Federal Communications Commission
Washington, DC 20554

August 3, 2026

DA 26-811

SMALL ENTITY COMPLIANCE GUIDE

Facilitating Implementation of Next Generation 911 Services (NG911); Improving 911 Reliability

FCC 26-39
PS Docket Nos. 21-479, 13-75
Released June 26, 2026

In accordance with Section 212 of the Small Business Regulatory Enforcement Fairness Act of 1996, this Small Entity Compliance Guide (Guide) is intended to help small entities—small businesses, small organizations (non-profits), and small governmental jurisdictions—comply with the rules adopted in the above-referenced Federal Communications Commission (FCC or Commission) rulemaking dockets. This Guide is not intended to replace or supersede these rules, but to facilitate compliance with the rules. Although we have attempted to cover all parts of the rules that might be especially important to small entities, the coverage may not be exhaustive. This Guide cannot anticipate all situations in which the rules apply. Furthermore, the Commission retains the discretion to adopt case-by-case approaches, where appropriate, that may differ from this Guide. Any decision regarding a particular small entity will be based on the statute and any relevant rules.

In any civil or administrative action against a small entity for a violation of rules, the content of the Guide may be considered as evidence of the reasonableness or appropriateness of proposed fines, penalties or damages. Interested parties are free to file comments regarding this Guide in the above referenced docket and the appropriateness of its application to a particular situation. The Commission will then consider whether the recommendations or interpretations in the Guide are appropriate in that situation. The Commission may decide to revise this Guide without public notice to reflect changes in its approach to implementing a rule, or it may clarify or update the text of the Guide. Please direct comments and recommendations, or requests for further assistance, to the FCC's Consumer Center:

1-888-CALL-FCC (1-888-225-5322)

Videophone: 1-844-4-FCC-ASL (1-844-432-2275)

Fax: 1-866-418-0232

TABLE OF CONTENTS

I. OBJECTIVES OF THE PROCEEDING

The June 2026 NG911 Reliability *Order*[1] modernizes the Federal Communications Commission's (Commission or FCC) 911 reliability rules to strengthen the resiliency of NG911 networks. It also promotes NG911 network interoperability between states, while significantly reducing regulatory burdens on covered 911 service providers. The *Order* updates the Commission's 911 reliability rules, originally adopted in 2013 and focused on legacy 911 network components and their equivalents, for IP-based NG911 networks and environments. The *Order* leaves the substantive requirements for providers of legacy 911 networks intact with only minor revisions for streamlining, reorganization, and regulatory efficiency, and for reducing the compliance burden of annual certification filings, as discussed below.

As a result of the *Order*, reliability requirements will apply to new categories of covered 911 service providers whose operations are essential to NG911 call delivery and whose failure could cause significant outages. Internet Protocol (IP) service providers that control or operate critical pathways and components in NG911 networks and systems. The 911 network reliability benchmarks applicable to covered 911 service providers also now include best practices that are appropriate to IP-based networks. These benchmarks incorporate well-established IP best practices in the areas of physical diversity, operational integrity, and network monitoring. To support the seamless transfer of 911 calls and associated data across the NG911 ecosystem, the Commission requires Emergency Services IP Network (ESInet) providers and Next Generation Core Services (NGCS) covered 911 service providers to report on their recent actions to enable interstate NG911 interoperability. All covered 911 service providers will file a one-time certification with the Commission, to be updated only as needed in the event of material changes. Covered 911 service providers who have not previously filed a reliability certification will also be required to submit a one-time attestation. This streamlined process replaces the requirement for covered 911 service providers to annually file compliance certifications. Statewide, territorial, and tribal 911 Authorities may request reliability information directly from covered 911 service providers, subject to appropriate confidentiality protections, in order to improve state and local oversight during the NG911 transition.

These rules are intended to improve NG911 network reliability and interoperability to prevent outages and service disruptions and improve coordination between 911 Authorities and covered 911 service providers during the NG911 transition. The rules will also benefit small businesses that originate customer 911 calls by ensuring those calls connect to first responders in NG911 systems regardless of how many intermediary third-party networks the calls must traverse. Improving 911 reliability produces significant benefits for public safety emergency response and therefore advances the Commission's statutory charge to promote the safety of life and property through the use of wire and radio communications.

