

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of

Wireless Emergency Alerts

The Emergency Alert System

Modernization of the Nation's Alerting Systems

PS Docket No. 15-91

PS Docket No. 15-94

PS Docket No. 25-224

REPLY COMMENTS OF GATEWELL GROUP LLC

Filed in reply to comments on the Further Notice of Proposed Rulemaking, FCC 26-38, published at 91 Fed. Reg. 48320 (July 31, 2026).

I. Introduction and Statement of Interest

This reply addresses paragraph 112 of the Further Notice and its two questions, which are what evidence a certification application for EAS software should carry and whether foreign-produced EAS software should be prohibited on Covered List grounds. As in its opening comment, "Gatewell addresses only how the facts those two questions depend on can be established and documented." Comments of Gatewell Group LLC, PS Docket Nos. 25-224, 15-94, 15-91, § I (filed Aug. 24, 2026) (ECFS No. 26110072735) (Gatewell Comments). Gatewell takes no position on the cybersecurity standards or test procedures against which EAS software should be assessed, or on any question of alerting policy.

Gatewell's interest is commercial. Gatewell Group LLC advises buyers and manufacturers on Covered List exposure and origin evidence. It publishes the Gatewell Protocol for Origin Evidence, an open documentation standard for the evidence file behind a not-covered certification. Gatewell sells services assembling and verifying files

under that standard. Gatewell does not ask the Commission to adopt or endorse that standard. Nothing recommended below would require a certification applicant to retain Gatewell or any other party.

II. Summary of Recommendation

Gatewell asks the Commission to take the following five steps.

1. State which population § 2.902 supplies to paragraph 112.
2. Place the documentation requirement in § 11.34 as proposed in Appendix B rather than in Part 2.
3. Require the certifying party to hold and produce a provenance record covering the four roles, the ownership and control of each entity under § 2.902, and the testing facility.
4. Require independent confirmation of the three entries that carry access to a running installation.
5. Extend the § 2.911(d)(5) certification to each entity in that record and require screening against the Covered List and the § 1.50002 designations on a stated cycle and on change.

III. The Rules That Govern Paragraph 112's Two Questions

Paragraph 112 opens with the process question.

> "Should a Declaration of Conformity with specific standards or best practices, a cybersecurity audit or test report, or other evidence be required to be included in the EAS software's certification application?"

FCC 26-38 ¶ 112, at 60. The Commission's footnote states what that instrument is. "In general, a Declaration of Conformity is an attestation from the responsible party that the equipment or software has been shown to comply with the applicable technical standards and other applicable requirements of the conformity assessment regime against which it is being issued." Id. at 60 n.363. An attestation states a conclusion without the facts on which it rests.

The paragraph closes with the supply-chain question.

> "Should foreign-produced EAS software be subject to importation and use prohibitions where national security is implicated, for example, where the software designer, manufacturer, or responsible party for certification is on the Covered List?"

Id. ¶ 112, at 61. Its footnote reads in full, "See, e.g., 47 CFR § 2.902." Id. at 61 n.366.

Paragraph 112's text says Covered List. Its footnote points to § 2.902, whose defined term "Prohibited entities" reaches the Covered List, entities identified by six further sources, and entities Commerce identifies as "foreign adversaries." The same section's ownership test runs to "10% or more equity, voting interest, or stock." 47 CFR § 2.902. Gatewell asks the Commission to identify which population paragraph 112 intends.

The application-stage instrument that exists today speaks to one entity. Section 2.911(d)(5) requires "a written and signed certification" that the equipment "is not prohibited from receiving an equipment authorization pursuant to § 2.903" and "An affirmative or negative statement as to whether the applicant is identified on the Covered List, established pursuant to § 1.50002 of this chapter, as an entity producing covered communications equipment." 47 CFR § 2.911(d)(5). Paragraph 112 asks about three roles, while § 2.911(d)(5) requires a statement only from the applicant.

Proposed § 11.34 in Appendix B is where EAS software enters the Part 2 certification process. Proposed § 11.34(a) requires certification "in accordance with the procedures in part 2, subpart J, of this chapter," "with the exception that the requirement to demonstrate compliance with part 15 shall not apply to EAS Software," and proposed § 11.34(c) allows the combined functions to be "Certified as a single unit or as EAS Software defined in § 11.2(e)." FCC 26-38, App. B, at 80. It adds no Covered List, provenance, or responsible-party language anywhere in the proposed text.

