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

In the Matter of

Modernization of the Nation's Alerting Systems

PS Docket No. 25-224

Amendment of Part 11 of the Commission's Rules Regarding the Emergency Alert System

PS Docket No. 15-94

Wireless Emergency Alerts

PS Docket No. 15-91

COMMENTS OF GATEWELL GROUP LLC

Filed in response to the Further Notice of Proposed Rulemaking, FCC 26-38, adopted June 25, 2026, released June 29, 2026, published at 91 Fed. Reg. 48320 (July 31, 2026). Comments are due on or before August 31, 2026; reply comments are due on or before September 29, 2026.

I. Introduction and Statement of Interest

Gatewell Group LLC is a Los Angeles consultancy. It sells advisory services on Covered List exposure and origin evidence to importers, distributors, engineering and construction contractors, project developers, and network operators. If the Commission requires applicants for EAS software certification to document who produced the software and whether any of them is a prohibited entity, Gatewell expects to advise clients on assembling that documentation, and it therefore has a commercial interest in what the rule requires. Gatewell is not an EAS Participant, is not a manufacturer or developer of EAS equipment or software, holds no equipment authorization, and has no product whose authorization status is at stake in this proceeding.

Gatewell has filed five comments in four related Commission proceedings: ECFS 26110071980 and 26110071982 in PS Docket 26-184 and ECFS 26110071981 in PS Docket 26-189, disseminated August 18, 2026; and ECFS 26110072507 in ET Docket 21-232 and ECFS 26110072506 in ET Docket 26-22, disseminated August 21, 2026.

These comments address one paragraph of the Further Notice. Paragraph 112 proposes that "before EAS software can be marketed or used, the responsible party seeking its certification should be required to demonstrate to the Commission that it has taken appropriate steps to secure the software," and asks: "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?" The paragraph closes with a second 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? See, e.g., 47 CFR § 2.902."

Gatewell addresses only how the facts those two questions depend on can be established and documented. It takes no position on whether EAS software should be certified, on which conformity assessment framework should apply, on test procedures or test laboratories (paragraphs 106 through 110), on which cybersecurity standard or program the Commission should adopt, on message authentication, on operational readiness, or on any question of alerting policy.

II. The two questions in paragraph 112 are different kinds of questions, and a Declaration of Conformity answers only one of them

Paragraph 112 describes a Declaration of Conformity as "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." Section 2.906(a) defines the Supplier's Declaration of Conformity as "a procedure where the responsible party, as defined in § 2.909, makes measurements or completes other procedures found acceptable to the Commission to ensure that the equipment complies with the appropriate technical standards and other applicable requirements." In both formulations the declarant is the party whose compliance is at issue. That is the instrument's design, not a defect in it.

The first question in paragraph 112 is a process question: whether the developer followed a secure development practice, against a named standard or program. The developer is the only party that holds the facts. A signed declaration against a specified standard is the proportionate instrument for that question, and an audit or test report adds a second witness where the Commission wants one. Gatewell takes no position on which standard or program should be named.

The second question is a provenance question: who designed, produced, and is responsible for the software, and whether any of them is on the Covered List. A Declaration of Conformity answers that question by asking the party whose provenance is in question to attest to its own provenance. The Commission's rules already treat this question as one that self-attestation does not settle. Section 2.906(d) provides that "equipment otherwise subject to the Supplier's Declaration of Conformity process that is produced by any entity identified on the Covered List, established pursuant to § 1.50002 of this chapter, is prohibited from obtaining equipment authorization through that process. The rules in this chapter governing certification apply to authorization of such equipment." Section 2.907(c) says the same from the certification side. Certification, under § 2.907(a), is "an equipment authorization approved by the Commission or issued by a Telecommunication Certification Body (TCB) and authorized under the authority of the Commission, based on representations and test data submitted by the applicant." Where the Covered List is in play, the rules move the applicant from its own declaration to a record that a third party reviews.

Inside the certification process, the Covered List question is then handled by a specific signed certification. Section 2.911(d)(5) requires "a written and signed certification that, as of the date of the filing of the application with a TCB: (i) The equipment for which the applicant seeks equipment authorization through certification is not prohibited from receiving an equipment authorization pursuant to § 2.903; and (ii) 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." Section 2.911(d)(6) requires a fresh certification if the Covered List is modified between the certification and the grant. Two features of that certification matter here. It establishes the applicant's own status and the applicant's conclusion about the equipment. It does not attach the facts from which the conclusion was drawn — who produced the equipment at each stage of its production — and so

gives the TCB nothing to test the conclusion against. For hardware, the TCB has what § 2.911(c) requires with the application: test data, diagrams, and photographs of an identified device, from which it can see what was built and where it was tested. For software, it has a file and a signature.