II. COMPLIANCE REQUIREMENTS

The 911 reliability compliance requirements are codified at 47 CFR § 9.19 in part 9, subpart H of the FCC's rules.

Providing Reliable 911 Service – 47 CFR § 9.19

Covered 911 Service Providers and Covered 911 Services.

> Covered 911 Service Providers (CSPs) are required to implement certain measures under the 911 reliability rules. CSPs are entities that provide covered 911 services, which are 911, E911, or NG911 services for which a failure would impede the real-time routing, delivery, or transfer of 911 traffic. Covered 911 services include:

[1] *Facilitating Implementation of Next Generation 911 Services (NG911) et. al*, PS Docket Nos. 21-479 and 13-75, Second Report and Order, FCC 26-39, 2026 WL 2018708 (June 26, 2026) (*Order*).

- Providing 911, E911, or NG911 capabilities, including call routing, automatic location information (ALI), automatic number identification (ANI), or the functional equivalent of those capabilities, directly to a public safety answering point (PSAP); the operation of central office(s) that directly serve a PSAP, meaning the central office hosts a selective router or ALI/ANI database or equivalent NG911 capabilities, or is the last service-provider facility through which a 911 trunk or administrative line passes before connecting to a PSAP;
- Providing Next Generation Core Services (NGCS) facilities, including NGCS location facilities or NGCS routing facilities, directly by contract or tariffed service to any 911 Authority, whether via owned and operated facilities or leased or contracted facilities;
- Operating an ESInet or legacy PSAP gateway (LPG);
- Operating a Location Information Server (LIS) or equivalent IP 911 location database that provides service to two or more originating service providers (OSPs);
- Operating a Legacy Network Gateway (LNG), a legacy selective router gateway (LSRG), or an emergency services gateway (ESGW) used for IP conversion of 911 traffic, that provides service to two or more OSPs;
- Operating a major IP transport facility, which are dedicated Session Initiation Protocol (SIP) transport facilities that include voice and text transport, when those facilities meet or exceed Optical Carrier 48 (OC48) or 2.5 Gbps in capacity, and collect and/or transmit IP 911 traffic mixed with non-911 traffic originated from two or more OSPs (excluding the provider's own OSP traffic) for transport over interstate routes for ultimate delivery to an NG911 Delivery Point or equivalent ESInet point of interconnection.
- Operating a IP 911 traffic aggregation facility, which is a facility that collects and segregates IP 911 traffic from non-911 traffic for two or more OSPs (excluding the provider's own OSP traffic), or transports such 911-only traffic for ultimate delivery to an NG911 Delivery Point or equivalent ESInet point of interconnection; or
- Operating interstate interconnecting ESInet facilities, which are interstate facilities that transport IP 911 traffic from an ESInet for ultimate delivery to another ESInet, including facilities designated for occasional or backup exchange of IP 911 traffic between ESInets.

The following entities are not CSPs: PSAPs, 911 Authorities, or other governmental authorities providing 911, E911, or NG911 capabilities; or OSPs that allow customers to originate 911 calls, but use another provider or network to deliver those calls and associated information to the appropriate 911 Authority.

Providing Reliable 911 Service.

CSPs must take reasonable measures to provide reliable 911 service. Certifying to meeting the benchmarks designated by the Commission for physical diversity, operational integrity, and network monitoring presumptively satisfies the requirement to provide reliable 911 service. CSPs may also use alternative measures that are reasonably sufficient to ensure reliability, in which case the FCC will determine whether the CSP is satisfying the requirement to provide reliable 911 service.

911 Reliability Benchmarks.

The 911 reliability benchmarks to which CSPs may certify pertain to physical diversity, operational integrity, and network monitoring. For each of these benchmarks, the requirements differ for legacy and IP circuits, paths, and facilities.