The comments answered below were filed on August 31, 2026. Eleven days later, in *Protecting Against National Security Threats to the Communications Supply Chain Through the Equipment Authorization Program*, 91 Fed. Reg. 57798 (Sept. 11, 2026) (FR Doc. 2026-18535) (FCC 26-50, ET Docket No. 21-232), effective October 13, 2026, the Commission adopted a component-level prohibition and drew its boundary.

> "The Commission also declines to extend the prohibition to software or firmware components at this time."

Id. at 57799. The prohibition reaches a device that incorporates a "logic-bearing hardware component produced by an entity identified on the Covered List," a term the same publication defines as a "physical component." Id. at 57801 (new 47 CFR §§ 2.903(b)(2), 2.902). Two consequences follow. Part 2's component prohibition does not reach software or firmware components, so a prohibition on Covered-List-produced EAS software cannot be built on it. Part 2 does reach the equipment or software that is itself the subject of the authorization, because § 2.903(a) prohibits "All equipment on the Covered List, as established pursuant to § 1.50002 of this chapter," from obtaining an authorization under subpart J.

IV. The Evidentiary Content of an EAS Software Certification Application

The gap that paragraph 112 identifies is documentary. Gatewell asks the Commission to state the evidentiary content in three levels and to name the party who answers for it.

A. Level one, the record of the entities behind the software

The application should attach the record of entities on which the certification rests. Gatewell asked in the opening round that the record state the legal name, jurisdiction of organization, and principal place of business of each entity that directs the development of the software and controls its source, builds the binary that is distributed, holds the code-signing key with which the release is signed, and operates the channel through which EAS Participants receive releases and updates. Gatewell Comments § II. For each of those entities the record should state who owns, controls, or directs it under the test in § 2.902, and it should carry the identity and location of the testing facility, which § 2.906(a)(1) already makes relevant. Id.; 47 CFR § 2.906(a)(1). Extending the § 2.911(d)(5) certification to each entity named in that record, and refreshing it on the model of § 2.911(d)(6), would bring § 2.911(d)(5) into line with the question paragraph 112 asks. The answer would then appear on the record at grant.

B. Level two, independent confirmation for the elements that carry access

Statements in the record that no one confirms leave the same evidentiary gap the record is meant to close. Digital Alert Systems states that "Security requirements have limited

value if compliance is established only through manufacturer assertion," asks for "appropriate independent testing or verification as part of certification," and, in its companion filing, for an "independent certification and verification process, rather than supplier self-verification." Comments of Digital Alert Systems, PS Docket No. 25-224 (filed Aug. 31, 2026) (ECFS Nos. 26110074056, at 18 (DAS Part I Comments), and 26110074061, at 6 (DAS Part II Comments)). Confirmation should attach to the entries that carry access to a running EAS installation, which are the holder of the code-signing key, the operator of the build environment, and the operator of the update and remote administration channel. A false entry in any of the three changes what reaches an EAS Participant's equipment. This level concerns who verifies three entries in the provenance record. It does not touch the standards against which the software is tested.

C. Level three, screening on a stated cycle

The designations enumerated in § 2.902 and the entries on the Covered List change after a certification is granted. Ownership or control of a developer can change with nothing changing in the software. A change in any of the four roles, or in ownership or control of any of them under § 2.902, should itself require the grantee to refresh the provenance record and the § 2.911(d)(5) certification and file them with the TCB. Gatewell Comments § VI. Screening should run against the Covered List and the § 1.50002 designations on a stated cycle and on change, with the date of each inquiry recorded.

D. Naming a responsible party for software in Part 11

Section 2.909 identifies a responsible party only in terms drawn from hardware. It provides that "the party to whom that grant of certification is issued is responsible for the compliance of the equipment," and it assigns responsibility under the Supplier's Declaration of Conformity through roles drawn from goods, among them the manufacturer, the assembler, the importer, the retailer, and the party performing a modification. 47 CFR § 2.909(a), (b). The Further Notice cites the section once, for the proposition that the responsible party is "typically the manufacturer." FCC 26-38 at 56 & n.342. None of those roles describes an entity that signs a release or hosts an update channel. Gatewell asks the Commission to define these roles for software in rule text, as follows. A designer is the entity that directs the development of the software and controls its source. A manufacturer is the entity that builds the binary that is distributed

to EAS Participants. The grantee under § 2.909(a) would be required to identify both and in every case the holder of the code-signing key. Gatewell Comments § III.

