, and subject to certification-impact review where appropriate.

6. **Configuration control.** Critical monitoring, authentication, routing, certificate, logging, and alert-processing settings must be protected from unauthorized change and subject to documented configuration control.

7. **Operational resilience.** The certified configuration must identify its material dependencies and demonstrate continued required operation, fallback capability, or defined recovery behavior when shared storage, endpoint protection, identity services, a time source, network segmentation, or the virtualization environment fails or is compromised.

8. **Certification boundary.** The certification boundary must identify the application, operating system, hypervisor where applicable, hardware, configuration, cryptographic modules, update process, and other elements that materially affect the complete deployed system.

9. **Accountability and support.** The grant and associated documentation must identify responsibility for restoring required EAS capability when a failure spans the application, host, network, enterprise IT, or managed-service layers.

These are not objections to innovation. They are minimum conditions for authorization. They do not require the Commission to mandate a single technical design or to exclude any virtualized, distributed, or software-forward architecture. Instead, they require the Commission to ensure that any authorized architecture remains a known, secure, testable, recoverable, and supportable system rather than a loosely bounded workload whose compliance depends on an uncontrolled environment.

The central distinction is not hardware versus software. It is whether the required EAS functions remain bound to a known, secure, testable, recoverable, and supportable system. Dedicated appliances are one way to establish that boundary. Virtualized, distributed, or software-forward models may also be viable if they provide equivalent

assurance through device identity, platform integrity, signed components, protected credentials, controlled updates, tamper-evident logging, and clear certification boundaries.

If the Commission proceeds, it should define EAS software narrowly and require any software-based implementation to include the platform-trust controls expected of critical-infrastructure systems.

## 6 EAS Software Should Be Regulated as Part of a Certified System

Modern EAS devices already include substantial software. Those functions do not become a separate regulatory category merely because software performs them; they remain part of an integrated certified EAS system.

Any software-based EAS Implementation must preserve the existing system's required monitoring sources, CAP-first processing, over-the-air fallback capability, local alert processing, and independent logging and control. Changing the platform on which EAS functions operate must not make required alert reception or transmission dependent upon Internet availability, enterprise services, shared storage, remote licensing, or another communications pathway that may be impaired during the same emergency.

Defining EAS software as a checklist of functions could blur the line between a certified system and an application that performs only part of the required work on a host selected later by the Participant or a signal-chain vendor.

Certification should attach to a defined EAS system configuration, including the host environment, operating system, security configuration, dependencies, required interfaces, update process, logging, operator access, and downstream connections necessary for compliance. The authorization should cover the complete configuration, not software functions in the abstract.

The rules should also make clear that station automation, routing, audio or video processing, playout, transport encoding, multiplexing, program replacement, alert insertion, and broadcast-payload generation do not become EAS software merely because they exchange audio, data, metadata, or control signals with a certified EAS system. Such components should fall under Part 11 only when they are submitted, tested, and certified as part of the EAS implementation.

### *6.1 Local Installation Alone Does Not Establish Resilience*

DAS supports the Commission's proposal to exclude cloud-based EAS functions and third-party cloud EAS services. Local operation is necessary but not sufficient.

The proposal would require EAS software to be located at the Participant's facility, such as a studio, transmitter site, or cable headend. This appropriately recognizes the risk of relying on Internet or wide-area connectivity for functions that must remain operational during an emergency.

A local software instance can still depend on fragile shared infrastructure, including LAN switches, VLANs, virtual audio paths, IP-routed monitoring sources, shared storage, authentication services, licenses, hypervisors, time sources, remote-access systems, and domain controllers. A system may be geographically local yet remain dependent on a complex and dispersed IT environment.

Accordingly, local installation should be paired with a requirement that software-based EAS operate only within an identified, hardened, documented, supported, and certified system configuration.

### *6.2 The Host Environment Must Be Within the Certification Boundary*

EAS software cannot be meaningfully certified independently from its host. The same application can exhibit materially different reliability, security, timing, audio, logging, and support characteristics on a hardened appliance, an industrial computer, a general-purpose PC, an automation server, a virtual machine, a shared server, or a signal-processing component.

A certification application should identify the hardware platform or representative hardware class, the operating system, the hypervisor where applicable, required dependencies, audio and data interfaces, network interfaces, operator interface, logging method, update method, storage, security configuration, and any external interfaces required for operation.

This need not limit certification to a single hardware model. The Commission could authorize a specific platform, a defined platform family, or a representative hardware class. However, it should not permit an "install anywhere" concept that separates the software from the computing environment that determines whether or not it will work reliably.

Distributed installation across several signal-chain components should not be authorized through an abstract or application-only certification. A distributed architecture may be authorized when the complete integrated configuration is identified, tested, documented, and certified as a single EAS Implementation. Certification should not attach to an abstract function that may later be spread across indeterminate combinations of station equipment.

## 7 A Workable Software-EAS Framework Must Address the Full System

Software-based EAS may be workable, but only if the Commission recognizes the system that must surround the application. The software cannot be treated as a generic workload running on an arbitrary host.

A credible framework would require a defined trust boundary, authenticated machine identity, platform-integrity controls, protected credentials, controlled updates, configuration integrity, tamper-evident logs, operational resilience, and clear responsibility and accountability for failures.

In practical terms, the software, host platform, operating system, firmware, cryptographic identity, configuration, update process, logging, interfaces, and recovery model all constitute the regulated EAS implementation.