Recommendation. For the process question, accept a Declaration of Conformity against whatever standard the Commission names. For the provenance question, require the application to attach a record rather than a conclusion: (1) the legal name, jurisdiction of organization, and principal place of business of each entity that (a) directs the development of the software and controls its source, (b) builds the binary that is distributed, (c) holds the code-signing key with which the release is signed, and (d) operates the channel through which EAS Participants receive releases and updates; (2) for each such entity, a statement identifying any entity that owns, controls, or directs it under the test in § 2.902; (3) the certification required by § 2.911(d)(5), extended to state whether any entity identified under (1) or (2) is on the Covered List; and (4) the identity and location of the facility at which compliance testing was performed, which § 2.906(a)(1) already makes a fact the rules care about by providing that testing "must not be performed at a measurement facility that is owned by, controlled by, or under the direction of a prohibited entity, as defined in § 2.902." A record of this kind can be checked by a TCB against public registries and signing infrastructure. A declaration cannot.

III. Paragraph 112 names three roles, and Part 2 defines the responsible party only through physical-goods roles

The second question names "the software designer, manufacturer, or responsible party for certification." Of the three, only the last is defined in the rules, and it is defined for objects.

Under § 2.909(a), for equipment that requires certification, the responsible party is "the party to whom that grant of certification is issued." Under § 2.909(b), for equipment subject to a Supplier's Declaration of Conformity, the responsible party is "the manufacturer or, if the equipment is assembled from individual component parts and the resulting system is subject to authorization under Supplier's Declaration of Conformity, the assembler"; the importer, if the equipment is imported; a retailer or original equipment manufacturer that agrees to assume the role; and, under § 2.909(b)

(4), "[i]f the radio frequency equipment is modified by any party not working under the authority of the responsible party, the party performing the modifications, if located within the U.S., or the importer, if the equipment is imported subsequent to the modifications, becomes the new responsible party." Each of these roles is a physical-goods role. Software has no assembler in the sense of § 2.909(b)(1). Software delivered electronically has no importer. And modification of software is not an event but a stream: each update by a party outside the grantee's authority would, on a literal reading of § 2.909(b)(4), transfer the responsible-party role. The permissive-change rule points the same way. Section 2.1043(a) provides that "[c]hanges to the software installed in a transmitter that do not affect the radio frequency emissions do not require any additional filings and may be made by parties other than the holder of the grant of certification." Applied to a product that is entirely software, that sentence permits the thing the Commission is asking about to change hands without a record.

"Designer" and "manufacturer" are not defined at all. The operative concept in the Covered List rules is "produced." Section 1.50002(b)(1) reaches equipment that "[i]s produced or provided by any entity" subject to the listed determinations, and the Commission has said that "produced by" is to be read broadly: it "likely includes substantial responsibility for or control over any major stage of the process by which a device comes into existence," and "'produced by' is not limited to the manufacture or assembly of a device." Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program, ET Docket No. 21-232, Second Report and Order and Second Further Notice of Proposed Rulemaking, 40 FCC Rcd 8430, 8456-57, paras. 51-53 (2025). For software, the major stages by which the product comes into existence are authoring and controlling the source, building the binary, signing the release, and distributing it. These are routinely performed by different entities in different jurisdictions, and a contract developer, a build service, a signing-key custodian, and a distribution platform can each be a different company from the one whose name is on the application.

Recommendation. The Commission should define the three roles for EAS software in rule text: "designer" as the entity that directs the development of the software and controls its source; "manufacturer" as the entity that builds the binary that is distributed to EAS Participants; and "responsible party for certification" as the grantee under § 2.909(a). It should require the grantee to identify the designer and the manufacturer

where they are not the grantee, and to identify in every case the holder of the code-signing key, because a signature is the one provenance fact an EAS Participant can verify on its own system against a published key. The code-signing key holder and the operator of the build environment are the two roles that leave verifiable records — a signature verifies or it does not, and a build produces an artifact with a recorded origin — and the rule should anchor on them rather than on terms borrowed from hardware.

IV. An "importation prohibition" has no operative trigger for software delivered electronically

Paragraph 112 asks whether foreign-produced EAS software should be subject to "importation and use prohibitions." The importation rules in Part 2, Subpart K, are built on physical entry. Section 2.1201(b) states that the subpart sets out "the conditions under which radio frequency devices as defined in § 2.801 that are capable of causing harmful interference to radio communications may be imported into the U.S.A." Section 2.1203(a) provides that "[n]o radio frequency device may be imported into the Customs territory of the United States unless the importer or ultimate consignee, or their designated customs broker, determines that the device meets one of the conditions for entry set out in § 2.1204," the first of which, in § 2.1204(a)(1), is a valid equipment authorization. Section 2.1203(c) requires "[w]hoever makes a determination pursuant to § 2.1203(a)" to produce, on request made within one year of entry, "documentation on how an imported radio frequency device was determined to be in compliance with Commission requirements." Section 2.1202(d) excludes from the subpart "[s]ubassemblies, parts, or components of radio frequency devices" short of an essentially completed device.

Every hook in that structure is a customs event involving a device: entry into the Customs territory, an importer or ultimate consignee, a broker's determination, and documentation tied to the date of entry. Software transmitted electronically produces none of them. There is no entry, no importer of record, no determination under § 2.1203(a), and no date of entry from which the one-year documentation period could run. An importation prohibition written for EAS software would describe a transaction the rules cannot see and would give the Commission nothing to enforce against.