- *Physical diversity*. CSPs must certify that their covered 911 circuits and paths are physically diverse.
    - *Legacy circuits.* CSPs must certify for all legacy covered 911 circuits that they have conducted yearly diversity audits and all such circuits are tagged and are physically diverse such that no network facility element constitutes a single point of failure. Legacy covered 911 circuits are 911 facilities that originate at a selective router and terminate in the central office that serves the PSAP(s) to which the selective router delivers 911 calls. Legacy covered 911 circuits also include ALI and ANI facilities that originate at the ALI or ANI database and terminate in the central office that serves the PSAP(s) to which the ALI or ANI databases deliver 911 caller information, including all equipment in the serving central office necessary for the delivery of such information to the PSAP(s). In NG911 transitional architecture, circuits connected to LSRGs, ESGWs, or LPGs are also legacy covered 911 circuits.
    - *IP paths.* CSPs must certify for all IP covered 911 paths in their networks whether they have implemented automatic rerouting and failover capabilities, load balancing, and geographically distributed routing facilities, transport nodes, and node links sufficient to reasonably mitigate the risks of single points of failure. The use of dedicated diverse private facilities such as MPLS, cloud-based path redundancy, or VPN services over the public Internet or equally secure industry protocols as automatically re-routed paths satisfies this benchmark. IP covered 911 paths are paths carrying IP communications that either: originate at an NG911 Delivery Point or equivalent ESInet point of interconnection and terminate at the last routing facility before the NG911 PSAP or the legacy PSAP gateway; transport 911 traffic via major IP transport facilities for ultimate delivery at an NG911 Delivery Point or equivalent ESInet point of interconnection; or transport 911 traffic via IP 911 traffic aggregation facilities for ultimate delivery at an NG911 Delivery Point or equivalent ESInet point of interconnection.
- *Operational integrity*. CSPs must certify that their central offices hosting selective routers, ALI/ANI, or functioning as the last central office serving a PSAP, or their LNG, LIS, LSRG, ESGW, LPG, or NGCS functional elements achieve operational integrity.
    - *Legacy services and facilities*. CSPs must certify that their legacy services and facilities have backup power for at least 24 hours if the central office directly serves a PSAP, or for at least 72 hours if the central office hosts a selective router.
    - *IP services and facilities.* CSPs must certify that their IP-based services and facilities, including LNGs, LISs, LSRGs, ESGWs, LPGs, and NGCS facilities, have an uninterruptible and continuous power supply and automatic switchover to geographically diverse backup facilities sufficient to prevent service disruption.
    - *Transitional services and facilities*. Transitional elements for TDM-IP conversion, such as the LSRG or LPG, may certify to either the IP or legacy operational integrity benchmarks above, in the latter case with 24 hours of backup power.
- *Network monitoring*. CSPs must certify that they use physically diverse monitoring to detect outages and disruptions in their covered facilities.
    - *Legacy covered 911 circuits.* CSPs operating legacy covered 911 circuits from selective routers or equivalent facilities meet this benchmark by maintaining and annually auditing physically diverse monitoring aggregation points, monitoring links, and NOCs to monitor their covered 911 circuits from selective routers or equivalent routing facilities.

- *IP covered 911 facilities.* CSPs operating IP covered 911 services or facilities meet this benchmark by using geographically distributed automatic disruption detection and alarm systems to monitor their IP covered services and facilities, including their server facilities and their IP routers, transport nodes, and node links used for path diversity.

III. RECORDKEEPING AND REPORTING REQUIREMENTS

CSPs' recordkeeping and reporting requirements are codified at 47 CFR § 9.20 in part 9, subpart H of the FCC's rules.[2]

911 Reliability Certifications, Interoperability Reports, and Cessation Notices – 47 CFR § 9.20

911 Reliability Attestations and Certifications.

- *Attestations.* Within six months after the release of a public notice announcing compliance dates for information collections contained in the 911 reliability rules, any CSP that has not previously filed a 911 reliability certification must file an attestation with the FCC that it is a CSP. If a new entity starts providing a covered 911 service after this date, it must also file this one-time attestation when it begins service.
- *Certifications.* Within 18 months after the release of a public notice announcing compliance dates for information collections contained in the 911 reliability rules, a certifying official of each CSP must file a certification addressing each of the 911 reliability benchmarks. If the CSP does not conform the benchmarks of 911 reliability identified by the Commission, it must include in its certification for each of its covered 911 circuits or paths and covered 911 services whether it has taken alternative measures to mitigate the risks of not implementing these benchmarks, or that the benchmark is not applicable.
    - *Updating a certification.* A CSP must update its certification within 90 days of discovery of a material change that renders its certification inaccurate, and must exercise reasonable judgment in determining whether there is a material change to its ownership structure, networks, facilities, operations, or reliability practices that would trigger an updated filing. Material changes do not include changes which are remedied within 90 days, incremental improvements to conform to the reliability benchmarks for less than 50% of a CSP's covered 911 services, paths, and circuits, or pro forma ownership changes.
    - *Answering additional questions.* A CSP must also answer additional questions regarding its covered 911 services and covered 911 facilities as directed by the FCC's Public Safety and Homeland Security Bureau (Bureau).