That is a substantial shift in technical, cybersecurity, operational, and compliance responsibilities. It should be explicitly recognized rather than treated as a minor change in product form.

### *7.1 Authorized Host Platform and Machine Identity*

Software-based EAS should run only on an authorized and supportable platform configuration. The platform may be a purpose-built appliance, server, virtualized environment, or integrated broadcast system, but it should not be an undefined host selected after certification by a Participant or IT provider.

The supported configuration should specify the processor architecture, operating system, hypervisor (where applicable), firmware dependencies, hardware security capabilities, network interfaces, time source, update and logging paths, insertion interfaces, and other operational dependencies.

The implementation should also include a protected machine identity to ensure that operational authority cannot be copied merely by duplicating software, credentials, certificates, license files, or virtual-machine images. TPMs, HSMs, secure elements, secure enclaves, or equivalent mechanisms may provide that function, but they also require provisioning, key management, recovery, and lifecycle support.

### *7.2 Platform Integrity and Attestation*

Certified EAS functions should not activate unless the underlying platform is in an expected state. The implementation should verify, using secure boot, measured boot, or equivalent controls, the integrity of firmware, bootloaders, the operating system, runtime components, and the EAS application.

The system should also be able to demonstrate that it is running on an authorized platform in an approved configuration. Depending on the architecture, this may require local or remote attestation or another method of platform verification.

Without such controls, neither the vendor, the Participant, nor the Commission can be certain that the deployed system still matches the certified configuration. These mechanisms add complexity, but that complexity is inherent to operating critical public-warning software on a general-purpose or shared platform.

### *7.3 Updates, Configuration, and Lifecycle Control*

Software, firmware, and configuration updates should be authenticated, integrity-checked, logged, and protected against unauthorized rollback. The same discipline should apply to operating-system components, drivers, authentication libraries, certificates, and other dependencies that materially affect EAS operation.

Configuration changes can be as consequential as code changes. Monitoring assignments, location codes, event filters, relay behavior, authentication parameters, audio routing, automation interfaces, certificates, time sources, permissions, logging settings, and alert-processing rules all affect whether the system functions correctly.

A software-based implementation therefore requires role-based access control, tamper-evident configuration records, protection of critical settings, backup and restore controls, version control, regression testing, and a documented process for determining whether a change requires permissive-change review, retesting, or new certification.

### *7.4 Operational Resilience and Accountability*

Software-based EAS inherits dependencies from its host environment, including the operating system, hypervisor, shared storage, endpoint protection, identity management, certificate services, remote-access tools, backup systems, time synchronization, virtual networking, firewalls, and patch management systems.

The certification record should address common failure conditions, including operating system update failures, hypervisor migration, endpoint security interference, certificate expiration, loss of a time source or a domain controller, disk failure, network segmentation changes, backup restoration, and loss of enterprise identity services.

These are common IT failure modes, but EAS is ***not*** an ordinary IT workload. Required functions must remain available, testable, recoverable, and supportable during emergencies and under degraded facility conditions.

The FNPRM asks if software-based EAS might enable “an immediate fail-over of functionality” to backup EAS software in other locations. The Commission should not treat automatic failover as a capability unique to software-

based EAS. That same continuity objective can be achieved through a properly engineered appliance-based or hybrid architecture, including redundant DASDEC systems at geographically separated locations, with health monitoring, defined handoff procedures, and tested backup operation. DAS's HALO platform demonstrates the ability to monitor the health and communication status of distributed EAS systems; combined with an appropriately designed redundant architecture, such monitoring can support prompt operator action or the automated transfer of required functions when a primary device or facility becomes unavailable.

The relevant question is therefore not whether the EAS function is characterized as software, but whether the complete EAS Implementation can continue to receive, process, log, and transmit required alerts when personnel must evacuate a facility or when a primary site becomes unavailable. Any failover arrangement must preserve the current configuration, monitoring inputs, authentication credentials, logging, output paths, and clearly defined operational authority, while preventing duplicate, conflicting, or missed alert actions. These are system-design and certification questions, not inherent advantages of software alone.

### *7.5 Clear Certification and Support Boundaries*

Certification of the application alone would be incomplete. The authorization should cover the supported host, operating system or runtime, firmware dependencies, cryptographic modules, configuration controls, update mechanism, logging, network interfaces, alert inputs, required outputs, and integration points with automation, audio, video, CAP, and legacy EAS paths.

The certification grant should specify which variations are permitted and which changes require additional review. A certified application running on an uncertified or materially altered host is not the same system as the one tested.

The Commission must also define responsibility when failures span the application, operating system, hypervisor, security software, firewall policy, identity services, certificates, storage, networking, or a managed service provider. A software model does not simplify EAS if responsibility is divided among several parties when an alert fails to forward.

For each certified configuration, the manufacturer, Participant, host-platform provider, and any managed-service provider should clearly document responsibilities for security, maintenance, recovery, and support.

### *7.6 The Practical Result*

A workable software-based EAS framework would require authorized hosts, protected machine identity, platform-integrity verification, signed updates, rollback protection, configuration control, operational resilience, clear certification boundaries, and clear accountability. Those are appropriate requirements for critical infrastructure, but they are substantial.

Software-based EAS is often presented as a lower-cost, lower-burden alternative. Once the necessary host, cybersecurity, certification, and recovery controls are included, it may instead shift – or even add to - the cost and complexity into the Participant's IT environment.