The requirement belongs in Part 11. Amending Part 2 to reach software would reopen a question the Commission has just declined to decide. Section 11.34 as proposed needs no such reopening. A documentation requirement placed in § 11.34 would state what the certifying party holds and produces on request, would leave Part 2's prohibitions unchanged, and would give the Commission the record on which § 2.903(a) is applied at the point of application.

V. The Opening Comments

Based on the comments in ECFS in PS Docket No. 25-224 as of September 18, 2026, three reach paragraph 112. Two filings in the round name the Covered List, both from Digital Alert Systems. No filing in the round uses the term "prohibited entities," and none cites § 2.902 or § 1.50002.

A. Digital Alert Systems' disclosure proposal and the prohibition it attaches

DAS proposes the disclosure Gatewell proposed in the opening round. It would require applicants "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," and would extend the protections "to white-labeled products and embedded or copied code." DAS Part II Comments at 27. Gatewell supports that list. Section IV adds who confirms the entries and when they are refreshed.

Gatewell does not join the prohibition DAS proposes. DAS asks that rules "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" Id. Three problems attend that framing. First, the component route is closed for the reason stated in Section III. Second, the importation route does not fit the facts, as DAS states when it observes that a software product "may continue to be distributed electronically, activated remotely, or materially changed through updates without another physical

device crossing the border." DAS Part II Comments at 27. Third, "produced or controlled by" is neither the Covered List's term nor the population § 2.902 defines.

For software, the regulable events are the certification application and the use. Section 2.903(a) reaches the application, proposed § 11.34(a) and (c) carry EAS software into it, and an EAS Participant is already subject to Part 11. Neither depends on importation.

B. NAB's self-certification proposal and §§ 2.906(d) and 2.907(c)

NAB would leave the showing to the vendor. "As under current practice, the FCC should rely on EAS software providers to follow reasonable cybersecurity best practices and self-certify the security of their product." Comments of the National Association of Broadcasters, PS Docket No. 25-224, at 13 (filed Aug. 31, 2026) (ECFS No. 26110073927). It adds that "We see no reason that part 2 of the rules cannot be applied to EAS software, with a few minor changes." *Id.* at 9.

Current practice does not rely on self-attestation for the entities paragraph 112's closing sentence names. Equipment "otherwise subject to the Supplier's Declaration of Conformity process that is produced by any entity identified on the Covered List . . . is prohibited from obtaining equipment authorization through that process," and must instead "obtain equipment authorization through the certification process." 47 CFR §§ 2.906(d), 2.907(c); see DAS Part I Comments at 18 n.18. NAB does not address that sentence and does not use the term Covered List. NAB's comment therefore does not reach the supply-chain question in paragraph 112's closing sentence.

C. ACA Connects' Part 11 alternative

ACA Connects would keep Part 2 away from software-only EAS. "The Commission should also not extend the Part 2 equipment certification process to software-only EAS." Comments of ACA Connects, PS Docket No. 25-224, at 5 (filed Aug. 31, 2026) (ECFS No. 26110074010). Its alternative is the existing Part 11 requirements "together with vendor testing and documentation." *Id.* at 5-6.

The closing sentence of paragraph 112 can be answered in Part 11, where the obligations on EAS Participants already apply. ACA Connects identifies Part 11 without stating what Part 11 would require. Section IV states that content. It adds no regime beyond the certification Appendix B already proposes.

VI. Conclusion

Gatewell asks the Commission to answer paragraph 112 in § 11.34 as proposed in Appendix B. The certifying party would hold, and produce on request, a record identifying the entities that develop, build, sign, update, and remotely administer the software, their ownership and control under the test in § 2.902, and the testing facility. The five steps set out in Section II state the recommendation in full.

Respectfully submitted,

/s/ Ilya Tsimerinov

Ilya Tsimerinov

Principal

Gatewell Group LLC

811 W 7th Street, Suite 900

Los Angeles, California 90017

inquiries@gatewellgroup.com

September 19, 2026