911 Interoperability Reports.

Within 18 months after the release of a public notice announcing compliance dates for information collections contained in the 911 reliability rules, each NGCS and ESInet CSP must file a one-time report with the FCC identifying its specific actions and plans to enable NG911 interoperability, and must answer additional questions as directed by the Bureau. "Interoperability" is the technical and operational capability of NG911 systems, networks, and services to exchange 911 voice, text, data, and multimedia between jurisdictions, PSAPs, and service providers, in real time without the need for proprietary interfaces and regardless of jurisdiction, equipment, device, software, service provider, or other relevant factors.

[2] The 2013 rules for 911 reliability recordkeeping and reporting, previously codified at 47 CFR § 9.19, have been significantly revised and moved to 47 CFR § 9.20, which also contains new reporting requirements described in this section.

Confidential Treatment.

Information submitted with 911 reliability certifications and interoperability reports is presumed confidential to the extent that it consists of non-public descriptions of networks or facilities, compliance plans, or additional information requested by the Bureau. The mere fact that a CSP either filed or did not file a certification or report is not confidential.

911 Authority Access to Certifications and Reports.

- After the 18-month compliance date has passed, statewide, tribal, or territorial government 911 Authorities may ask CSPs to provide them with copies of their reliability certifications and interoperability reports to the extent those filings pertain to covered 911 services or covered 911 circuits and paths located within or providing services to the 911 Authority's jurisdiction.
- CSPs must provide eligible 911 Authorities copies of those filings within 14 days of a request. CSPs may condition granting such requests on the execution of a confidentiality agreement for these certifications and reports, and may redact or otherwise limit the produced copies to only information about networks and facilities located in or serving the 911 Authority's jurisdiction. The confidentiality terms may not be more stringent than those for access to Network Outage Reporting System (NORS) data under 47 CFR § 4.2.
- Eligible 911 Authorities may also request copies of the filings from the Bureau only after attempting to obtain such filings from CSPs. The filings produced will be subject to the same confidentiality as under 47 CFR § 4.2, but Bureau staff are not required to redact CSP filings when providing the filings under such procedures.

Record Retention.

CSPs must retain records related to their certifications and reports for two years after submitting a filing to the FCC and must make those records available to the FCC if requested. If the CSP keeps electronic records, the records must be produced to the FCC in electronic format. At a minimum, CSPs must keep audit records, internal reports about reliability and interoperability compliance, records of action to achieve reliability and interoperability compliance, and testing and maintenance of reliability and interoperability measures and technology.

CSP Cessation Notifications.

CSPs must file a notification with the FCC within 60 days after they cease providing all covered 911 services and are no longer CSPs.

Remedial Action Orders and Procedures.

The Chief of the Public Safety and Homeland Security Bureau (Bureau Chief) is authorized to order remedial action on a case-by-case basis to ensure the reliability of 911 service in accordance with the 911 reliability rules. The Bureau Chief may initiate non-public proceedings under certain circumstances to ensure compliance with the 911 reliability rules. If the 911 reliability certifications or other information available indicate that a CSP may not be taking reasonable measures to provide reliable 911 service, the Bureau Chief may send the CSP a notice describing apparent deficiencies and proposing remedial actions. The notice may include a request the CSP submit relevant documents or information to the Bureau. Within 30 days, CSPs must submit a written response to the notice and to provide any requested documents or information.