DAS supports innovation, but software implementation should not mean platform indifference. Any authorization should preserve the trust, resilience, accountability, and certification clarity expected of national public-warning infrastructure.

### *7.7 Software Defects and Change Control*

The proposed 72-hour repair period for defective EAS software appears to assume that software can be repaired quickly. That may be true for some application defects, but software failures can also arise from interactions with the operating system, hypervisor, drivers, security tools, storage, network configuration, certificates, licenses, and downstream interfaces.

A faulty update can affect many installations at once, and a cybersecurity incident may require an investigation before restoration. Some failures may disable functions without an obvious physical fault or a clear division of responsibility.

The final rules should establish a lifecycle framework covering update integrity, rollback, patch testing, version control, vulnerability reporting, support obligations, end-of-support treatment, backup operation, recovery time, and certification impact.

Material changes to software, host hardware, the operating system, hypervisor, drivers, dependencies, security configuration, logging, monitored-source interfaces, outputs, or downstream control interfaces should undergo a documented certification-impact review.

## 8 Intellectual-Property Considerations Require Disclosure

The Commission asks whether patents or other intellectual-property considerations may affect software-based EAS. They may, particularly if EAS functions are embedded in or distributed across a Participant's signal-processing chain.

DAS is not asking the Commission to decide questions of patent validity or licensing. The practical concern is narrower: some architectures may rely on patented or proprietary methods to replace ordinary programming with EAS or other emergency content. The Commission should avoid rules or certification procedures that unintentionally favor such architectures or conceal dependencies that could affect implementation and support.

The public patent record includes, at a minimum, the following patent family:

1. U.S. Patent No. 11,337,049, "Replacement of channel content with notification content";
2. U.S. Patent No. 11,877,223, "Switching emergency action messages into select media broadcasts."
3. U.S. Patent Publication No. 2021/0058763, the related published application;
4. U.S. Patent Publication No. 2022/0279333, "Switching emergency action messages into select media broadcasts"; and

The two publications are applications, not separate issued patents. The issued patents are the more relevant items for enforceable rights.

U.S. Patent No. 11,337,049 includes claims involving a switching module that sends ordinary channel content to a transport encoder, receives notification content associated with an EAS message, and sends that notification content in place of the ordinary content. Other claims describe an in-band, on-channel importer-exporter that performs related replacement functions.

U.S. Patent No. 11,877,223 includes claims involving an importer-exporter that receives ordinary channel packets and EAS packets, and to a switching module and multiplexer that select content for inclusion in media-channel broadcasts. Other claims address authorization, login, payload generation, transmission, heartbeat alarms, and coexistence with legacy EAS signals.

Those patents may be relevant to configurations in which EAS software is hosted, integrated with, or directly controls routers, playout systems, transport encoders, importers/exporters, multiplexers, or broadcast-payload generation systems to replace ordinary content with EAS content. Such dependencies could affect vendor entry, licensing costs, interoperability, certification boundaries, Participant choice, and long-term support.

DAS also discloses that it is the assignee of:

5. U.S. Patent No. 11,620,295, titled "Method, System and Program Product for Monitoring EAS Devices."

This patent relates generally to monitoring EAS implementations, including changes to configuration settings and software or firmware, maintaining chronological configuration records, aggregating compliance logs, searching and consolidating reports, and managing licenses. DAS does not contend that the patent covers software-based EAS generally. It is identified because some proposals may involve functions related to monitoring, configuration management, update tracking, EAS log reporting, licensing, or enterprise oversight.[11]

If the Commission proceeds, a certification applicant should identify any proprietary, patented, or license-restricted interfaces or methods required by the submitted configuration that could materially affect interoperability, availability, cost, or long-term support. The requirement should focus on dependencies incorporated into the proposed configuration, not on every patent that might be asserted against a broader technology category.

This would provide the Commission and EAS Participants with useful information without requiring the agency to resolve private patent disputes.

## 9 The Commission Should Adopt a Coherent, Technology-Neutral Taxonomy for EAS Functions and Implementations

The Commission need not create separate regulatory regimes for appliances and software. It can establish common functional requirements and apply them to the complete configuration that performs those functions. The relevant questions are what functions the implementation performs, what falls within its certification boundary, whether the deployed system conforms to the authorization, and whether it can perform the required functions locally and reliably.

DAS recommends organizing the proposed rules around a technology-neutral "EAS Implementation." Encoding, decoding, Attention Signal, and CAP processing are regulated functions. Hardware, software, and hybrid systems are implementation forms. Certification applies to a defined configuration, whereas the operational rules apply to each deployed installation.

[11] TVNewsCheck Staff. "Digital Alert Systems Earns Patent on HALO System For EAS/CAP Device Management." TVNewsCheck, 8 June 2023, https://tvnewscheck.com/tech/article/digital-alert-systems-earns-patent-on-halo-system-for-eas-cap-device-management/. Accessed 1 August 2026.

The draft currently uses the same vocabulary for four distinct concepts:

1. **Function:** encoding, decoding, Attention Signal, and CAP processing;
2. **Implementation form:** hardware, software, or hybrid;
3. **Certification object:** the defined configuration that is tested and approved; and
4. **Deployment:** the operational installation at an EAS Participant's facility.

These concepts are related, but they are not interchangeable. Treating them as interchangeable creates uncertainty about whether software is a device, whether each component of a distributed system is separately regulated, what falls within the certification boundary, and whether monitoring or administrative applications qualify as EAS software.