Recommendation. If the Commission adopts a prohibition for EAS software produced by a Covered List entity, it should anchor the prohibition on events that exist

for software. The first is the application: § 2.903(a) already prohibits equipment on the Covered List from obtaining an equipment authorization, and § 11.34(a) through (c) already condition EAS encoders and decoders on certification under Part 2, Subpart J, so a certification requirement for EAS software carries the prohibition into software at the point of application without new importation language. The second is use: a Part 11 obligation on the EAS Participant not to use EAS software that has no certification, or whose certification has been cancelled, is enforceable because the Participant is already subject to Part 11 and already keeps the operational records that § 11.35 requires. If the Commission also wants a marketing prohibition, the event should be the first offer or delivery of the software to an EAS Participant in the United States, with the grantee as the accountable party. The word "importation" should not be used for software at all.

V. The question cites § 2.902 but names only the Covered List; the rule defines a wider population and an ownership test that no distribution channel surfaces

The second question asks about software whose designer, manufacturer, or responsible party "is on the Covered List," and cites § 2.902. Section 2.902 defines "prohibited entities" as each entity on the Covered List under § 1.50002 and, in addition, entities identified on the Department of Commerce Entity List and Military End-User List, the Department of Homeland Security UFLPA Entity List, the lists maintained under section 5949 of the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023 and section 1260H of the National Defense Authorization Act for Fiscal Year 2021, the Department of the Treasury Non-SDN Chinese Military-Industrial Complex Companies List, and entities identified as "foreign adversaries" by the Department of Commerce under 15 CFR 791.4. Section 2.902 also defines "owned by, controlled by, or subject to the direction of" to reach any entity in which another entity "has direct or indirect ownership or control of 10% or more equity, voting interest, or stock," any entity another entity has the power to direct on important matters, and any entity acting as another's agent or under its supervision or financing.

The question as posed and the rule it cites describe materially different populations. They also differ in what has to be proved. Membership on a list is a lookup. The ownership test is a tracing exercise through holding structures, and nothing in the way software reaches an EAS Participant — a download, a signature, a license key — surfaces

who holds 10% of the vendor or of the vendor's build contractor. The rules already apply the § 2.902 definition in the conformity assessment setting, through § 2.906(a)(1)'s restriction on test facilities, so the Commission has a working precedent for either choice.

Recommendation. The Commission should state expressly whether the prohibition it is considering for EAS software uses the Covered List alone or the "prohibited entities" population defined in § 2.902. Whichever it chooses, the record required under Part II above should include, for each of the four roles, a statement of ownership and control at the 10% threshold in § 2.902, so that the answer to the ownership question is documented at the time of application rather than inferred from a company name.

VI. Provenance changes with each release; the recertification question in paragraph 110 should carry the provenance record with it

Paragraph 110 asks "what modifications, if any, to EAS software — and by extension, EAS performance — should require resubmission of certification information," and "whether software is sufficiently different from physical hardware that it should require a periodic recertification throughout its life cycle." Gatewell takes no position on the functional triggers. It notes one consequence of Parts II and III for whatever triggers the Commission adopts. A change in any of the four provenance roles — the entity controlling the source, the entity building the binary, the holder of the signing key, or the operator of the distribution channel — or a change in the ownership of any of them, changes the answer to the Covered List question without changing a line of code that an EAS Participant can see. The rules already recognize the principle for the list itself: § 2.911(d)(6) requires a new certification when the Covered List changes between certification and grant.

Recommendation. A change in any of the four provenance roles, or in the 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, on the model of § 2.911(d)(6). A change of the code-signing key should additionally require notice to EAS Participants, because a Participant that verifies signatures will otherwise see a valid update from an unrecognized key and have no way to know whether that is a key rotation or a change of producer.

VII. Conclusion

Gatewell asks the Commission to specify in rule text, rather than in accompanying discussion, how the two questions in paragraph 112 are to be answered:

1. A Declaration of Conformity for the secure-development question, and an attached provenance record, not a declaration, for the Covered List question: the identity, jurisdiction, and ownership of the entity controlling the source, the entity building the binary, the holder of the code-signing key, and the operator of the distribution channel, together with the certification required by § 2.911(d)(5) extended to each of them and the location of the test facility.

2. Definitions of "designer," "manufacturer," and "responsible party for certification" for EAS software, anchored on the code-signing key holder and the build-environment operator as the roles that leave verifiable records.

3. No importation prohibition for software. A prohibition anchored on the application under § 2.903 and on use by the EAS Participant under Part 11, with the first offer or delivery to an EAS Participant in the United States as the marketing event if one is adopted.

4. An express statement of whether the prohibition uses the Covered List or the § 2.902 "prohibited entities" population, with the § 2.902 ownership statement required at application in either case.

5. A refresh of the provenance record and the § 2.911(d)(5) certification on any change in the four provenance roles or their ownership, and notice to EAS Participants on any change of the code-signing key.

Respectfully submitted,

/s/ Ilya Tsimerinov

Ilya Tsimerinov

Principal

Gatewell Group LLC

811 W 7th Street, Suite 900

Los Angeles, California 90017

inquiries@gatewellgroup.com

August 22, 2026