After 30 days, the Bureau Chief may issue an order finding the CSP deficient under the 911 reliability rules and specifying the actions the CSP must take to mitigate the deficiencies. The order may provide deadlines for the CSP to complete the required actions and may require the CSP to submit

new information to demonstrate its compliance. The CSP must send a copy of the Bureau Chief's order to the relevant 911 Authorities in the areas which the CSP's facilities or services have been found deficient and where the CSP is directed to take remedial action for reliability improvements.

V. IMPLEMENTATION DATES

The rules in the *Order* were published in the Federal Register on July 10, 2026, and therefore become effective on August 10, 2026. Compliance with some of the existing reliability requirements adopted in 2013 will remain in effect, but the Commission immediately eliminated the annual reporting requirement. In addition, compliance with new reliability and interoperability requirements will be gradually phased in. The Bureau will release a public notice announcing compliance dates following the approval of certain information collection provisions by the Office of Management and Budget.

Legacy 911 Reliability Requirements.

- CSPs covered by the 2013 rules are entities providing 911, E911, or NG911 capabilities, including call routing, ALI, ANI, or the functional equivalent of those capabilities, directly to a PSAP; the operation of central office(s) that directly serve a PSAP, meaning the central office hosts a selective router or ALI/ANI database or equivalent NG911 capabilities, or is the last service-provider facility through which a 911 trunk or administrative line passes before connecting to a PSAP. These CSPs remain subject to the requirement to take reasonable measures to provide reliable 911 service specified in the 2013 rules, which remain in effect.[3]
- The legacy requirement to send a notification to the FCC when a CSP ceases providing all covered 911 services and is no longer a CSP also remains in effect for CSPs covered by the 2013 rules, as do the legacy recordkeeping requirements.[4]
- As of August 10, 2026, the Commission has eliminated the existing annual certification filing requirement for all CSPs, including for CSPs covered by the 2013 rules, and replaced it with the modified certification and reporting requirements described in the next paragraph below.

Phasing In New 911 Reliability, Interoperability, and Reporting Requirements.

- Six months after the release of the Bureau's public notice announcing compliance dates under the new rules, CSPs that have not previously filed a 911 reliability certification will be required to file an attestation identifying themselves as CSPs to the FCC. Any new CSP that begins covered 911 service after this date must submit an attestation when it begins service.
- Eighteen months after the release of the Bureau's public notice:
    - All CSPs will be required to file an initial reliability certification with the Commission.
    - CSPs providing NGCS and ESInet covered 911 services are also required to file one-time interoperability reports with the Commission.
    - All CSPs will be required to comply with the requirement to provide reliable 911 service.
    - Eligible 911 Authorities may also request 911 reliability certifications from CSPs.

---

[3] 47 CFR § 9.19(b). *See also Improving 911 Reliability et al.*, PS Docket Nos. 13-75 et al., Report and Order, 28 FCC Rcd 17476, 17492, para. 45 (2013) ("To promote reliable 911 service, we adopt a rule that requires all Covered 911 Service Providers to take reasonable measures to ensure 911 circuit diversity, availability of backup power at central offices that directly serve PSAPs, and diversity of network monitoring links"). Small businesses with further questions about the 2013 rules may also consult the Small Entity Compliance Guide for those rules, available at: https://www.fcc.gov/document/improving-911-reliability.

[4] *See* 47 CFR §§ 9.20(e), (f). These rules were previously codified at 47 CFR §§ 9.19(d)(3), (d)(4).

- After the 18-month compliance date, a CSP must file an updated certification within 90 days after it discovers a material change that renders its previous certification no longer accurate.

V. INTERNET LINKS

A copy of the *Order* is available at:

https://www.fcc.gov/document/fcc-modernizes-next-generation-911-reliability-and-interoperability-0

A copy of the Federal Register Summary of the *Order* is available at:

https://www.federalregister.gov/documents/2026/07/10/2026-13998/facilitating-implementation-of-next-generation-911-services-ng911-improving-911-reliability

The complete text of the newly amended 47 CFR §§ 9.19 and 9.20 regulations at part 9, subpart H of the FCC's rules will be available after August 10, 2026 at:

https://www.ecfr.gov/current/title-47/chapter-I/subchapter-A/part-9/subpart-H

A copy of the Small Entity Compliance Guide for the 2013 911 reliability rules is available at:

https://www.fcc.gov/document/improving-911-reliability