Without clearer distinctions, manufacturers, laboratories, Participants, and enforcement personnel may reach different conclusions about what was certified, what constitutes an EAS system, which components are authorized, and when a modification or failure triggers regulatory obligations.

Proposed § 11.2(e) defines EAS software as software that "performs and/or manages" certain Part 11 requirements, allows it to operate on a single device or across multiple components, and places location and cloud restrictions within the definition. Proposed §§ 11.34 and 11.35 then alternate among encoders, decoders, combined units, EAS software, and "defective equipment."

The result is an unclear regulatory scope. Software may perform a required function, directly control it, or merely monitor and administer a separate system. Those arrangements should not be grouped under the open-ended phrase "performs and/or manages."

The Commission can remain technology-neutral by defining the regulated implementation, identifying its functions, setting the certification boundary, and separately addressing location and operational requirements.

The following revisions would accomplish that:

### *9.1 Amend § 11.2 to Define the Regulated Implementation*

DAS recommends replacing proposed § 11.2(e) with the following definitions:

> **(e) EAS Implementation.** A hardware, software, or hybrid configuration that performs or directly controls one or more functions required by §§ 11.32, 11.33, or 11.56 and is certified or otherwise authorized under § 11.34. When multiple components are certified to operate together, they constitute a single EAS Implementation unless the certification grant identifies them as separately authorized implementations.
>
> **(f) EAS Software Implementation.** An EAS Implementation in which one or more functions required by §§ 11.32, 11.33, or 11.56 are performed principally by software executing on one or more host computing components. An EAS Software Implementation includes the software and the host-environment elements identified within the applicable certification boundary.
>
> Software that solely monitors, logs, reports on, updates, maintains, or administers an EAS Implementation, and does not perform or directly control a function required by §§ 11.32, 11.33, or 11.56, is not an EAS Software Implementation unless it is expressly included within the certification boundary.

> **(g) Certification Boundary.** The software, firmware, hardware, operating system, virtualization or container environment, interfaces, dependencies, deployment topology, and security controls that together constitute the configuration evaluated and authorized under § 11.34.

These definitions would make the complete implementation, rather than an executable file or an isolated component, the regulated object.

They also permit a distributed configuration to be certified as a single implementation while allowing separately certified components to remain distinct.

Finally, they exclude ancillary monitoring, reporting, licensing, and maintenance software unless it performs or directly controls the required function or is expressly included within the certification boundary.

The Commission should therefore remove "manages" from the proposed definition. The term lacks a clear boundary and could apply to almost any application connected to an EAS system.

### *9.2 Treat Encoding and Decoding as Functions Rather Than Product Types*

Sections 11.32 and 11.33 should describe the required encoder and decoder functions rather than assume their implementation in specific physical products. The current organization reflects the appliance-based architecture under which Part 11 was developed.

DAS recommends retitling the sections and revising their introductory language as follows:

> **§ 11.32 EAS encoder-function requirements.**
>
> **(a)** An EAS Implementation that performs the encoder function must, at a minimum, be capable of encoding the EAS Protocol described in § 11.31 and of providing the EAS code transmission functions described in § 11.51. Each such implementation must comply with the following minimum requirements:
>
> **§ 11.33 EAS decoder-function requirements.**
>
> **(a)** An EAS Implementation that performs the decoder function must, at a minimum, be capable of providing the monitoring functions described in § 11.52, decoding EAS messages formatted in accordance with the EAS Protocol described in § 11.31, and processing CAP-formatted EAS messages in accordance with § 11.56. Each such implementation must comply with the following minimum requirements:

References to "the encoder" or "the decoder" should be revised, where appropriate, to "the EAS Implementation performing the encoder function" or "the EAS Implementation performing the decoder function."

This preserves the existing functional requirements, including virtual or physical inputs, outputs, displays, and interfaces, without creating separate substantive standards merely because software performs those functions.

### *9.3 Rewrite § 11.34 Around the Certification Boundary*

Section 11.34 should be retitled "Certification of EAS Implementations" and should clearly specify what the Commission is certifying.

DAS recommends language along the following lines:

> § 11.34 Certification of EAS Implementations.

**(a)** An EAS Implementation that performs an encoder or decoder function required by this part must be certified in accordance with part 2, subpart J, of this chapter.

**(b)** An application for certification must identify the certification boundary and must demonstrate that the complete configuration satisfies all applicable requirements of this part.

**(c)** The certification application must identify, as applicable:

1. the software and firmware products and versions;
2. the permitted host-computing characteristics;
3. the supported operating systems;
4. any virtualization or container environment;
5. required interfaces, services, and dependencies;
6. permitted deployment topologies;
7. required security and access-control mechanisms; and
8. any redundancy, failover, storage, or external components necessary to satisfy Part 11.

**(d)** Encoder, decoder, Attention Signal, and CAP-processing functions may be certified separately or in any combination. Multiple components designed and evaluated to operate together may be certified as a single EAS Implementation.

**(e)** The certification grant must state whether the authorization applies to a specific configuration or to a defined range of configurations, and must identify any permissible variations in host hardware, operating systems, virtualization environments, interfaces, or deployment topology.

**(f)** The grantee must provide instructions sufficient to install, configure, operate, secure, update, and maintain the EAS Implementation within its certification boundary.

**(g)** Software code, considered separately from host-computing equipment, is not required to demonstrate compliance with part 15. Host equipment within the certification boundary remains subject to otherwise applicable part 15 requirements.

**(h)** Waiver requests involving EAS Implementations constructed for use by an EAS Participant but not offered for sale will be considered individually under part 1, subpart G.

This would replace the proposed reference to certification "as a single unit or as EAS Software." A unit and software are not parallel objects; software operates on computing components. Certification should attach to the defined configuration that performs the regulated functions.

### *9.4 Narrow the Treatment of Software Changes*

Proposed § 11.34(f) would treat modifications required to implement new EAS codes as Class I permissive changes. That is reasonable for a limited code table update, but it should not create a broader safe harbor for a software revision merely because the revision also includes a new code.

DAS recommends:

**(i)** A modification limited to implementing Commission-prescribed EAS codes under § 11.31 may be treated as a Class I permissive change where the modification does not alter:

1. the certification boundary;
2. alert-processing or validation logic unrelated to the new code;
3. required inputs or outputs;
4. security or access-control mechanisms;
5. host-system requirements;
6. external dependencies; or
7. deployment topology.

The grantee must verify and document continued compliance with all applicable requirements.

A modification that alters a required EAS function or materially changes the certification boundary must be evaluated under § 2.1043 and is subject to additional testing, filing, or new certification, as applicable.

This would preserve an efficient process for routine code updates without exempting architectural or functional changes from appropriate review.

### *9.5 Move Location and Cloud Restrictions to § 11.35*

The proposed definition combines what EAS software is with where it may operate. Local operation is an operational and resilience requirement, not an intrinsic property of software.

The Commission should move the local-facility and cloud restrictions from § 11.2 to § 11.35.

DAS recommends retitling § 11.35 "Operational Readiness of EAS Implementations" and adding:

> **(a)** Each EAS Participant must ensure that every EAS Implementation used to satisfy this part is installed and operated so that all required monitoring, decoding, encoding, and transmitting functions are available during the times the participant's stations or systems are in operation.
>
> **(b)** An EAS Software Implementation used to satisfy the requirements of this part must perform its required EAS functions at an EAS Participant facility used to provide service, including a broadcast studio, control point, transmitter site, cable headend, or other local service-delivery facility.
>
> **(c)** The required functions of receiving, validating, decoding, generating, and transmitting EAS alerts must not depend upon real-time processing by a remote or cloud-based third-party EAS service.
>
> **(d)** Nothing in this section prohibits remote monitoring, administration, technical support, update distribution, backup storage, compliance reporting, or other ancillary services, provided that:
>
> 1. those services do not perform a required EAS function on behalf of the local EAS Implementation;
> 2. loss of external connectivity does not prevent the local EAS Implementation from performing all required EAS functions; and
> 3. the ancillary service does not place the EAS Implementation outside its certification boundary.

This language avoids the proposed phrase "physically integrated" within an "audio and video processing system." Software is physically resident on a host and logically integrated with other systems. "Signal-processing or service-delivery system" is also more inclusive of radio and other EAS Participants.

### *9.6 Use a Single Term in the Operational-Readiness and Defect Provisions*

Section 11.35 should not list encoders, decoders, combined units, Intermediary Devices, and EAS software when the same requirement applies to all certified implementations.

The Commission should use "EAS Implementation" throughout § 11.35 and distinguish between software and non-software implementations only when different repair periods are intended:

> (e) If an EAS Implementation becomes inoperative or materially incapable of satisfying the requirements of this part, the EAS Participant may operate without that implementation pending repair or replacement for the period specified in this paragraph.
>
> For an EAS Implementation other than an EAS Software Implementation, the permitted period is 60 days.
>
> For an EAS Software Implementation, the permitted period is 72 hours.

For purposes of this paragraph, an EAS Software Implementation becomes inoperative when a component within its certification boundary fails or becomes unavailable in a manner that prevents a required EAS function.

This language also replaces "defective equipment" with "becomes inoperative or materially incapable of satisfying the requirements of this part," a trigger that applies more naturally to hardware, software, and hybrid systems.

## 10 The Commission Should Address Foreign-Supply Risks

The Commission should apply the same forward-looking national-security logic reflected in PS Docket No. 26-184 to EAS equipment and potential software.[12] In that proceeding, PSHSB and OET propose to prohibit the continued importation and marketing of previously authorized equipment determined to pose an unacceptable risk, including associated software, rather than allowing additional products to enter the Nation's communications infrastructure merely because an authorization was granted before the risk was identified. The Commission has also established a prospective mechanism that can restrict further importation and marketing without necessarily requiring the immediate removal of equipment already in service. EAS warrants at least the same precaution. An EAS product can receive, authenticate, process, modify, originate, suppress, and distribute emergency information. Compromise of that functionality could permit an adversary to block a valid warning, transmit false information, delay delivery, manipulate geographic targeting, or create a common point of failure across multiple Participants.

This recommendation supplements DAS's earlier proposal that EAS appliances and software be subject to SBOM, provenance, trusted signing and development, secure update, vulnerability disclosure, and continuing oversight requirements. The Covered List mechanism would provide an additional means of preventing the importation,

[12] FCC PSHSB & OET, PS Docket No. 26-184; DA 26-742; FR ID 359713, 6712-01, Seeking Comment on Prohibiting the Importation and Marketing of Certain Covered UAS and UAS Critical Components and Equipment Listed in Section 1709 of FY2025 NDAA.

marketing, activation, or updating of products that are later determined to present an unacceptable national-security risk.[13]

Accordingly, any rules authorizing software EAS should expressly prohibit the certification, importation, marketing, activation, or distribution of an EAS appliance, software product, critical component, firmware image, or update service produced or controlled by an entity on the Commission's Covered List, or otherwise determined by an authorized national-security agency to present an unacceptable risk. Certification applicants should be required to disclose the identity, ownership, and control of the product developer; the provenance of logic-bearing components and source code; the locations from which software is developed, signed, updated, or remotely administered; and any third parties capable of accessing or modifying the system. These protections should extend to white-labeled products and embedded or copied code, so that restricted equipment or software cannot enter the EAS ecosystem under another company's brand. The Commission is already considering comparable supply-chain transparency measures, including hardware and software bills of materials and restrictions involving Covered List components and software.

The Commission should also preserve an explicit mechanism to restrict the future importation, marketing, licensing, activation, and updating of previously certified EAS products if a later national-security determination identifies an unacceptable risk. That authority is especially important for software EAS, where a product may continue to be distributed electronically, activated remotely, or materially changed through updates without another physical device crossing the border. The Commission should not create a software-EAS pathway that is easier for foreign-controlled or opaque suppliers to enter than for the Commission to close. In a system established to protect life, property, and national defense, supply-chain eligibility must be addressed at certification, not after potentially compromised products have become embedded throughout the national warning infrastructure.

## 11 Market Impacts: Supplier Sustainability and National Resilience

The Commission asks how software authorization may affect EAS manufacturers. In this market, that question is tied directly to long-term public-warning reliability. DAS previously explained that the EAS equipment market is compliance-driven and that manufacturers must recover the costs of engineering, certification, regulatory updates, cybersecurity, interoperability, support, and backward compatibility from a limited customer base.[14] Software authorization does not alter those underlying economics. It changes how the finite replacement demand that supports those activities is divided among suppliers.

The EAS equipment market is small, specialized, and concentrated, driven largely by replacement demand. A change in the compliance pathway can therefore affect which suppliers can continue to provide engineering, certification, cybersecurity, regulatory updates, manufacturing, and field service.

The key economic distinction is that the proposal would not simply authorize a new way to serve new demand. It would change the competitive position of firms in an existing market. Federal OMB guidance recognizes that a

[13] Comments of Digital Alert Systems

[14] Comments of Digital Alert Systems

regulation can advantage some firms when its standards are easier for them to satisfy or reduce their costs disproportionately.[15]

### *11.1 The Market Is Small, Concentrated, and Replacement-Driven*

The significance of concentration is not that existing manufacturers should be insulated from competition. It is rather that a niche market supported by few suppliers and limited, finite replacement volume, has little room for another exit. The Commission identifies three manufacturers currently producing, marketing, servicing, and updating stand-alone EAS equipment, while another historical supplier no longer manufactures new units.

The degree of concentration is significant even without precise manufacturer market-share data. The Commission identifies only three firms currently manufacturing new stand-alone EAS encoder/decoder devices. Assuming, *solely for illustration*, equal shares among those three firms would produce an HHI of approximately 3,333. The Department of Justice and Federal Trade Commission identify markets above 1,800 as highly concentrated. Although the Merger Guidelines do not supply a legal standard for this proceeding, they provide a useful economic benchmark for understanding the existing market structure.[16] Software-based EAS will largely compete for the same replacement demand that supports appliance development and manufacturing. A supplier with a large installed base of aging or discontinued equipment may be able to retain those customers through software migration, while active appliance manufacturers lose sales used to recover fixed costs.

The scale of the replacement market also matters. Based on industry installed-base and useful-life estimates, DAS estimates that annual replacement opportunities constitute only a few thousand units across the entire national market. In a market of that size, migration of even a fraction of a large legacy installed base to a different compliance pathway could redirect hundreds of annual replacement opportunities. These figures are not forecasts of software adoption; they illustrate why seemingly modest shifts in compliance choices can materially affect the volume available to support competing product lines.This mechanism is consistent with established industrial-organization economics. Where suppliers incur continuing fixed and sunk costs, changes in the demand available to recover those costs can affect firm value, entry and exit decisions, and long-run market structure. Econometric research has found entry costs and incumbent fixed costs to be important determinants of firm turnover and market structure.[17]

The competitive effect will therefore depend on who is prepared to offer software and on whether software and appliance suppliers face genuinely equivalent certification, cybersecurity, lifecycle, and support obligations. A

---

[15] Office of Information and Regulatory Affairs, Office of Management and Budget. “OMB Guidance on Accounting for Competition Effects When Developing and Analyzing Regulatory Actions.” October 2023.

[16] See Modernization of the Nation’s Alerting Systems, Report and Order and Further Notice of Proposed Rulemaking, FCC 26-38, para. 102 & n.335 (2026) (identifying DAS, VIAVI Solutions, and Gorman-Redlich as the three manufacturers currently producing, marketing, servicing, and updating stand-alone EAS encoder/decoder devices, and noting that Sage no longer manufactures new devices); U.S. Dept. of Justice & Fed. Trade Commission, Merger Guidelines § 2.1 (Dec. 18, 2023) (identifying markets with an HHI greater than 1,800 as highly concentrated). The illustrative HHI assumes equal one-third shares and is offered simply as a measure of concentration.

[17] See Timothy Dunne, Shawn D. Klimek, Mark J. Roberts & Daniel Yi Xu, Entry, Exit, and the Determinants of Market Structure, 44 RAND J. Econ. 462, 462-487 (2013), doi:10.1111/1756-2171.12027.

lower-cost or narrower compliance pathway for software could increase concentration rather than expand durable competition. The Commission itself states that the certification requirements under consideration are intended to ensure regulatory parity between EAS software and stand-alone devices. Regulatory parity should encompass the substantive obligations and costs associated with certification, cybersecurity, interoperability, lifecycle support, inspection, and recovery, not merely the existence of a certification filing.[18]

The Commission should not treat software authorization as inherently pro-competitive. Nor does the present record establish that authorization will materially increase the number of sustainable EAS suppliers. The Commission's own Initial Regulatory Flexibility Analysis acknowledges that software-certification costs are difficult to estimate because the number of vendors that may seek to enter the market is unknown and the burdens faced by different vendors may differ.[19] In a market this small, even a moderate shift can significantly affect costs, internal investment, pricing, product availability, support capabilities, and ultimately a supplier's viability. Precise prediction of future market shares is neither possible nor necessary; OMB guidance expressly recognizes that important competition effects should still be evaluated when they cannot be fully quantified or monetized.[20]

### *11.2 Authorization Would Affect Suppliers Unevenly*

Software authorization would not affect all suppliers equally. Firms already positioned to offer software, especially those with a large installed base of aging or discontinued equipment, could migrate customers at a comparatively low incremental cost and avoid the manufacturing and supply-chain costs of a new appliance.

A manufacturer without a software product would face a different choice: fund a new development and certification program while continuing to support its appliance line, or compete for a smaller share of the replacement market. The new compliance pathway would therefore be immediately usable by some firms and either costly or impractical for others.

At the same time, migration to software would reduce appliance sales, through which manufacturers recover fixed costs for engineering, certification, regulatory updates, cybersecurity, interoperability, manufacturing, and support.

This is a recognized regulatory-economic concern. OMB guidance directs agencies to consider whether an action disproportionately raises or lowers the costs of some firms, changes firms' ability to compete, or favors one production method over another. OMB specifically cautions that regulating firms differently according to their method of production can alter competition and identifies performance-based regulation as one means of avoiding unnecessary competitive distortion.[21]

---

[18] FCC 26-38, para. 102 (stating that the contemplated certification requirements are intended to ensure "regulatory parity" between EAS software and stand-alone EAS encoder/decoder devices).

[19] OMB, Guidance on Accounting for Competition Effects, supra note 2, at 27-28 (addressing quantified-but-not-monetized, qualitative, break-even, threshold, and order-of-magnitude analysis).

[20] FCC 26-38, Initial Regulatory Flexibility Analysis, para. 8 (noting uncertainty concerning the number of software vendors and differing certification burdens they may face).

21 Office of Information and Regulatory Affairs, Office of Management and Budget, Guidance on Accounting for Competition Effects When Developing and Analyzing Regulatory Actions 12–15 (Oct. 2023) (directing agencies to consider whether regulatory actions disproportionately raise or lower costs for particular firms and discussing

The proposal is not competitively neutral merely because appliances would remain permitted. The disparity would be greater if software certification covers only a representative host or places material integration, security, and lifecycle responsibilities outside the vendor's certified product boundary.

Software-based EAS may also advantage software-ready suppliers and reduce the market available to firms that continue to invest in complete appliance systems. In a small market, that can influence which suppliers remain viable and whether Participants retain meaningful choices.

The Commission should not authorize software-based EAS under materially lighter certification, cybersecurity, interoperability, lifecycle, inspection, support, or recovery obligations than those applicable to full appliance-based implementations. Nor should it permit a software applicant to obtain certification for an application while shifting material compliance responsibilities and costs to the EAS Participant, host provider, signal-chain vendor, or other parties outside the certified product boundary. Such an approach would not be technology neutral; it would confer a regulatory cost advantage on one implementation form and distort competition in the existing replacement market.

### *11.3 Software Authorization Could Disadvantage Continued Investment in Certified EAS Equipment*

The competitive concern presented here is more specific than supplier concentration alone. EAS manufacturers have made different business and investment decisions in response to the same specialized and relatively small market. Some manufacturers have continued to invest in the development, certification, cybersecurity, component sourcing, manufacture, support, and evolution of complete EAS equipment. Others have ceased manufacturing new EAS devices. The Commission itself recognizes this distinction, noting that Sage no longer manufactures new EAS devices but continues to support its installed base.[22]

Software authorization could affect those suppliers very differently. software authorization would not merely facilitate entry by new competitors. It could provide an alternative means for a supplier that has exited new-equipment manufacturing to retain or migrate a substantial installed customer base without undertaking the engineering, component procurement, manufacturing, inventory, and supply-chain investment associated with developing a successor appliance.

At the same time, software migration would compete directly for the finite replacement demand that supports manufacturers that have continued to make those investments. An active equipment manufacturer must continue to recover the costs of engineering, certification, cybersecurity, interoperability, regulatory changes, manufacturing, component management, inventory, technical support, and long-term product maintenance. Those costs do not disappear simply because another supplier is permitted to satisfy Part 11 through a different implementation model. If the new pathway allows substantially lower costs or narrower certification and lifecycle

---

competitive effects of regulating firms differently according to production method). See also OMB Circular No. A-4, Regulatory Analysis 64–65 (Nov. 9, 2023) (directing agencies, where relevant, to account for changes in market power induced by regulation, including changes in entry barriers, switching costs, product quality, and incentives to innovate).

[22] FCC, Further Notice of Proposed Rulemaking, Released June 29, 2026,

obligations, the Commission could unintentionally place the manufacturer that continued to invest in complete certified EAS equipment at a competitive disadvantage to one that ceased doing so.

That result deserves particular scrutiny because the Commission's action would itself create the alternative compliance pathway. OMB guidance specifically directs agencies to consider whether regulatory actions disproportionately raise or lower the costs of particular firms and whether different regulatory treatment based on production methods may alter competitive conditions. The Commission therefore should not assume that permitting appliances and software side-by-side is necessarily competitively neutral. The relevant question is whether the requirements applicable to each approach impose genuinely comparable obligations for certification, cybersecurity, interoperability, lifecycle support, testing, recovery, and accountability.

This is not an argument that DAS, or any incumbent manufacturer, should be protected from competition. Competition should reward better products, lower costs, innovation, reliability, and service. The concern arises where regulatory design itself may alter the competitive balance by relieving one implementation model of costs and responsibilities that another must continue to bear. Particularly in a small compliance-driven market, the Commission should consider whether that result would discourage continued investment in complete EAS equipment and, over time, reduce rather than expand the range of viable EAS solutions available to Participants.

The consequences extend beyond individual manufacturers. Continued investment in multiple EAS architectures provides Participants with alternative suppliers, independent technical approaches, different supply chains, replacement options, and different responses to cybersecurity vulnerabilities or component failures. Federal supply-chain policy recognizes supplier diversity and reduced dependence on concentrated sources as elements of resilience. The Commission therefore should consider not only whether software authorization creates a new product option in the short term, but whether the regulatory structure supporting that option preserves incentives for continued investment across the EAS ecosystem over the longer term.

## 12 Conclusion

The Commission should not adopt a general authorization of EAS software unless its final rules establish an authorization model that preserves the public-safety assurances required by Part 11. The question is not whether software can perform individual EAS functions. Modern certified EAS equipment already relies extensively on software. The question is whether the Commission's rules require an implementation that distributes or relocates required EAS functions onto general-purpose hosts, shared platforms, or multiple signal-processing components to remain a defined, secure, resilient, inspectable, and accountable public-warning system.

The proposed rules do not establish that result. A software application, considered in isolation, is not the regulated object that receives, authenticates, processes, logs, and transmits emergency alerts. The relevant regulatory object is the complete EAS Implementation: the defined configuration that performs or directly controls required EAS functions, including the host environment and those interfaces, dependencies, security controls, update mechanisms, and recovery arrangements that materially affect Part 11 compliance. Unless the Commission can identify that complete implementation, reproduce the configuration that was tested, determine whether a deployed installation conforms to it, and assign responsibility when required functions fail, it has not established a certifiable or administrable authorization model.

Nor may those determinations rest on self-verification by an application developer, host-platform provider, or EAS Participant. EAS is mandatory public-warning infrastructure. A false, altered, delayed, suppressed, or unavailable

alert can affect not only the individual Participant but also downstream systems, public safety authorities, and the public. The Commission must therefore retain an FCC-administered or FCC-recognized independent certification and verification process for complete EAS Implementations. That process must provide an objective basis for authorization, field inspection, enforcement, corrective action, and ongoing accountability as software, hosts, dependencies, and operating conditions change over time.

Any authorization must also preserve the operational protections that make EAS dependable during emergencies and degraded conditions. Required monitoring, CAP processing, local alert processing, logging, independent fallback capability, and transmission functions must continue to operate when Internet connectivity, enterprise services, hosts, networks, or other external dependencies fail. The Commission likewise must require effective platform identity and integrity protections, authenticated and controlled updates, vulnerability and lifecycle management, defined support and recovery responsibilities, and a certification-impact review when a change materially affects the implementation. Remote monitoring, administration, support, reporting, and update distribution may be useful ancillary capabilities; they must not become unexamined dependencies for the performance of mandatory EAS functions.

The Commission should reject the premise that presumed flexibility, reduced rack space, or asserted cost savings establishes equivalent public-warning assurance. Functional equivalence is not system equivalence. A software pathway that certifies only an application while externalizing material cybersecurity, integration, lifecycle, support, and failure responsibilities to the Participant or other third parties would not be technology neutral. It would weaken accountability, complicate inspection and enforcement, distort competition among suppliers subject to different regulatory burdens, and risk replacing diverse, bounded implementations with common proprietary or platform-dependent failure points. The Commission must also ensure that any EAS authorization addresses intellectual property dependencies, supply chain transparency, trusted development and signing, foreign control risks, and the long-term sustainability of the specialized supplier base on which EAS Participants depend.

DAS therefore urges the Commission not to adopt a general EAS software authorization under the proposed application-centric framework. The Commission should instead resolve the threshold issues identified in these comments by adopting rules that define the complete EAS Implementation, establish its certification boundary, require independent certification and field-verifiable conformity, preserve local and resilient operation, control material changes, and assign responsibility throughout the implementation's operating life. If the Commission concludes that those requirements cannot be adequately established in this proceeding, it may use a focused further notice, a technical workshop, a laboratory evaluation, a controlled field trial, a waiver process, or another mechanism to refine them. Modernization should strengthen the Nation's public-warning infrastructure—not transform mandatory EAS compliance into a shifting collection of arbitrary hosts, proprietary interfaces, external dependencies, and divided responsibility.